DEVELOPMENT OF A GOVERNANCE FRAMEWORK FOR DELIVERY OF COLLABORATIVE AND SECURITY-MINDED BIM PROJECTS

Mohammed Tahir Mamun

P.H.D Thesis **2021**

DEVELOPMENT OF A GOVERNANCE FRAMEWORK FOR DELIVERY OF COLLABORATIVE AND SECURITY-MINDED BIM PROJECTS

Mohammed Tahir Mamun

School of Science, Engineering and Environment

University of Salford, Salford, UK

Submitted in Partial Fulfilment of the Requirements of the Degree of Doctor of Philosophy, October 2021

List of figures

Table of Abbreviations

AEC	Architectural, Engineering and Construction
AIR	Asset Information Requirements
API	Application Programming Interface
BEP	BIM Execution Plan
BIM	Building Information Model, Modelling or Management
BMS	Building Management System
BSI	British Standards Institution
CAD	Computer Aided Design
CDE	Common Data Environment
CISO	Chief Information Security Officer
CNI	Critical National Infrastructure
CPNI	Centre for Protection of National Infrastructures
COBie	Construction Operations Building Information Exchange
DBB	Design, Bid, Build Project Delivery
DT	Downstream collaborator
EIRS	Employer's Information Requirements
GIS	Geographic Information Systems
GR	Governing Role
GUID	Globally Unique Identified
ICO	Information Commissioners Officer
ID	Interdependency (task or collaborator)
IPD	Integrated Project Delivery
IDM	Information Delivery Manual
IFC	Industry Foundation Classes
IG	Information generation
IM	Information management
IPR	Intellectual property rights
IS	Information sharing
LOI and LOD	Level of Information – Level of Detail
MCS	Model Collaboration Server
MEP	Mechanical, Electrical and Plumbing
MVD	Model View Definition
NEC	New Engineering and Construction Contract Suite
PLQ	Plain Language Questions
RACI	Responsible, Accountable, Consulted, Informed (Responsibility Matrix)
RBAC	Role Based Access Control
RFI	Request for information
SaaS	Software as a service
SCADA	Supervisory control and data acquisition
SME	Small to medium enterprises
TC	Team level collaborator (individual within team)
UT	Upstream collaborator
TM	Team Manager

Acknowledgements

I would like to thank my supervisory team, the Thinklab and Arup for funding this research project. I express my sincere gratitude to my supervisors Professor Terrence Fernando and Mr Martin Simpson for their continued expertise, guidance, and encouragement. I cannot thank them enough for their input, support, motivation and feedback, especially in these difficult times. This work would not have been possible without them. I also thank Dr Kate Canning for being absolutely amazing in the last leg of the work. A special thank you to Hanneke van Dijk for your door always being open for the motivational support. I also thank everyone who has contributed to the research and has helped me along the way, of course, including the participants of the research. I of course thank my wife Fatima for dealing with my tantrums before submission. I am sure she is happy to see this work finally sent out. Finally, I of course thank my family, my mother and father (ILWIR). Above all, I thank God for guiding my knowledge of the unseen.

Declaration

I declare that the research in this thesis was solely carried out by me. It has not been previously submitted to this or any other institute for the award of this degree or any other qualification.

Abstract

This study explores secure-collaboration for BIM projects in response to concerns as to whether project environments concerned with critical national infrastructure are able to govern digital security-risks whilst also reconciling tensions between collaborative motives, leading to difficulties in sharing enough information to ensure stakeholder efficiency whilst not exposing sensitivities and elevating security-risk. This research aims to address these issues by: **Devising a conceptual process and data governance framework to enable secure collaboration for BIM projects**. In achieving this aim, the study captures the framework's requirements by answering the first research question: **What is the nature of tensions between collaboration and security motives within security-minded BIM projects that are barriers to achieving secure-collaboration?** This question's answer is central to answering the second question: **What is the nature of the process and data governance framework that is required to resolve existing tensions and enable secure-collaboration?**

This thesis captures requirements via a thorough study (primary and secondary) in the context of security-minded BIM projects. The design-science methodology was adopted to guide the framework development and evaluation; semi-structured interviews with 13 experts were used to diagnose the tensions concerning: security-risk governance, BIM process and technology implementation, alongside BIM governance limitations. Based upon findings, the framework's requirements for comprising process and data governance concepts were developed. The framework was evaluated with 8 experts via a qualitative feedback categorisation technique to assess its capacity to facilitate secure-collaboration.

The outcome of the diagnostics process revealed that tensions arise within projects due to a lack of a holistic security-risk governance approach, and a misalignment between project collaboration and security requirements. This leads to a cascade of incompatible project implementation choices, which limits the efficacy of information governance to appropriately secure critical assets, whilst diminishing collaboration capacity to ensure a timely and cost-effective project-delivery. Stakeholders are also constrained by security-measures which are not integrated with their informational needs, resulting in issues such as securely coordinating sensitive information amongst partners, or professionals being unable to access information due to inaccurate sensitivity classification and clearance constraints. These tensions are also linked to divergent cultural pressures for increased digitisation and openness, versus the need for security-minded approaches which are accompanied by administrative, commercial and contractual burdens. These tensions are the sources of great frustration within security-minded environments interviewed in effortlessly achieving secure collaboration, whereas a bleaker picture is present for the broader AEC sector as to whether organisations can support the secure digitisation needs of inexperienced clients and protect their assets within an evolving digital security-risk landscape.

Alleviating such tensions requires clients to apply holistic security-risk governance approaches and define integrated project requirements that reconcile security, collaboration and efficiency motives. Findings also indicate that information-flow tensions are present for professionals to be able to seamlessly share and receive only the necessary information, when and to who necessary, at an appropriate and secured level of detail. Alleviating such tensions is difficult as they are tied to the limitations of BIM-based governance approaches utilised within practices. To resolve such information-flow tensions, findings propose that the key elements to be integrated into the process and data governance framework are considerations for information planning, transaction and governance concepts. At an overarching level, this is by ensuring practitioners securely share and receive only the atomic information-sets which are necessary for them to deliver high-quality project outcomes. The proposed framework has been validated via a high-level qualitative technique as the framework is conceptual in nature. Therefore, future research is required to implement and validate the framework in real-life project settings.

1 Motivation

The process of design and construction in the Architectural, Engineering and Construction (AEC) industry is long and arduous, going through numerous phases. Within any given project phase, multiple entities are grouped within multi-disciplinary project delivery-teams (Shen et al., 2010). These teams are inclusive of disjoint disciplines within AEC projects such as architects, civil / structural engineers, MEP etc. (Stewart, 2015; Eastman et al., 2018). An overlap of disparate sources is necessary as a 'master builder' who is aware of every aspect of work, from start to completion does not exist (Prins and Owen, 2010). In reality, professionals possess implicit knowledge and competencies mostly constrained to their own disciplines (Macdonald, 2011; Crotty, 2016).

Building Information Modelling (BIM) as a methodology for digitial AEC work is however particularly useful for facilitating this overlap by allowing different disciplines to effectively coordinate design efforts in an otherwise fragmented sector (Isikdag and Underwood, 2010) through the application of synergetic technologies and work processes (Succar 2009; Bolpagni and Hooper, 2021). BIM informtion-management approaches include the utilisation of shared data repositories in the industry specific form of common data environments (CDEs) which improve the management of project information throughout the entirety of the project lifecycle (Ford and Shana'a, 2020a), thereby optimising project workflows (Al Hattab and Hamzeh, 2013; Meadati and Irizarry, 2014).

Further technological visions for BIM includes fully integrated and secure collaborative BIM workflow systems (Macdonald, 2011; Afsari et al., 2016) through which interoperable information can be more accurately and appropriately disseminated to AEC professionals through centralised or distributed repositories of knowledge (Underwood and Isikdag, 2011). Complex issues must still however be addressed in enabling both collaborative and security-minded multi-organisational design work within virtual, physical, and contractual environments (Mahamadu et al., 2013; Pärn and Soto, 2020).

Traditional security focuses in the built-environment have been upon the physical / operations security (Pärn and Soto, 2020) where digital security has been overlooked (Mantha et al., 2021b). Despite this, instances of cyber-attacks pertinent to the sector are increasing (Pärn and Soto, 2020). A notable attack on a sensitive asset was upon the Australian Intelligence Service HQ where attackers exploited weaknesses in disjoint construction supply-chains to infiltrate the networks of a contractor. This led to the exposure of the asset's design-plans and the locations of communication and computer networks (Taylor, 2013). Further still are attacks which exploit the emergence of cyber-physical assets, such as the attack on a US based retailer where threat actors gained access to the retailer's systems via third party access of its heating, ventilation and air conditioning building control vendors (Lawson, 2015). Politically motivated attacks include those afflicting critical national infrastructure (CNI), including infamous cyber-attacks which disarmed, and exposed Iranian industrial and national military assets at a nuclear facility (Lindsay, 2015). Other incidents include a malware attack on sensitive control systems of a power grid in Ukraine which led to blackouts for hundreds of thousands (Mantha et al., 2021a).

Whilst a growing menace is afflicting CNI, the relationship between risks to posed to CNI from the increased digitisation efforts for the built-environment has not been clearly correlated (Pärn & Soto, 2020). This is despite the central role in the design and construction of CNI wherein 'golden threads' of accumulating data on such assets presents a scenario of a 'doubled edged sword'. On one hand, digitisation leads to more sound asset operations for services such as energy-generation and transport via the transformation of accurate design-information to models and services for effective asset-operations (National Infrastructure Commission, 2017). On the other, the same modes of information-delivery present avenues for attackers to exploit the interconnectivity posed – even before operations commence (Ghadiminia et al., 2021).

As such, there is a need to further expand the sectors capability to act as a first-line of defence for such sensitive assets and the built-environment as a whole. Similarly to ensuring optimal efficiency of asset-operations whilst maintaining security, the AEC industry must also be able to securely optimise its design and construction workflow efficiency. Specific gaps yet to be solved include the ability to identify, accurately and easily *'who should possess what information at any point in time?'* (Jonas, 2007). This is linked to a further question of *'who needs to provide what information, to meet what other parties need to know?'* (Jonas, 2007). Answers to these questions must also consider that information-planning requirements of AEC stakeholders are obscure, constantly shifting and therefore slowly uncovered as projects progress (Boyes, 2014; Bolpagni and Hooper, 2021).

As such, these gaps infringe upon a broader perspective of how stakeholders approach information-planning, and thus cannot be solved solely via infrastructure-level security mechanisms alone (Singh et al., 2011; Mahamadu et al., 2013; Oraee et al., 2019). Such mechanisms to set controls over information include role-based access-control mechanisms which provide the ability to set constraints, but do not themselves provide the necessary project-knowledge of what information practitioners require (Alreshidi et al., 2014). They are also not explicitly tied to context of task level work (Beresnevichiene, 2003; Ghadiminia et al., 2021) that AEC practitioners must carry out. This represents risks of limited specificity and that practitioners are provided too little or too much information (Beresnevichiene, 2003; Mahamadu et al., 2013).

Furthermore, governing roles such as information managers are expected to possess knowledge over what 'ground-level' professionals require (Mahamadu et al., 2013; BSI, 2020). As such, dialogue between professionals and governing roles should occur as part of progressive security-conscious decisions on what information practitioners should have access to throughout the entire project process (Beresnevichiene, 2003; Christian, 2020). Currently, this dialogue and knowledge capture is not detailed as part of BIM information-planning methods and correspondingly embedded within BIM information-management (IM) systems (Beach et al., 2015).

In aiming to resolve the aforementioned concerns, the focus of this research will be to address process and information governance via the development of a process and data governance framework. The framework represents a future 'to-be' type of approach in achieving secure collaboration within BIM projects where the specific focus is upon atomic BIM project processes and information-flows between interdependent professionals, both intra and inter-organisationally. The framework explores conceptual considerations for how stakeholders and practitioners could work as part of the overarching approach that is proposed to enable secure collaboration on BIM projects. The concepts explored simultaneously serve as considerations for how the proposed methods of work could be implemented via future system solutions. These concepts include atomic information-security methods which incorporate the complex and evolving process requirements of any given project (Kayworth and Whitten, 2012). Such methods should be matched to governance approaches that can be used by governing roles to make informed decisions on the information professionals require of their work.

As such, the specific purpose of this project is to investigate the necessary steps and mechanisms to offer 'Secure collaboration during complex BIM projects via process-oriented governance over atomic information-flows on a need to know and share basis.' Accomplishing this aim will require in-depth analysis of the difficulties faced within the context of projects of a security-critical nature. Issues captured within this context will be analysed through the lens of specific themes in academia (Succar, 2009) such as 'data-management' and 'access-control' and 'data-governance' (Alreshidi et al., 2017).

Such environments have been chosen to extract, identify and analyse security concerns relevant both to security-minded projects and the broader AEC sector (BSI, 2020). Security-minded projects include those pertaining to the design, construction, and management of critical infrastructure assets. They were chosen as their working practices introduce rigorous constraints over what information can be shared amongst stakeholders due to serious adverse consequences if sensitive information were to be exposed. (Bernstein and Pittman, 2004; Cabinet Office, 2016, 2018). However, such working practices may also mean that professionals are unable to gain access to asset related data (sensitive or otherwise) necessary for their collaborative workflows (Boyes, 2013; BSI, 2020).

This points to a potential tension between collaborative and overly security-rigorous approaches. Recent case studies for CNI having encountered this tension for secure and collaborative governance include infrastructure operations within the US department of transportation. The case study pointed to difficulties in effectively governing their processes to balance the value-driven perspective of reliable, organised and accurate data whilst effortlessly governing security-constraints as one of numerous tensions (Christian, 2020). Furthermore, operations within the nuclear sector have also dealt with the tensions of both seeking to restrict information, whilst also ensuring openness and accessibility, having conceived the almost paradoxical nature of these conflicting motives (Office for Nuclear Regulation, 2014; Ulrich et al., 2015). Scenarios of such tensions conflict with the aim of improving workflows through the realisation of more effective coordination of information amongst professionals. Reconciling such differences will therefore require proportional and balanced approaches which enable both security and collaboration, but not at a detriment to either motive (BSI, 2020).

In conclusion, a tension has presented itself via divergent approaches for current inadequate security procedures and requirements to improve the collaborative potential of security-minded projects, particularly during the design-phase. It is proposed that this gap must be bridged to deliver both benefits by developing a framework to detail procedural and technological approaches to future secure and collaborative information-flows. Such an approach must be applicable to secure settings and projects whilst also delivering improvements to collaboration for disciplinary professionals. The difficulty is identifying what approaches will be required to facilitate secure by design BIM where current visions are clouded by the many different ideas in academia and industry on how to achieve this high-level vision (Jiao et al., 2013; LDAC, 2014; Miettinen and Paavola, 2014). This being a source of confusion in industry of how to make use of such research. As such, research must be mutually relevant for both academia and industry through the research being a two-way process that informs each other. The hope is that research will be of value to both parties and close a gap existing in industry.

1.1 Research Aims

The aim of this research is to devise a conceptual process and data governance framework to enable secure collaboration for BIM projects. This aim will be achieved through the following research objectives and answering the following research questions.

1.2 Research Questions

This study aims to explore and answer the following research questions.

1) What is the nature of tensions that exist between collaboration and security motives within security-minded BIM projects that are barriers to achieving secure collaboration?

2) What is the nature of the process and data governance framework that is required to resolve existing tensions and enable secure collaboration within security-minded BIM projects?

1.3 Research Objectives

1) To conduct a thorough study (primary and secondary) to identify the key security and collaboration barriers within complex security-minded projects and to identify the corresponding enablers for secure collaboration.

2) To capture security and collaboration needs within a governance framework for enabling future secure collaboration on security-minded BIM projects.

3) To explore the governance concepts that will be necessary in enabling future secure and collaborative BIM processes.

4) To validate the framework with a number of experts.

2 Research Background

2.1 Industry Trends

The U.K. AEC Industry should currently be operating in-line with the level of BIM maturity that the ISO 19650 BIM standards (ISO, 2018a) promote as part of optimising all stages of the digital construction project-lifecycle. The reality however is that this is still a mounting challenge to achieve in view of the complexities of upskilling the entire sector, and the lack of consensus of how to implement BIM information-mangement (IM) standards (Construction Innovation Hub, 2021) such as the ISO 19650 suite (ISO, 2018a, 2018b). This is both for motives of effective project-delivery, but also in deriving quality asset-information to drive operational benefits such as building-safety and other client and user-driven outcomes (Ford and Shana'a, 2020b). This is despite an increasing amount of effort by practitioners (Underwood and Isikdag, 2011; Kähkönen and Rannisto, 2015), and academia to guide industry vision and promote further BIM maturity (British Standards Institution, 2013; Ganah and John, 2015).

This is due to a range of overlapping difficulties in implementing BIM as a driver for holistic digital process optimisation (Azhar, 2011; Hartmann et al., 2012; Oraee et al., 2019), the mismatch of technologies to meet real industry needs (Tse et al., 2005; Howard and Björk, 2008; Papadonikolaki et al., 2019) and the culutural, contractual and socio-technical barriers in deploying open and efficient collaboration across multi-organisational units comprised of long, disjointed supply-chains (García de Soto et al., 2020). Despite these challenges, both industry and academia have set their sights on progressing to further optimised methods of digital design and construction, detailing visions of what it will mean in practice and how it will be achieved (BIM Task Group, 2015).

These visions include fully integrated, concurrent, and distributed BIM workflows, proposed for the realisation of more productive and efficient work and IM scenarios during the design, construction and operational phases (Sun et al., 2017; PwC, 2020). This in turn links to desires of 'golden-threads', persistent information on a built-asset from inception to decommissioning, where actor's requirements to produce atomic BIM information is kept traceable, accurate and up to date (Atkins, 2021). This also acts as the information-delivery tube for digital-twins (Parn & Edwards, 2019) and the wide-reaching societal benefits that these aim to bring. For example, to prevent the damage of infrastructure arising from a lack of oversight of how weaknesses posed from interconnection of infrastructure (Centre for Digital Built Britain, 2020).

It has however been noted such visions are insulated by rhetoric of their benefits (Miettinen and Paavola, 2014) throughout the AEC sphere, which feature limited criticality of how these visions will be applied (Zomer et al., 2020), and the challenges to be overcome to achieve their benefits. For example, the challenges of factoring small to medium enterprises (SMEs) into the bigger picture of effecitve project delivery (Sun et al., 2017) includes still-standing issues of their readiness to embrace new forms of collaborative and digital workflows (Ganah and John, 2015; Ahmed and Abuelmaatti, 2018) where implementing BIM for smaller projects is still a significant issue (Chartered Institute of Building, 2020).

Other related issues include contractual arrangements which limit equal participation amongst stakeholders (Elghaish et al., 2020). Visions of intergrated project delivery (IPD) approaches aimed to dismantle these types of issues by encouraging shared risk and reward cultures (Winfield and Rock, 2018) and increase connectivity amongst stakeholders at all levels; this is is of especial importance given the disconnectivity of workforce units as a result of the Covid-19 pandemic (Evans et al., 2021). Such visions are however blocked without comprehensive improvement in all project-areas. This includes overcoming technical barriers in enabling interoperable exchage (Oraee et al., 2019), to addressing a lack of project governance over clear, agreed upon policy over stakeholder's roles, resposibilities (Alreshidi et al., 2017) to name but a few of the issues.

Visions for future BIM based paradigms, such as the restructuring of inefficient workflows must therefore be met by building upon and solving issues still present in industry (Oraee et al., 2021). This further includes issues faced in improving IM which broadly fall under the need to synchronously address contractual, operational, managerial and technical difficulties as part of moving forward with future visions (Newman et al., 2020). Such issues faced under present BIM workflows (Succar 2009; Azhar, 2011) were envisioned to be solvable by implementing cloud-based, integrated and openBIM (Beetz et al., 2010; Berlo, 2019).

OpenBIM has been characterised by enabling software data-exchange interoperability agenda (Berlo et al., 2012). At their core, the propositions of open and integrated approaches are to improve difficulties faced within work environments such as ineffective IS amongst participants throughout all project phases (Afsari, Eastman and Shelden, 2016; Pauwels et al., 2020). Further technical development and research is required however to address the needs of growing interoperability use-cases for AEC domains (Berlo, 2019), such as road and rail (Ait-Lamallam et al., 2021) as well as the security aspects of integrated, multi-organisational implementations (Azhar, 2011; Berlo et al., 2012; Parn and Edwards, 2019).

For example, the extranet based nature of network infrastructures such as SaaS is open to security-risks if not properly underpinned by appropriate network security policy (Boyes, 2015). Within such scenarios, sensitive information such as construction employee details can be accessed and is open to misuse by malicious parties (Boyes, 2014; CPNI, 2020). AEC collaboration 'Common Data Environment's' (CDEs) inherit such generalist cyber-security concerns (Singh et al., 2011; Berlo et al., 2012) alongside an additional layer of 'secure collaboration' complexity. This arises by factoring in the collaborative facilities of CDEs and the dispersed stakeholder environments which they serve to integrate (Singh et al., 2011). The integrated usage of CDEs amongst numerous stakeholders and appointment-chains (Ford and Shana'a, 2020a) requires new atomic layers of management methods to facilitate secure collaborative workflows of professionals wherein their logically centralised nature leads to elevated security-concerns such as the aggregation or cross association of datasets (Mahamadu et al., 2013; BSI, 2020).

Atomic data management approaches to deal with this security aspect of such platforms and digital workflows are still in their infancy and relatively uncovered within the AEC domain (Alreshidi et al., 2014; Mantha et al., 2021). Furthermore, the need for collaborative approaches built upon, and explicitly addressing an accurate security context of project work has only recently become a concern within the AEC sector and noticed as an avenue for further research (Mantha et al., 2021b). As a result, there will be many themes of secure and collaborative atomic data governance that will become apparent through further exploration of the problem-environment (Hevner et al., 2004).

Accordingly, concerns identified are in relation to secure collaboration in the AEC industry where the adoption of cloud-based technologies and digital workflows more broadly possesses their own significant and unique risks (BSI, 2020). These include exposure of valuable information in the nations interests and concerns over data integrity and privacy especially when multiple organisations are involved (Mahamadu et al., 2013; BSI, 2020). There are obviously technical hurdles to overcome, but socio-technical issues such as distrustful nature to other project participants, and limited transparency (Oraee et al., 2019) must also be overcome.

The concerns of project parties working through centralised environments are not unfounded (Redmond et al., 2012; Oraee et al., 2019). Due to the one-of-a-kind nature of construction projects, which sees the inclusion of temporary and often inexperienced participants (Wilkinson, 2014), it is necessary to ensure that these integrated technologies provide the mechanisms and appropriate policy to uphold the necessary security requirements when working in integrated virtual organisations (Wilkinson, 2014). Furthermore, cultural, legal and contractual issues are to be addressed here also through the shifting and reviewing of contractual arrangements (Eadie et al., 2015; British Standards Institution, 2015).

These issues must be addressed based on the industries strategy to progress to optimised methods of working (Infrastructure and Projects Authority, 2016) and the integration of datasets in readying a national digital infrastructure (Centre for Digital Built Britain, 2020). The deployment of digital BIM enabled workflows, whilst ignoring security concerns is not an ideal future vision. Costs of security breaches from other sectors have ranged in the millions with significant downtime (Soomro et al., 2016). This is especially problematic for security-minded environments handling exchange of highly sensitive information (CPNI, 2020). How extensive security breaches involving multiple parties on larger CNI projects, however, has still yet to be conclusively seen (McGraw, 2013). This is an evolving area of concern that must be proactively addressed now to avoid the emergence, and realisation of future threats (García de Soto et al., 2020).

2.2 BIM Based Collaboration

The adoption of BIM has shown to have a significant positive impact on financial and efficiency benefits of construction projects alongside the reduction of project risk (Underwood and Khosrowshahi, 2012; NBS, 2020). This demonstrates the importance of multi-organisational stakeholders engaging in collaborative workflows (Latiffi et al., 2014) to enable coordinated work processes and optimised information management (IM) amongst stakeholders (Atkins, 2021). This in turn enables stakeholders to progress their project tasks effectively (Egan, 1998; Carson and Baker, 2006; Kähkönen and Rannisto, 2015; Eastman, 2018) and is essential for overall project success (Raziq et al., 2020).

AEC project work is also inherently knowledge intensive (Kamara et al., 2002; Shi, Wang, and Guo, 2021) where professionals must possess the *'know-how'* to undertake their tasks (Hossain et al., 2020). For example, clear communication of design intent via BIM enabled processes provides them with the knowledge necessary to carry out their own tasks, feedback on others and come to a mutual understanding of others work and its relation to their own (Kamara et al., 2002; Wilkinson, 2014). This ultimately results in a shared design generation greater and more innovative than the sum of its parts (Wilkinson, 2014; Shi, Wang, & Guo, 2021).

This can only however come about as a continuous and meaningful stream of information from other project participants (Succar 2009; Kassem et al., 2013). Sufficient communication, co-ordination amongst professionals on what their work entails (Patel, Pettitt and Wilson, 2012), as well as the effective IM as an explicit aspect of the total knowledge to be exchanged (Kamara et al., 2002; Shi et al., 2021), are crucial enablers of collaboration. IM is especially important because of how quality information is intrinsically linked as a pre-requisite for effective collaborative project flows (Emmitt and Gorse, 2006; Dennis, Fuller and Valacich, 2008; Ford and Shana'a, 2020b).

Thus far however, the implementation of BIM maturity has been criticised as being too 'standalone' in not fully fostering integrated partnerships (Chuang et al., 2011; Wong et al., 2014) and thereby limiting the potential for high-quality information-flows amongst stakeholders (Durdyev et al., 2019; Winfield 2020). To this end, the combination of integrated project delivery methods and digital workflows have been envisaged to meet an ideal collaborative scenario, encompassing the entirety of professionals in a manner which breaks down the inefficiencies associated with traditional project-delivery methods and phases (Succar 2009; Durdyev et al., 2019). Consequently, the ideal is for project-work to become more co-ordinated and streamlined (Succar 2009) where it will be possible to realise multi-disciplinary work scenarios such as professionals carrying out design-work concurrently, and gain efficiency benefits derived from optimised collaborative modes of work (Dave et al., 2013; Adamu et al., 2015; Oraee et al., 2021).

Visions of integrated collaborative environments both in academic, software-vendor and project implementation contexts have however been criticised too focused on the technological dimensions of collaboration (Charalambous et al., 2012; Miettinen and Paavola, 2014; Oraee et al., 2019). For example, systems procurement is influenced by the vendor's marketing of their functionalities (Prins and Owen, 2010) as opposed to providing a clear strategy for inter-organisational collaboration (Bolpagni and Hooper, 2021) where effective collaboration amongst project-participants relies on far more than technology driven initiatives (Oraee et al., 2021). Collaboration is a vast social construct where many interacting factors are at play (Patel et al., 2012; Coates, Biscaya, and Rachid, 2018).

System development and implementation must also therefore explicitly incorporate the actual collaborative characteristic of AEC multi-disciplinary and organisational project work based around an in-depth understanding of how optimal collaboration is enabled through technology (Lou et al., 2012; Shafiq et al., 2013). As a pre-requisite for this incorporation, both the current and envisioned nature of collaborative project-work must be understood against social-working and behavioural theories to allow for optimal collaborative potential amongst participants and project work as a whole (Steiner, 1972; Kaptelinin and Nardi, 2007; Zomer et al., 2020).

The application of these theories to solve problems such as ineffective and untrusting temporary multi-organisational structures found in real-life BIM projects has only recently begun to be applied to research (Miettinen et al., 2012; Miettinen and Paavola, 2014; Adamu et al., 2015). In addition, cultural and mindset issues limit stakeholders in getting the most from digital workflows, where further issues include contracts defined by legal teams with limited understanding of the principles of effective collaboration (Winfield, 2020).

Improvements to collaborative potential will therefore also be approached from a project and organisational eco-system perspective (Simpson et al., 2019) where inhibitors to collaboration such as redundant and un-coordinated business workflows and information-flows will be eliminated and restructured (Kerosuo et al., 2015; BIM Task Group, 2015). There is also a need to address the issues that still pose significant issues to inter-organisational collaboration due to the industries inherent fragmentation (Leicht et al., 2009; Winfield, 2020) along with other inhibitors such as dated and potentially adversarial contracts (Construction Management Association of America, 2012; Winfield, 2020).

The potential for organisations to collaborate is also seen to be limited when a strict security context is present (Zomer et al., 2020). This can be due to factors such as the application of strict policies on exchanging information (British Standards Institution, 2015) which can adversely impact project communication and coordination (Emmtt and Gorse, 2007). On the other hand, effective security spanning multiple dimensions is known to be difficult to achieve (British Standards Institution, 2014; Soomro, Shah and Ahmed, 2016). Enabling secure collaboration on top of this is complex where achieving effective, honest and open collaboration amongst stakeholders is itself a challenge within the sector as a whole (CPNI, 2020).

In conclusion, the problem to be addressed is multi-faceted because issues exist on both sides of the security and collaboration equation, without a clear route from both a system and project IM perspective to facilitate security whilst maximising collaborative potential (Needham-Laing, 2016). An approach must therefore be identified that can derive the aforementioned benefits of collaboration and as open as possible data sharing whilst not exposing a project to unnecessary security-risks. Issues still to be addressed in defining such an approach pertain to effective IM to facilitate secure collaborative workflows (Jørgensen et al., 2008; Zhang, Beetz, and Weise, 2015) and how these can be achieved via atomic process and data governance approaches. The approach must address the progression of 'as-is' (current) IM practices that are matched to asynchronous and inefficient workflows (Succar 2009) throughout wider practice, to visions of integrated collaborative workflows (Winfield and Rock, 2018). Approaches must also address security and privacy concerns gaps when moving to more integrated and open approaches to work such as IPD (Miettinen and Paavola, 2014).

2.3 Information and Data Management

The need for high-quality information is crucial to any enterprise, and the built environment is no different. Rather, the drivers for quality information are only increasing due to a need for effective asset information-management at all project phases, and driving societal-level improvements for digital twins, infrastructure and the public good (Atkins, 2021). Issues faced of information-management (IM) and information-sharing (IS) approaches however are their inability to uphold the primary characteristics of computability (Bernstein and Pittman, 2004) and overall utility on projects such as timeliness, information to be meaningful and accurate at the point of access (Demian et al., 2019) and to be seamlessly coordinated between social and system-based actors in facilitating collaborative workflows (Dennis et al., 2008; Jørgensen et al., 2008).

Early issues in relation to document-based IM such as such as physical degradation (Rezgui and Cooper, 2002; İLAL, 2007) were solved through digitised BIM repositories (Meadati and Irizarry, 2014). Digital IM issues such as such as the error prone and inconsistent nature of information deliverables (Smith and Tardif, 2009) however still exist (Oraee et al., 2021), pointing to immature and still evolving digital IM approaches in industry (Akintoye et al., 2012; Construction Innovation Hub, 2021). This poses as a barrier to effective collaboration during the project-lifecycle, and also poses considerable issues for Construction 4.0 (Winfield, 2020).

Ill-structured, inconsistent, and redundant information arises within current practices due to poor managerial approaches and inefficient utilisation of data amongst stakeholders (Smith and Tardif, 2009). Technical complexities have also arisen due to the requirement for the IM capabilities of software to be based around a new socio-technological field (Volk et al., 2014) which integrates processes, people, policies, and technology as seen through approaches such as IPD (Elghaish et al., 2019). This has led to evolving and unsolved business scenarios where the needs of stakeholders for managed information are blurred (Bernstein and Pittman, 2004; Sackey et al., 2015). Complex questions such as 'who is the owner of data generated through inter-organisational project work at any particular point in time?' have arisen in light integrated approaches (Volk et al., 2014; Atkins, 2021) and nature of BIM information-flows where information is passed through and made use of by multiple actors throughout different phases (Pradeep et al., 2021).

Digital IM approaches must therefore evolve around unsolved business scenarios, incorporating them, but also aiming to minimise operational disruption (Arayici et al., 2012; Hartmann et al., 2012) as a first step to optimising workflows in practice (Bernstein and Pittman, 2005; Construction Innovation Hub, 2021). Future approaches must incorporate the unique needs of stakeholders, where organisational specific factors such as their processes and working practices must be accounted for to suit the bigger picture needs of the project (Singh et al., 2011; Arayici et al., 2012). For example, issues of legacy practices within organisations poses a significant barrier for the industry as a whole to adopt consistent IM approaches based upon the ISO standards (ISO, 2018a, 2018b). As such, many nuances must be accounted for in the development of holistic IM approaches (Singh et al., 2011; Arayici et al., 2012) as opposed to solely technology driven approaches (Autodesk, 2014; Papadonikolaki et al., 2019).

IM also comprises data management where within the context of design work, data-rich BIM models must be managed (Eastman et al., 2018). Data management approaches must be able to facilitate effective multi-party usage of BIM datasets within cloud environments such that despite multiple parties acting upon the data, it is consistent, accurate, up to date and available at all times in order to facilitate further collaborative work based around the BIM data (Singh et al., 2011, Shafiq et al., 2013). Another issue is ability to understand who has acted upon what data, and potential liabilities stemming from inaccurate information (Pradeep et al., 2021).

Further associated to effective IM, 'Interoperability' which enables multiple parties to effectively integrate information generated from proprietary software tools with other software tools and data environments resulting in accurate and usable information that can be used to facilitate effective downstream processes (Yang and Zhang, 2006; Shelden et al., 2020). Achieving this must account for both syntactic and semantic interoperability so that the entirety of a given dataset, including the intent behind the original information can be properly conveyed and translated in the receiving tools data-schema resulting in an ideal 1-1 representation of the original data and design-intent (Yang and Zhang, 2006). This is to enable the design and thereby commercial benefits of effective interoperability (Gallaher et al., 2004) and maintaining a golden thread of high-quality information (BIM Interoperability Expert Group, 2020).

Enabling interoperable workflows relies upon the industry foundation classes (IFC) as a common schema to describe the digital world of the built-environment, and all of its numerous disciplinary concepts therein (Kiviniemi et al., 2005; Zhang et al., 2015). Complex IM approaches must therefore be defined with IFC in mind due to its pertinence in fostering visions of integrated collaborative workflows. These integrated collaborative workflows will be enabled by system functionalities such as model merging and concurrent visualisation. (Adamu et al., 2015) which will themselves be built upon holistic data management approaches focused on evolving business needs.

Specific sub-themes should be addressed as part of future approaches such as the ownership of data in multi-user environments, integrity, availability, and data tracking among others (Emmitt and Gorse, 2007; Jørgensen et al., 2008). Information security management is also a key issue that must still be addressed for integrated cloud-based workflows (Redmond et al., 2012). Current IM initiatives also neglect to address how specific issues will overlap as the industry moves towards integrated workflows (BIM Task Group, 2015) that result in the requirement for managed, interoperable information-flows that also addresses security-concerns.

As an example, the current IDM and MVD initiatives delineate an approach to define and program an interoperable exchange at a particular business process stage (Wix and Karlshøj, 2010; Volk et al., 2014). The current standards are based upon a waterfall methodology which requires significant degree of time in defining and validating processes and exchanges (Kannengiesser and Roxin, 2016). Furthermore, the current interoperability standards do not appear to adequately address the project-specific people and process level considerations of effectively defining design-processes and programming their associated exchanges (Arayici et al., 2018; Berlo, 2019).

On the other hand, future consideration could be expanded via agile and project-specific approaches that address issues of inflexibility (Berlo, 2019) alongside security-specific concerns of ensuring appropriate data-access. Such concerns could be solved in tandem by identifying high-level exchanges required on a project and to then identify which specific practitioners will require exactly what information from exchanges. It would encapsulate reusability at its core as the loosely coupled modular processes could be utilised for usage for similar granular processes (Kannengiesser and Roxin, 2016; Berlo, 2019).

In conclusion, inclusive and holistic approaches to the secure management of information that incorporate multiple factors such as organisational managerial issues (Azhar 2011), alignment of information system infrastructure, interoperability and security needs (Soomro et al., 2016) are yet to be achieved (Mahamadu et al., 2013). These concerns will be exposed as the implications of security in an integrated cloud environment become better understood such as, what is an appropriate level of detail to share information amongst other parties in virtual environments (k, 2015). As more security issues become apparent, there is a real need therefore for data security to be simultaneously addressed in conjunction with collaborative workflows (Boyes, 2014) and as part of a security-minded approach to ensure safe industry development.

2.4 Security Context Within the AEC Industry

Within construction scenarios heavily invested in security, immaterial types of contextual information (Abowd et al., 1999) build up a picture, and contribute to the overall security climate of digital construction projects (Boyes, 2015). These range from aspects such as the security maturity of appointees and their supply-chains (Abedi et al., 2013) to broader national concerns over CNI tied to the physical and economic safety of society (Parn and Edwards, 2019). Standards such as NIST (National Institute of Standards and Technology, 2018) and ISO 19650-5 (BSI, 2020) detail security-risk assessment procedures to guide the determination of a project's security-climate, alongside security-minded approaches to implement in view of factors such as the sensitivity of assets to be built, maintained and interconnected as digital twins (Centre for Digital Built Britain, 2020).

Thus far, security focuses within AEC industrial and research spheres are limited which include naïve initiatives centred upon cyber and network security (Das et al., 2021) as opposed to a holistic view of security-relevant project factors (BSI, 2020). This includes those arising from the organisational, personnel, process, cyber / cyber-physical and information dimensions of AEC projects (BSI, 2020), and types of security-risks specific to Construction 4.0, including safety, utility and resilience (Boyes, 2015). The implications of this limited focus are broader still, with the AEC sector being ill-equipped to act as the first line of defence for a digitally secure built environment for both CNI and the rest of the industry (García de Soto et al., 2020).

Projects should also account for contractually enforceable requirements that certain information only be exchanged with certain other actors within and across appointment-chains during specific project-phases (Eadie et al., 2015). This is reflective of information requirement planning (Bolpagni and Hooper, 2021) and information governance (Alreshidi et al., 2017) within security-minded scenarios requiring precise selectivity in respect to who should receive information and to what level (Mahamadu et al., 2013; Ghadiminia et al., 2021). This has been noted as difficult to achieve in practice however, especially from the perspective of both knowing of, and governing identified security-risks (Parn and Edwards, 2019).

Principles of 'selectivity' and 'least privilege' mitigate numerous types of security-risks present throughout the project lifecycle including unauthorised dissemination of confidential or sensitive design information from CDEs which presents higher risk either on its own, in aggregation with other sensitive or potentially innocuous datasets (Boyes, 2014; CPNI, 2020). This can result in any number of adverse security-risk scenarios such as exposure of critical building systems information thereby compromising security and safety (Boyes, 2013). As such, the intended form and function of an asset's cyber-physicality during operations should be protected from project inception (CPNI, 2020). This is crucial given drivers to deliver digital-twins (Bolton et al., 2018) which in turn represents the potential for threat-actors to exploit increased cyber-physical interconnectivity, such as structural-systems and counterweights that respond to real-world feedback via sensors (García de Soto et al., 2020) in IoT based systems (Alshammari et al., 2021).

Security focuses for both CNI and for the broader built-environment are however focused upon the management of risks at the point of operations and maintenance of an asset (García de Soto et al., 2020). For example, the National Institute of Standards and Technology's cybersecurity framework (National Institute of Standards and Technology, 2018) focuses upon assessment and management of CNI security-risks during asset-operations but does not readily consider the chain of cascading security-risk implications present from activities during the design and construction phases, such as exposure during bidding activities (García de Soto et al., 2020).

In response to such risks, there is a need for rigorous management of security-risk and preliminary academic initiatives are working towards a holistic appreciation of security-risk management for all stages of the asset-lifecycle (BIM+, 2021; Mantha et al., 2021a). This is alongside the overlaps between CNI in both understanding the cross-relevancy of the types of risks to a broader range of built-assets, and where lessons may be learnt from CNI practices to be applied to guide security for the AEC industry (Pärn and Soto, 2020).

A further feature that is not present in the literature however is the overlap between such ideal holistic security-risk management approaches and the operational, efficiency and collaborative motives of digital optimisation for AECO operations. This includes cross-association of risks to certain physical and digital resources, such as information which may enable or widen threat avenues and therefore to deliver it on a 'need to know' basis (Jonas, 2007; Cabinet Office, 2018). In practice however, information governance requires a broader understanding of stakeholder's information-needs (Jonas, 2007; Demian et al., 2019). The application of the 'need to know' principle may be hampered if decisions on permissions do not capture an atomic understanding of precisely what information a party requires to effectively carry out their work (Jonas, 2007; Ghadiminia et al., 2021).

The potential outcome being that participants do not gain information relevant for their project tasks and their ability to provide value is lessened (Azhar, 2011). Furthermore, current appreciation of the principle within CNI contexts such as nuclear and rail are opposed to an ideal scenario where 'needs' are clearly tied to professional's work requirements and thereby what information practitioners actually require to produce value (Ghadiminia et al., 2021). The ideal scenario should simultaneously mitigate risks by accessing whether the information required, sensitive or otherwise presents risks either on its own or in aggregation with other information (Boyes, 2014). Understanding exactly what combination of information poses risks would allow governing roles to be both better aware of the risks and mitigate them by assigning the correct security-cleared practitioners to tasks requiring the information. It would also not allow needless sharing of potentially high-risk information (Boyes, 2014).

There is therefore still an issue in understanding to a high-level of accuracy and considering potential risks, a given practitioners information requirements as part of information governance procedure to decide 'Who should have access to what information?' (Best, 2011; Mahamadu et al., 2013; Ghadiminia et al., 2021). Information governance focuses upon both the decision-making process to decide a practitioners 'need' or 'requirement' for information throughout different project phases (Bolpagni and Hooper, 2021) and the technologies implementing these decisions in the form of permissions to data (Mahamadu et al., 2013). In this sense it is the underlying thinking and linchpin underpinning IM in practice (Alreshidi et al., 2014, 2017).

Current information planning and governance approaches appear static in that governing roles such as BIM information-managers define information requirements, and by extension levels of access (Alreshidi et al., 2017) which is not representative of dynamic AEC processes. This is where stakeholders' information-requirements (Bolpagni and Hooper, 2021), and by extension, degrees of data-access required (Beresnevichiene, 2003) change according to evolving stakeholder information-needs (Mahamadu et al., 2013; Soomro et al., 2016). Current governance mechanisms do not however facilitate the evolving identification, communication and overall management and verification of changing information needs of various stakeholders at atomic levels (Alreshidi et al., 2014; Beach, 2019). A more representative approach that could meet this characteristic of changing information requirements within the AEC workflow would be to enable information governance decisions to be made iteratively by governing roles as the project progresses to ensure dynamic security (Boyes, 2014).

Academic approaches attempting to address security concerns include the development of a guidance framework to guide security-minded measures for sensitive projects (Miceli Junior et al., 2020). Whilst it considers high-level public governance factors such as external accountability in a sensitive project, the overall purpose of security guidance is provided by the ISO 19650-5 (BSI, 2020). Currently, therefore, the only related BIM data governance framework (Beach et al., 2015) and (Alreshidi et al., 2017) propose models to capture the structure of a BIM model against within a cloud-based platform and embeds access-rights such that users can access different views of BIM data. In addition to not being truly dynamic, it captures the process dimension of AEC projects but only partially via the relation of different versions of BIM data with project stages (Alreshidi et al., 2017). The approach does not thereby capture the level of atomicity whereby governing roles can govern access based against practitioner's specific tasks throughout the workflow.

Additionally, the model itself and the mechanisms work upon the presumption that information-managers already possess knowledge for what access rights will be for each role, throughout the entire workflow. However, more likely than not, this tacit knowledge possessed by governing roles such as project and information managers over their team-level actors (professionals and teams as a whole) evolve as project-specific requirements become clearer (Boyes, 2014; Beach, 2019). The limitations of the governance model approach that it does actively provide the mechanisms to fully facilitate this governance process.

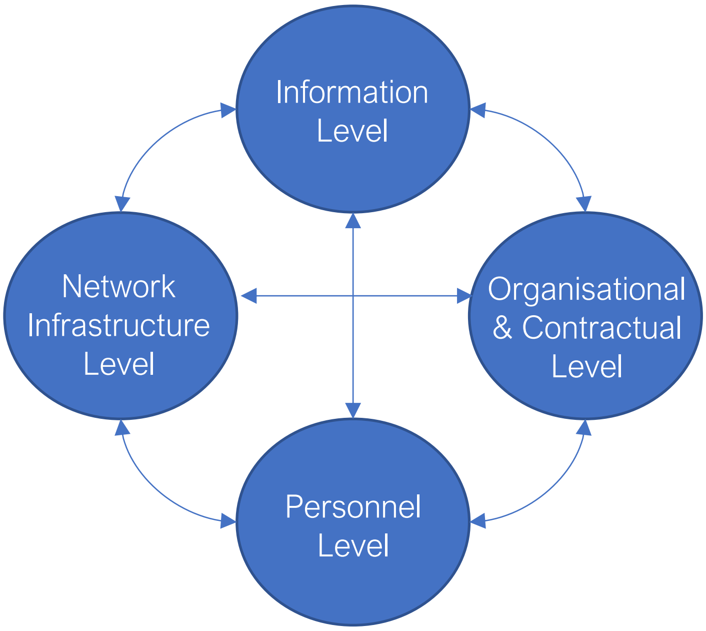

Information Level
Network Infrastructure Level
Organisational & Contractual Level
Personnel Level

Figure 2.1: Interacting Levels of BIM Security - Adapted from Mahamadu, Mahdjoubi and Booth, 2013

A more embedded approach could therefore capture the dynamism of projects in order to be contextually 'aware' (Abowd et al., 1999) of atomic and evolving information-needs. This is part of the proposed approach for information be delivered by the appropriate sharing party on a true need to know basis and at an appropriate level of detail and information (LOI & LOD) to facilitate effective yet secure collaboration (Mahamadu et al., 2013). Such an approach may also solve issues of current security approaches are argued as not being holistic enough (Redmond et al., 2012, Mahamadu et al., 2013). This is as opposed to incorporating multiple dimensions of security as depicted in **Figure 2.1.**

Current technological approaches focus upon infrastructure level security mechanisms such as access mechanisms available in proprietary collaboration platforms (Das et al., 2015) but to varying degrees of efficacy and operating at various levels in relation to file and folder level permissions (Singh et al., 2011, Shafiq et al., 2013). For example, few systems operate at a property level of access of BIM data structures (Alreshidi et al., 2017). The research will therefore aim to further explore how process and information governance mechanisms can enable fine-grained controls such as partitioning and at a property level, which should also be found at the information level of security to meet the need for placing detailed boundaries on information. The governance mechanisms should also incorporate the intelligence from organisational and personnel dimensions of complex and interacting organisational, managerial, and contractual themes that determine the information-management and security approach required for any given project context (Boyes, 2014; Mantha et al., 2021a).

2.5 State of the Art - Collaborative BIM Information Systems

Development of secure cloud-based systems for industrial practice is relatively recent (BIM Task Group, 2015; Das et al., 2021) and research is steadily delineating their applications for specific purposes (Wong et al., 2014). Examples include proposed co-creation with situational awareness (Adamu et al., 2015), multi-disciplinary design (Chen and Hou, 2014), life-cycle data management (Jiao et al., 2013), disaster emergency simulations (Mirahadi et al., 2019) and so on. These cloud-based initiatives are steadily growing but it has been noted that implementation based upon real-life usage is still a developing area for facilitating the full digital lifecycle for construction 4.0 (Wong et al., 2014; Sawhney et al., 2020).

Earlier technologies applied to solve collaboration issues include ImSvr and SABLE. SABLE posited an innovative idea for information exchange based around a middle-man approach (Jørgensen et al., 2008) addressing issues of multi-organisational exchange. However, it saw little uptake and the difficulties present in sharing building information models for the purpose of facilitating collaborative workflows still exist (Beetz et al., 2010).

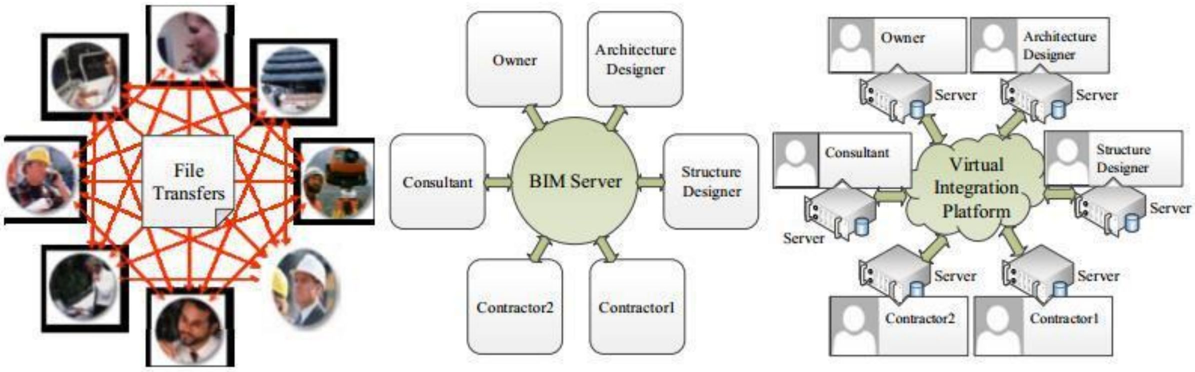


Figure 2.2: File-Based Mode (Left) vs Centralised Mode (Middle) vs Decentralised Mode (Right) - Zhang et al., 2014

Notable proprietary and non-proprietary cloud-based technologies such as BIMserver (Beetz et al., 2010), SocialBIM (Das et al., 2015), BIM 360, 3Drepo and many others feature a wide range of Model Collaboration System (MCS) functionalities for managing BIM models within CDEs (Shafiq et al., 2013; Chong et al., 2014; Meng et al., 2020). These functionalities such as federation and clash-checking work via intricate management, sharing and reuse of BIM data within multi-stakeholder cloud-based environments (Shafiq et al., 2013; Pradeep et al., 2021) to address collaborative workflow issues.

These technologies feature different modes of IS as seen within **Figure 2.2**. where the latter two modes aim to enable integrated visions. Centralised sharing (central of **Figure 2.2)** is far more efficient than file-based transfers but potentially lack assurances of data privacy, redundancy and retainment of IP that a logically connected, but physically decentralised and privatised networks **(Figure 2.2)** can aim to achieve (Zhang et al., 2014) in supporting the multi-contributor nature of construction projects.

Previous reviews of such systems have revealed a trend of solutions not inclusively addressing all features to meet collaborative needs in industry (Shafiq et al., 2013). Reasons for this include research-based projects such as BIMServer lacking in functionality (Zhang et al., 2014; Chong et al., 2014). Moreover, proprietary solutions may not accommodate the diversity present for industry needs (Chong et al., 2014) such as being a poor fit for usage with SME's and the difficulties present in operational implementation (Ahmed and Abuelmaatti, 2018). This also relates to the business models of vendors, wherein tailored implementations require significant package customisation for additional features (Pradeep et al., 2021), thereby increasing costs from baseline offerings.

In addition, another requirement for MSCs is to manage data at an atomic level in a dynamic manner (Cruz et al., 2009; Autodesk, 2014; Das et al., 2021). However, many are lacking in capabilities to intricately manage IFC data at a high level of granularity based around different requirements (Rezgui and Cooper, 2002; Wilkinson, 2014; Singh et al., 2011; Shafiq et al., 2013). As an example, Rezgui and Cooper's IFC information management approach operated at an 'object-level' of individual entities of a BIM model (Rezgui and Cooper, 2002) However, it did not explicitly address the intricacies of managing data at a property level within a shared virtual environment such as allowing multiple parties to concurrently edit information at this level (Singh et al., 2011). Bentley and other vendors have also been criticised for inadequate and shallow IFC merging procedures focused on the geometric federation as opposed to a comprehensive semantic map of an originators intention at a property level (Shafiq et al., 2013). This is alongside limitations in efficiently satisfying exchange requirements from a growing number of domains, an issue co-joined to the outdated nature of IFC based data-exchange strategies (Shelden et al., 2020).

Further to this, previous research has posited that development and implementation contexts must also cater to the 'softer issues' of collaboration to be effective (Singh et al., 2011). Recent commercial and research-based openBIM projects have not explicitly addressed how they could incorporate well-established social and collaborative work-theories (Steiner 1972) within their development and implementation approaches to deliver optimum collaborative workflows (Leicht et al., 2009; Jallow et al., 2010; Adamu et al., 2015). For example, extrapolating social-work theories initially defined by Steiner based around principals of divisible and non-divisible tasks to the context of AEC workflows would enable more in-depth understanding of the collaborative nature of task-work unique to project-specific contexts (Zomer et al., 2020). Others such as knot working (Kerosuo, 2015) could be more readily used to guide technological development of collaborative systems.

Conversely, social and behavioural science influenced research is recently increasing (Wong et al., 2014) which includes the application of activity theory to guide co-joined BIM project and technological adoption on a deeper level (Zomer et al., 2020). Social science influenced projects include a co-creation project with shared situation awareness based on an in-depth analysis of how project participants work (Adamu et al., 2015). There is currently however little research into developing secure cloud-based collaborative functionalities, as well as limited development on data-security specific functionality such as data-locking, auditing, versioning and tracking mechanisms (Shafiq et al., 2012, 2013). In turn, data-security concerns for cloud systems are increasing, where factors such as replication of data across multiple physical sites present unsolved concerns (Mahamadu et al., 2013; McGraw Hill Construction, 2014). It cannot currently be seen from the outlook of present system approaches that they can match the diverse and growing security requirements within industry (Volk et al, 2014; Wong et al., 2014).

Projects such as Social BIM cloud, 'Clouds for Co-ordination' (C4C) and the development of a BIM data governance models (Alreshidi et al., 2017) have however proposed they addressed security and governance issues. Their security focus is at the cloud-based network infrastructure level but also address security at a user-level through access control lists based around user groups which can access specific groupings of documents/objects relevant to them (Petri et al., 2015; Das et al., 2015). Such initiatives which focus upon providing the mechanisms to ensure confidentiality, integrity and assurance of data (Ghadiminia et al., 2021) do not however fully consider the information governance perspective in determining the 'knowledge' to ensure users should be given secure views of information. This should also be based at a property level which is a pre-requisite for specialised views of information to ensure that specific sensitive attributes are not disclosed (Boyes, 2013).

Moreover, such lack coverage of security and governance mechanism to address aggregation of security-risk arising via accumulation or cross-association of information of which there has been no work posited as of yet to solve this issue. At a database level, SocialBIMClouds distributed NoSQL database table approach could potentially allow for information to be gained by association. This is due to an object being linked by its GUID across the database tables, each capturing different aspects of the object e.g. table for material data. This could be exploited by malicious parties by cross-referencing tables with the relevant GUID to gain information on an object.

C4C, on the other hand, does not consider how data in its partial project phase silos (Adamu et al., 2015) can be effectively secured so that it is ensured that the multiple organisations utilising concurrent work will be doubly unaware of each other's processes if necessary. In addition, its decentralised nature may address ownership on the level that participants are able to keep track of their own information (Petri et al., 2015; Das et al., 2015). However, it does not accommodate for scenario's where for example, the client or governing body should be the custodian of all information (Cabinet Office, 2014; Winfield and Rock, 2018) or that custodianship but not ownership should be delegated such that other disciplines are able to edit information they may not necessarily have created and tracking indirect utilisation thereafter.

In addition, C4Cs approach does not explicitly account for the need for extensible sub-tasks dependent on the project (Adamu et al., 2015). Rather, it abstracts general stages outlined in the BS1192, therefore, the intricacies for secure data management at this granular task level are not explicitly addressed. In addition, their approach does not account for how information should be governed throughout the workflow at a granular task-level and how task-related authorisations should be explicitly defined at this level (Beresnevichiene, 2003). Similarly, the governance mechanisms to fully embed governing roles within the system to be made aware of changing requirements proposed by practitioners and to thereby react to such changing requirements as necessary are not present.

2.6 Research Background Summary and Discussion

In summary, a number of gaps were discussed for the overall approach in which secure collaboration is envisaged to be realised. One gap identified as mentioned previously, is that very few technological innovations have addressed socio-technical aspects as part of their approach to providing secure collaboration. In terms of being based around social and collaborative work theories, Co-Creation cloud by Adamu et al (2015) is the only collaboration system that take this into in-depth account for the development of their artefact. This demonstrates a large gap in how collaborative systems may be further optimised if this dimension is explicitly explored and incorporated.

Another core gap found from these systems is in relation to their governance and security approaches where a number of improvements appear needed in light of these secure data-management requirements, and the business rules that define these requirements still becoming better understood. It has been identified that as these requirements are becoming better understood, a number of potential different approaches for secure and optimised process and data governance will become apparent. C4C's data governance structure for example explicitly limited that only a given discipline would be able to edit work created in that same discipline. Whilst this can be justified as a potential approach to data integrity, whether this would work in practice where other disciplines may require temporary 'ownership' and therefore usage of the data as they see necessary has yet to be seen. In this sense, more questions must still be asked in relation to the data management approaches for a secure collaborative system.

In addition, whilst governance and secure IM has been proposed within the state-of-the-art systems, it appears to be static in that the approaches utilised do not account for how governing roles such as information-manager are provided a platform to continuously assess information requirements necessary for practitioners. In this sense, this capability would be explicitly tied to a system that delivers this feature but is more broadly representative that certain roles themselves should be more embedded as part of processes to govern information-requirements, information access and sharing. In addition, it may be necessary for other parties such as the practitioners themselves to communicate their requirements for information. How these mechanisms would be required to work and what rules would themselves govern the development of these mechanisms must still be uncovered.

Finally, the core gap that was identified from the literature search was the disjointedness of secure-collaboration research within the knowledgebase. Much of the security-research is focused upon a technological narrative of the security features that proof-of-concepts technologies provide for. There is however limited literature which explores the necessity for improved security-risk governance within the AEC sphere, and the overlaps with CNI. Rather, there is a significant lack of focus towards this aim within the academic sphere. Furthermore, there are very few academic sources that have explored the relatively recent overlap between collaboration and security-motives and tensions that may arise. As part of primary research therefore, it will be attempted to be identified what are the necessary industry-led requirements for a holistic approach for an artefact that provides a route towards secure-collaboration. In addition, the research will attempt to identify areas where the researcher may not have initially considered as it is undoubtedly the case that as requirements become clearer, new requirements representative of issues will also be uncovered.

3 Research Methodology

3.1 Methodology

Design Science was chosen due to its suitability to a project that is both theoretical and progressive where the final aim is a framework to be based and evaluated upon problems uncovered within real-life contexts (Hevner et al., 2004; Baskerville et al., 2018). Its choice was influenced by the research-onion (Saunders et al., 2019), which guided philosophical considerations based upon initial findings of the problem-environment, where problems are deeply interrelated, and where solutions must be based in view of enveloping positive change. In other words, the resolution of problems requires a *pragmatic* approach (Saunders et al., 2019). which deeply analyses the overlaps of problems and prescribes solutions that are designed to closely fit both security and collaboration needs in the sector.

Correspondingly, BIM research aligns to the development of technological artefact / frameworks that detail routes to solving existing problems (Kehily and Underwood, 2015). Traditional research methodologies for natural and behavioural sciences (Hevner et al., 2004) however aim to describe a problem in its current form, and utilise deductive and inductive approaches, where a deductive approach prescribes the testing of a theory and an inductive approach details the creation of a theory (March and Smith, 1995). Whilst these research approaches are suitable for the social sciences, they are ill-matched for research that requires change (Hevner et al., 2004), and the nature of this research which prescribes progression of the AEC industry (Kehily and Underwood, 2015). The Design science research methodology however aims to both (a) detail the gaps within a current problem and then (b) suggests solutions based on these gaps, which are developed and can then be evaluated (Kehily and Underwood, 2015) as part of an abductive approach (Saunders et al., 2019). Design science is thereby practical in combining traditional behavioural sciences with a progressive approach whereby research in defining a problem, feeds into the development of artefacts applied to solve the problem (Hevner et al., 2004).

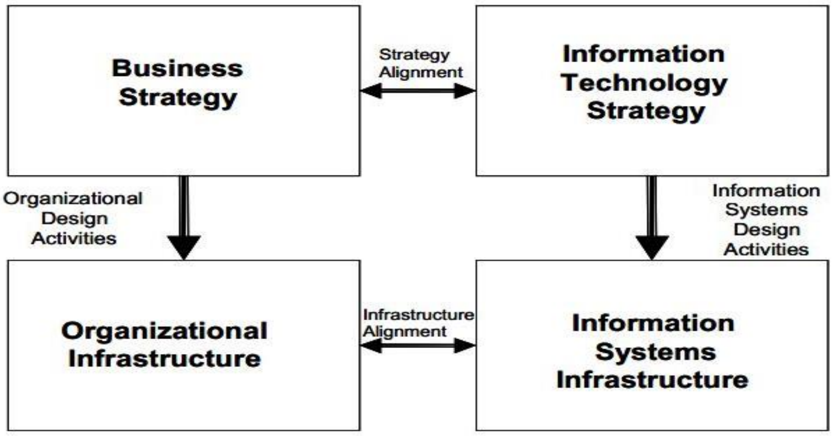

Business Strategy
Strategy Alignment
Information Technology Strategy
Organizational Design Activities
Information Systems Design Activities
Organizational Infrastructure
Infrastructure Alignment
Information Systems Infrastructure

Figure 3.1: Synthesised Infrastructures - Hevner et al., 2004

Likewise, it is depicted in **Figure 3.1** that the development of information systems cannot be separated from the social and organisational background within which it is designed for. Moreover, the creation of a synchronised organisational and information infrastructure requires interplay between the design and businesses and system strategies. An information systems infrastructure will thus be in the optimal position to support the organisational infrastructure when this synthesised design approach is present (Henderson and Venkatraman, 1993).

This interplay is especially crucial for BIM centric technical development which research has outlined lacks this necessary interplay (Kehily and Underwood, 2015) that design science aims to address (Hevner et al., 2004). This interplay is critical due to the complex contextual background of the industry that must be thoroughly incorporated for an artefact to enable security based upon industry and organisational needs (Orlikowski and Barley, 2001). This is thus a socio technological approach to solving a problem in an innovative fashion (Baskerville et al., 2009) through the incorporation of technology, business and industry culture.

3.2 Research Approach

The problem of holistic secure-collaboration is ill-structured and is an emerging question both within academia and industry (Soomro et al., 2016). There is little in the form of a common knowledge representation for holistic security-minded approaches in practice (Mantha et al., 2021b). Accordingly, the development of new artefacts will require central influence of primary research from both academic and industry sources who will likely possess varying views on how to best address issues of secure collaboration. It is therefore necessary to synthesise this information through the researcher's own interpretation to understand the underlying 'truth and reality' of analyses (Panas and Pantouvakis, 2010). Design Science is well suited as an approach for the fusion of this academic and industrial knowledge as seen in **Figure 3.2.**

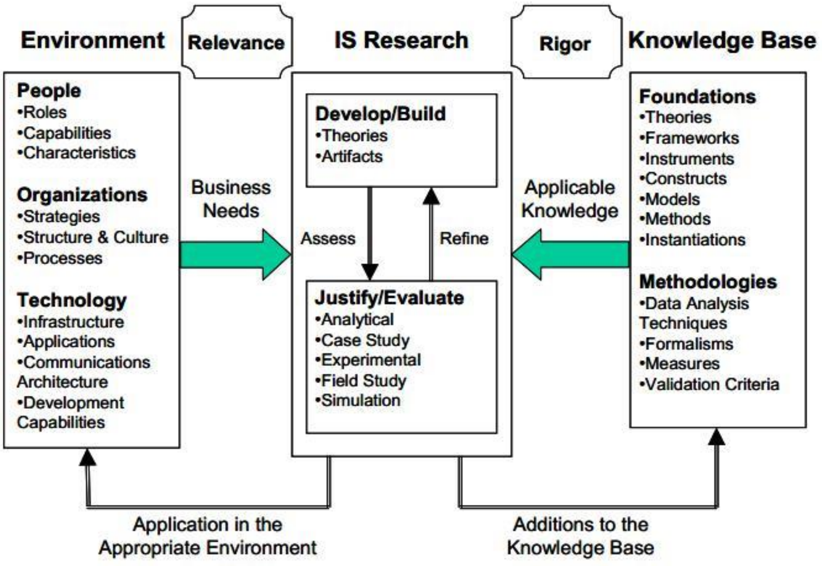


Figure 3.2: Design Science Research Integration of Knowledge-Base and Environment - Hevner et al., 2004

The generalised process of design science research as depicted in **Figure 3.2** starts by cementing the relevance of the research by ensuring there is a real and unsolved problem. A business need must therefore be present (Hevner et al., 2004). For this research, the 'business' need is characterised within the context of AEC projects and their stakeholders. Second to this, a 'search pattern' (Simon, 1996) is undertaken whereby the researcher investigates the problem within a given problem-environment. This requires an 'awareness of the problem' to understand where a gap exists between the current and desired business state that can be incrementally closed (Hevner et al., 2004). This is via the *design* of artefacts which propose a solution to the problem identified via a rigorous synthesis of the knowledgebase and industry expertise. Research rigour must be applied for both the problem-search and the development and assessment of proposed artefacts. This leads to the following stage as the application of the artefact relative to the problem-environment, and in reaching conclusions as to whether it can effectively solve issues identified (Jones and Gregor, 2007). Finally, the contribution of the artefact to the problem field and academic research should be met and conveyed effectively.

As depicted in **Figure 3.2**, IS research is the accumulation and interaction between the knowledgebase and problem-environment, where the problem-environment describes specific phenomena pertaining to the AEC industry such as their appointment-chains within security-minded settings, their disciplinary professionals (Simpson et al., 2019) and their current or planned technologies as variables towards secure digitisation (Silver et al., 1995). It also comprises the organisational dimension includes their existing work structures, strategies, culture, values, etc. around such secure settings (Boyes, 2014). Similarly, the people domain comprises their views and practices and their specific characteristics and roles. It may also include competencies of disciplinary professionals. Technologies in place will be judged against factors of the digital and organisational infrastructure, applications within such infrastructure, communications and secure exchange capabilities, system-architectures, and further development capabilities (Simon, 1996).

The stakeholder needs are also derived from the security and collaboration context of the aforementioned organisational and people issues, how they are related to technologies within the problem-environment and its processes, and future needs (Silver et al., 1995; Simon, 1996). The needs of any given organisation approached will comprise their own specific requirements that must be met within the context of their security-minded projects. The knowledgebase can however help to appreciate and thereby extract requirements to resolve the stakeholder's problem. This includes the application of relevant existing theories, frameworks, models, instruments and applications of methodologies such as data-analysis techniques to ensure research rigour (Hevner et al., 2004).

In the case of this research, an in-depth appreciation of governance practices, and standards will be necessary. This includes those found within domain-specific knowledge, such as guidance in the security categorisation of nuclear assets and security-plans (Office for Nuclear Regulation, 2017). This synthesis of the knowledge base and the problem domain will provide the foundation of a new secure collaboration artefact to solve the problems found in multiple contexts. The next section will discuss in more detail the consideration to design and evaluate.

3.2.1 Artefact Development and Evaluation Approach

Recent design science paradigms posit that instantiation of artefacts is optional (Peffers et al., 2018) and that conceptual artefacts are valid research outcomes (Jones and Gregor, 2007). The principles are embedded into the artefact as a 'blueprint' which is what enables effective reuse of the principles for future interventions across a broader spectrum of adopter's practices (Meth et al., 2015). The framework would serve as such a blueprint, and development methods will utilise relevant information-systems requirements capture as part of the research design approach (Cockburn, 2009); relevant social and security theories will also be incorporated into the development of the framework. The artefact itself may comprise conceptual diagrams of system views, functions, processes and data-schemas (Atan et al., 2012) etc.

Artefact evaluation requires consideration of variables including the type of artefact that is developed, it's focuses, the stage of its development life-cycle (Petter et al., 2010) and the context of the research project and problem-environment (Winter, 2008; Venable et al., 2016). For example, the evaluation of an implemented information-system may be positivist as its tangibility enables the capture of metrics to determine the efficacy of functionality (Venable et al., 2016). The evaluation of conceptual artefacts may be better contextualised in defining the 'nature' of the artefact that resolves issues faced in the project's approached (Jones and Gregor, 2007). In other words, deriving inferences, shared meanings and conclusions that the artefact is valid for different contexts, thereby driving future interventions in real practice (Venable et al., 2016).

Subgenres of design science are also fluid in their interpretation of a quality design and evaluation such as 'information systems design theory' (ISDT) and 'design science research methodology' (DSRM) (Peffers et al., 2018). The former promotes the development of design theory which prescribes the general solutions and understanding necessary to solve problems, whilst leaving open instantiation for those applying the theory (Jones and Gregor, 2007; Peffers et al., 2018). ISDT, DSRM and 'Patterns' (Petter et al., 2010) are also open to evaluative methods less formal in nature (Peffers et al., 2018). General evaluation methods include action research, logical arguments, expert-based evaluation, subject-based experiments and surveys (Peffers e al., 2012). It is noted these types of method appear suitable for conceptual artefacts prior to instantiation (Petter et al., 2010). This appears due to their suitability to evaluate concepts such that further findings can be analysed in-depth to guide deployment decisions in specific contexts.

Validation in this context should evaluate the problem-environment findings and the framework itself, including concepts and principles which must also be analysed in-depth as to their applicability and utility for improvement in the overlapping ecosystems of systems, people, and organisations (Venable et al., 2016) of multiple environments interviewed. An evaluation method must also be devised to capture and attribute shared meaning of the applicability, plausibility and feasibility off the artefact's design concepts and principles (Petter et al., 2010). This is as the framework will be critiqued based against different practices, and also whether the proposals would improve their common issues. Accordingly, a qualitative expert-based approach may be ideal to gather common meaning from the experts representing their practices in which the framework should be implemented as part of future work (Petter et al., 2010). The expert-based approach is also chosen and expanded upon in **Section 3.6** as a design choice for data-collection.

For this section, it is noted that such a qualitative approach is also relevant in gathering high-level feedback of the validity and applicability of the framework to different practices, where many types of functionalities will need to be verified simultaneously. In addition, a categorisation method for feedback and analysis is adopted based upon joint BIM industry and academic workshops (Simpson et al., 2019) where a matrix categorised the development of different BIM initiatives in view of their 'impact', 'urgency' and present 'maturity' against high-level attributes of 'high', 'medium' and 'low' levels'. The benefits of this method lie in the effective summarisation of findings of complex and overlapping initiatives, and in deriving shared meaning of the need for progressing future agenda for the initiatives individually, and as a whole. Another project applying a similar categorified evaluation also utilised design science to develop a framework which consisted of mapping the PAS 1192-5 security procedures (British Standards Institution, 2015) to three types of BIM project management. The evaluation featured fluid categorisation to derive understanding of the benefit of the guidance principles of the framework.

For both projects, codes or attributes were provided contextual meaning as part of assessing initiatives / guidance. Similarly, different types of codes could be applied for this research to categorise the correctness and appropriateness of principles in analysing and evaluating shared consensus amongst experts. It is noted however that the difference in context for the latter research project is that it does not prescribe a design theory for change in the environments it intends to influence. This framework will however represent the blueprint for positive change. Whilst a general method of categorisation can therefore be adopted based on the need to derive shared understanding and meaning amongst experts, there is also a need to link the feedback of concepts proposed and the issues they intend to resolve. A principle of Meth et al. (2015) is thereby adopted, by defining high-level relationships between the intended solution to the identified problems, to in-turn gauge and refine the effectiveness of the concepts in solving issues based upon feedback from subject-matter experts. To enable this principle, meaning attributed to categories should be based upon such an overall approach to categorise and later analyse findings in more depth. The chosen identifiers / code for categories include **'Verifications'**, **'Issues'** and **'Exceptions'**. These codes are provided additional context within **Chapter 6** for Validation. For this section, it is noted that these categories are useful in determining an overarching understanding whether the framework and its concepts are complete in its coverage of concepts to enable secure collaboration. This includes whether the framework is comprehensible, viable, flexible and reusable within the contexts of the intended environments (Petter et al., 2010), and overall, whether the design serves to meet the requirements that have been extracted of the domain, and whether experts meet a consensus on its need.

Discussion: Further mixed validation methods may convert the qualitative categorisations to numerical data, alongside the usage of surveys to gather general degrees of agreeability expressed by participants of the framework to further deepen insights into the quality of the artefact (Cleven et al., 2009). For the design-iterations covered by this project's scope, it is noted that whilst straightforward, the evaluation approach serves its purpose of evaluating findings that will validate and refine the applicability of the concepts in solving problems, whilst laying the groundwork for the framework instantiation. Finally, whilst outside scope, the tangibility of a prototype based upon the framework presents more options (Cleven et al., 2009) such as the evaluation in a field-experiment context within security-minded practices, and a as close to possible representation of a project to present viability before deployment. This may include the consideration of 'dummy sensitive data'. Criteria to evaluate the prototype may be based upon both objective and subjective measures of whether for example, functionalities such as sharing to be linked to access work appropriately, but also whether users believe they serve their intended benefit.

3.3 Research Guidelines

The table below shows the seven fundamental guidelines that design science researchers must utilise to understanding, executing and evaluating the research.

Table 3.1: Design Science Research Guidelines

Guideline	Response to Guideline
Guideline 1: Design as an Artefact	Developed artefacts will include a process and data governance framework which embeds the needs (i.e. requirements) for secure collaboration of BIM projects. It will also include framework concepts as high-level considerations of implementing the approach.
Guideline 2: Problem Relevance	The problem is to find and solve unexplored and unresolved issues and tensions that are posed for secure BIM collaboration at a process and information level.
Guideline 3: Design Evaluation	The research will be evaluated against experts within industry and industry methods in ensuring appropriateness and relevancy of the problem-environment and the framework in confirming / disproving the theories and proposals respectively.
Guideline 4: Research Contributions	The aim of this research is to provide solutions (via the process and data governance framework) to the complexities behind secure collaboration for teams involved in security-minded BIM projects.
Guideline 5: Research Rigour	This rigour of 'design as an artefact' and 'evaluation of design' should be met by applying the materials within the knowledgebase (secondary) / problem-environment (primary) to diagnose the issues with BIM and security experts and define the requirements of the solution. The problem-environment must be addressed holistically, considering all constituting factors to define and synchronously iterate and evaluate the artefact (via the qualitative expert-based feedback) to ensure that it provides a viable and useful solution to a (also verified) real and relevant problem.

Guideline 6: Design as a Research Process	The framework as a secure and collaborative approach will be developed around the problem-environment and will incorporate the needs of stakeholders to ensure it is relevant in its scope. Its design iterations will be achieved via the refinement of concepts from evaluation.
Guideline 7 Communication of Research	The intention is to publish in academic journals and international conferences. The communication of targeted audience will be researched by utilising journals in both computer science and built-environment research fields.

3.4 Research Interview Design

3.4.1 Semi-Structured Interview Design Approach

Via a semi-structured design, discussion should revolve around a number of key themes and issues which have been identified via the literature-search and have been deemed necessary to further explore via a critical literature-review process (Bashir et al., 2015). The themes to be discussed pertain to secure collaboration and are further expanded within the following sub-sections. As this is design-science research, these themes and issues were explored to potentially identify gaps and solutions within industry which may be in the form of recommendations or system architecture requirements (Hevner et al., 2004). A semi-structured interview design choice was deemed appropriate based upon the following benefits.

- They allow for flexible and detailed discussion with interviewees which is appropriate for research which is exploratory and concept building in nature (Bashir et al., 2015).
- They allow exploration of complex and inter-related topics in a manner that is difficult to replicate to the same degree via a written format (Navarrete, 2020).
- Interviewees can raise issues and themes they believe relevant to the topics presented, but which may not have initially been considered by the researcher (Wilson, 2014).
- They allow for the exploration of themes and issues of a sensitive nature that the interviewee may not be able to discuss via a written format (Oates 2006).

There are however drawbacks to semi-structured approaches such as the large volumes of research data generated, and longer analysis-cycles compared to structured interviews with standardised questions (Oates 2006; Wilson, 2014). These drawbacks are however negated by the potential to identify issues, gaps and solutions which can only be elicited through flexible yet detailed discussion of complex and inter-related topics to gather profound experiences

(Navarrete, 2020) of themes and issues which are relatively unexplored fields within academia (Mahamadu et al., 2013). A semi-structured interview design choice therefore appears to be the best choice for fluid interaction between issues, but also in capturing detailed insight into the problem environment (Hevner et al., 2004) The following subsections will expand on choices made of the interview design.

3.4.1.1 Introduction to Exploration of Interview Design Themes and Upper / Lower Tier Lenses

Within the literature review, the overarching themes of collaboration and security were upon reflection, the 'upper-tier' lenses on to which more specific issues and gaps were explored. I.e. each section of the literature review comprised sub-sections related to 'lower-tier' themes e.g. information-management which were the more specific 'lower-tier' themes, but which were still explored with the view to identify the overlap between collaboration and security (i.e. within the scope of the upper-tier lenses). Similarly, the interview design comprises lower-tier themes to be explored as part of the upper-tier sections. This is achieved via the following two-step approach.

1. **Upper-Tier Lenses**: Devising questions to be explored that correspond to themes of either:
    a. Exploration of collaboration practices.
    b. Exploration of security practices.
    c. Exploration of security and collaboration practices *overlap*.
    d. Exploration of BIM governance and management practices.
2. **Lower-Tier Lenses**: Questions devised as part of upper-tier lenses further correspond to themes from multiple overlapping project dimensions.
    a. Process dimension: BIM workflows and protocols*.*
    b. Technology dimension: BIM technologies and security access-models.
    c. Stakeholder dimension: Organisations and internal actors involved within the project.
    d. Socio-organisational dimension: Cultural and socio-technical issues faced.

The aforementioned upper-tier lenses are underpinned by the lower-tier lenses of themes. An example is depicted in the following **Figure 3.3**.

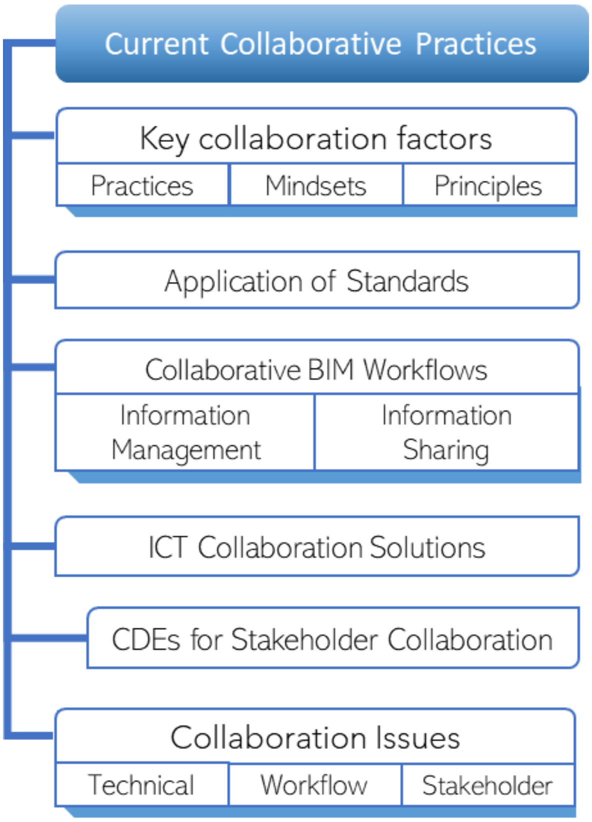

Current Collaborative Practices
Key collaboration factors
Practices
Mindsets
Principles
Application of Standards
Collaborative BIM Workflows
Information Management
Information Sharing
ICT Collaboration Solutions
CDEs for Stakeholder Collaboration
Collaboration Issues
Technical
Workflow
Stakeholder

Figure 3.3: Two-Tier Lens Approach and Individual Themes

Expanding upon **Figure 3.3**, the interview exploration of the upper-tier collaborative practices should include the discussion of the lower-tier themes of the appropriateness of CDEs to meet evolving information-management complexities of BIM processes (BIM Task Group, 2015). The lower-tier themes such as information-management were identified from gaps in the state-of-the-art for secure BIM collaboration.

Summary: This section has categorised the overarching approach whereby themes correspond to both an upper and lower lens. The following sections will further detail the design approach accordant to the upper lenses noted in this section.

3.4.1.2 Independent Exploration of Collaboration and Security Themes

As part of the interview design, the upper lenses of collaboration and security are explored independently where appropriate. This is based on literature-review findings that collaboration and security focuses face overlapping, yet distinct issues. For example, collaborative barriers are linked to technological information-exchange limitations (Redmond et al., 2012). Security-centric BIM focuses however face issues such as immature technical mechanisms for security (Afsari et al., 2016). Accordingly, specific themes were devised for individual sections to enable targeted exploration of specific issues. This 'Independent Exploration' approach is depicted in **Figure 3.4** which also extends the two-tier lens approach.

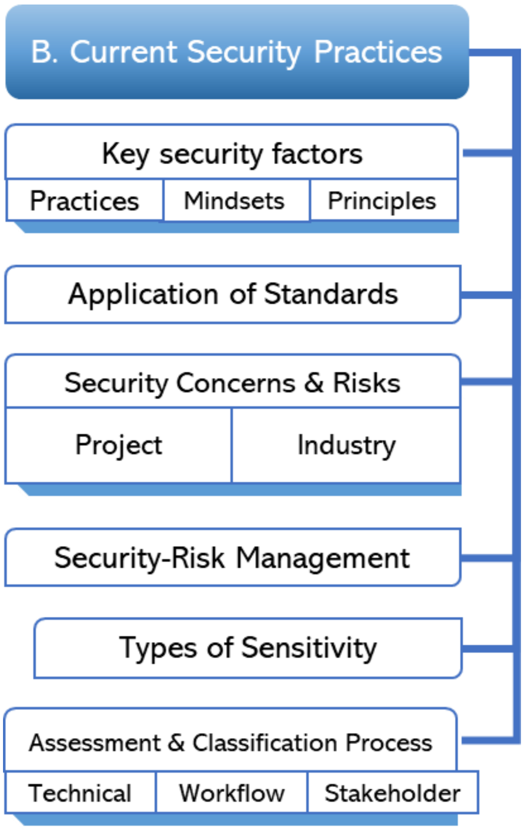
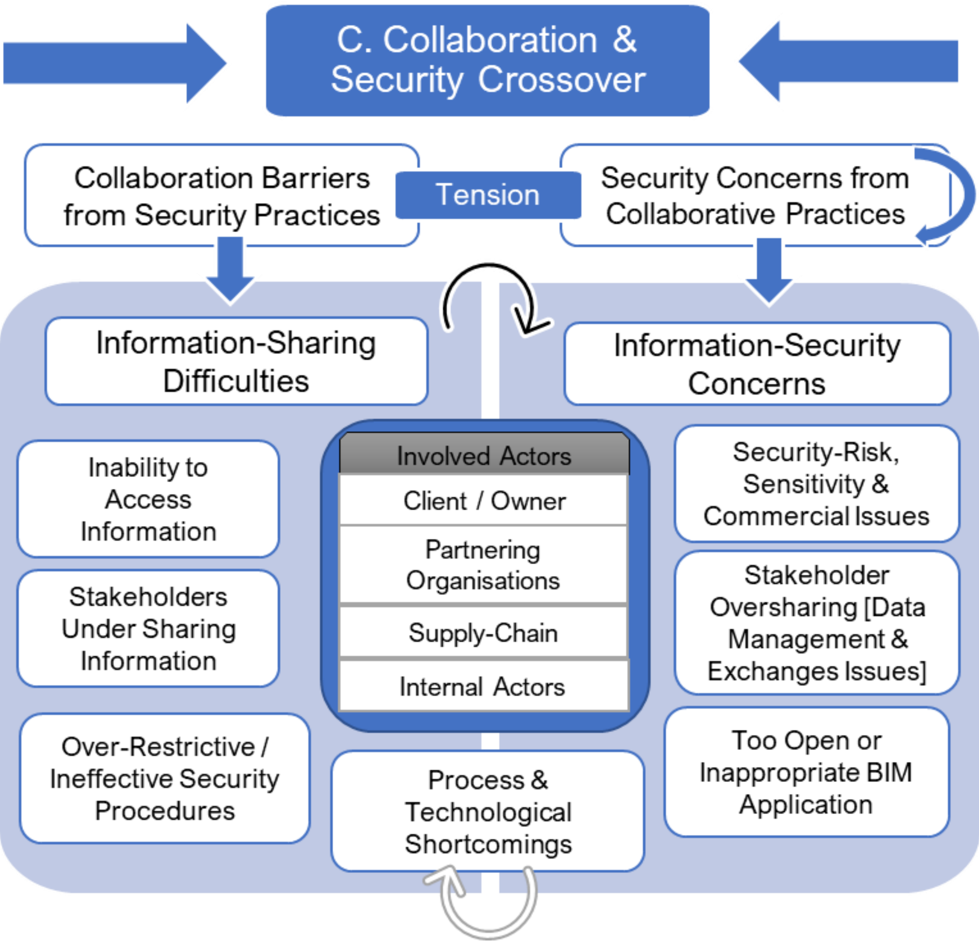


Figure 3.4: Individual Exploration (Security Example)

It is also noted **Figure 3.4** depicts the security-centric themes that were devised to be explored as part of the interview design. It is thereby the mirror to **Figure 3.3**. The following section also follows these two lenses approach but explores a section of the interview design which overlaps both upper lens of collaboration and security focuses.

3.4.1.3 Exploration of Overlapping Collaboration and Security Themes

The design also features a section of themes that overlap upper lens of collaboration and security. This pertains to a relatively unexplored theme of a potential tension between the contrasting motives of BIM collaboration and security (Office for Nuclear Regulation, 2014). This is depicted within **Figure 3.5.**



C. Collaboration & Security Crossover
Collaboration Barriers from Security Practices
Tension
Security Concerns from Collaborative Practices
Information-Sharing Difficulties
Information-Security Concerns
Inability to Access Information
Stakeholders Under Sharing Information
Over-Restrictive / Ineffective Security Procedures
Involved Actors
Client / Owner
Partnering Organisations
Supply-Chain
Internal Actors
Process & Technological Shortcomings
Security-Risk, Sensitivity & Commercial Issues
Stakeholder Oversharing [Data Management & Exchanges Issues]
Too Open or Inappropriate BIM Application

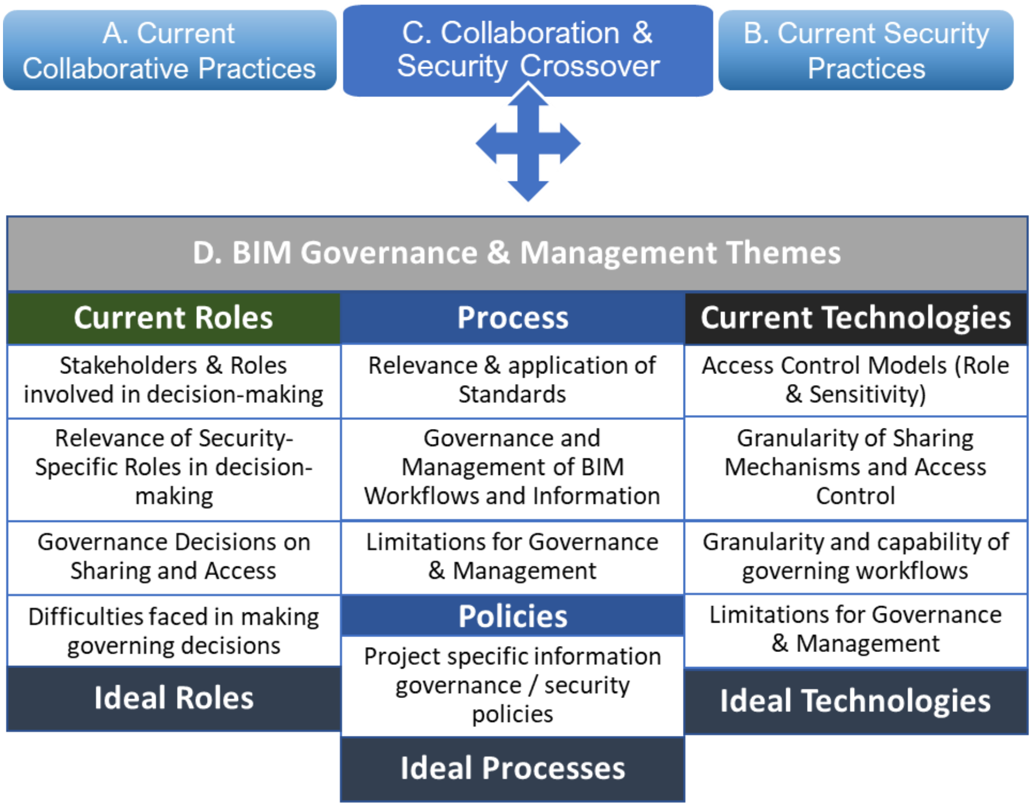
Figure 3.5: Security and Collaboration Themes Overlap

This tension is a central theme of the research design to explore how the overlapping motives of collaboration and security may pose as barriers to secure collaboration (Office for Nuclear Regulation, 2014). This is within the context of security-minded BIM projects and findings may also be relevant to the broader industry. Exploring the overlapping issues as part of the interview design also allows for free and detailed exploration of complex inter-related issues (Oates 2006). Key themes overlapping collaboration and security for this aspect of the interview design were

IM and IS, elevated security-risk, information / policies, and the need-to-know principles between internal and external stakeholders. The design takes such themes and will explore their overlap as hypothesised issues arising from the overlap of the themes when seen from the lens of attempting to be both secure and collaborative. For example, IS difficulties arising from overly strict application of security policies.

3.4.1.4 Exploration of BIM Governance and Management Themes

The upper-tier lens on to BIM governance and management is linked to norms and limitations of BIM information-governance and information-management. BIM information management and governance themes were explored as part of the literature-search (Alreshidi et al., 2017; Christian, 2020), and analysis led to a hypothesis that improved BIM governance over actors, processes, information and security-risk would alleviate tensions between collaborative and security approaches. The interview design reflects this hypothesis wherein the upper-tier lenses of collaborative practices, security practices and their overlap feed into this section. These aspects of the research design are depicted within **Figure 3.6.**



A. Current Collaborative Practices

C. Collaboration & Security Crossover

B. Current Security Practices

D. BIM Governance & Management Themes

Current Roles	Process	Current Technologies
Stakeholders & Roles involved in decision-making	Relevance & application of Standards	Access Control Models (Role & Sensitivity)
Relevance of Security-Specific Roles in decision-making	Governance and Management of BIM Workflows and Information	Granularity of Sharing Mechanisms and Access Control
Governance Decisions on Sharing and Access	Limitations for Governance & Management	Granularity and capability of governing workflows
Difficulties faced in making governing decisions	Policies	Limitations for Governance & Management
Ideal Roles	Project specific information governance / security policies	Ideal Technologies
	Ideal Processes	

Figure 3.6: BIM Governance and Management Themes

Expanding upon **Figure 3.6**, a central facet of the interview design is to uncover limitations of current BIM and information governance and management procedures adopted within projects and identify future requirements to enable secure collaboration. Questions focus on the governance and management underpinning current BIM workflows and the overlap between stakeholders, roles, technologies and project / information policies involved. A number of lower-tier themes of information-management and information-sharing are explored also, alongside factors that are relevant from the security perspective.

Summary: In summary, the semi-structured interview design is based upon themes and issues explored within the literature review, further tailored for pragmatic exploration of a complex and relatively uncovered problem environment. As such, a number of different design choices were necessary for the interview design to capture detailed, insightful, and meaningful knowledge of the problem environment.

3.4.2 Detailed Research Design Breakdown

This section will depict an overarching breakdown of the research design, in expanding upon **Figures 3.3** through **3.6** with an interrelated representation of the research design. This is having explored the individual components of the research design. Accordingly, **Figure 3.7** depicts the overlap between all aspects of the interview design, which is provided further context thereafter.

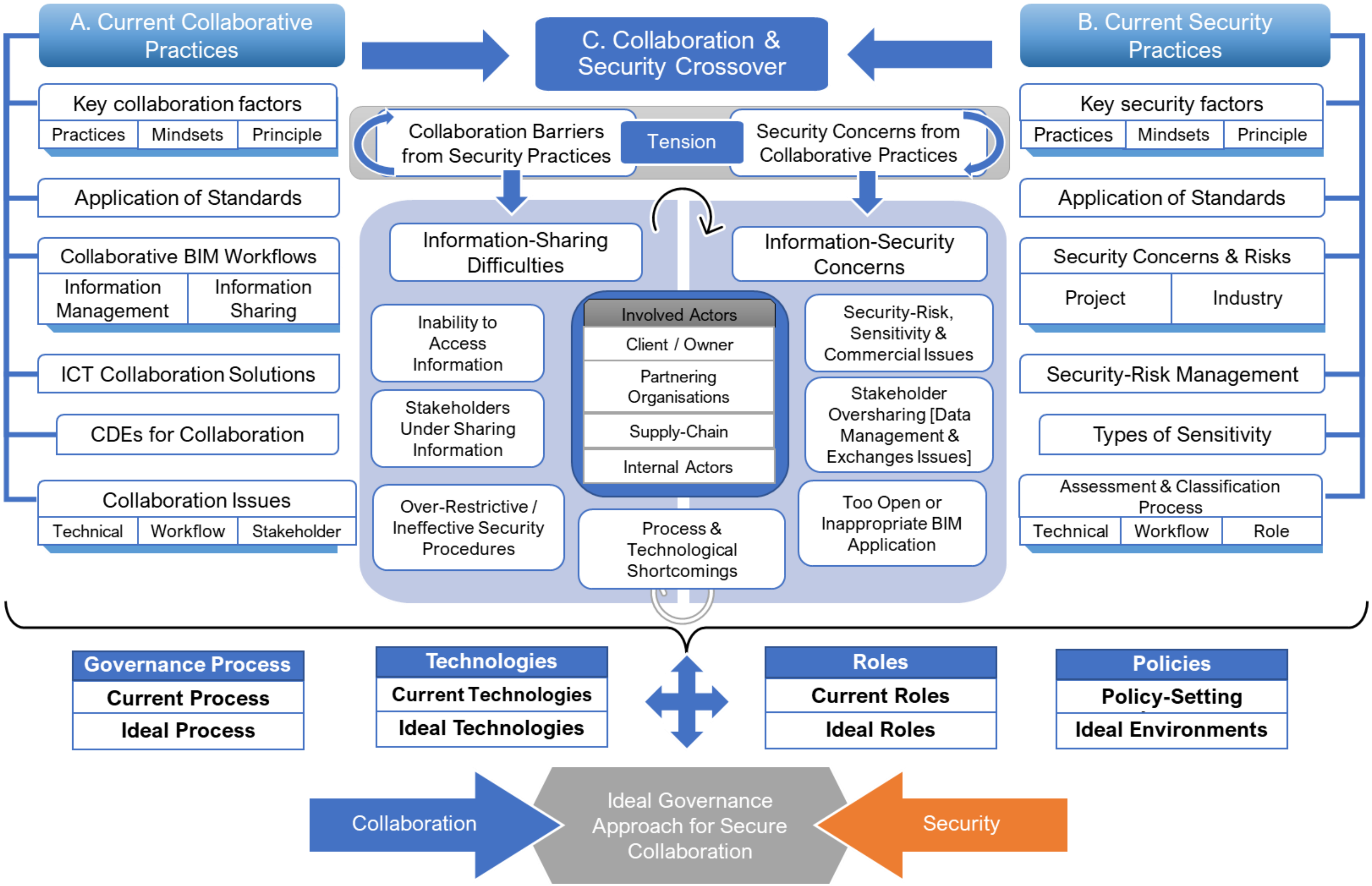

A. Current Collaborative Practices
Key collaboration factors
Practices
Mindsets
Principle
Application of Standards
Collaborative BIM Workflows
Information Management
Information Sharing
ICT Collaboration Solutions
CDEs for Collaboration
Collaboration Issues
Technical
Workflow
Stakeholder
C. Collaboration & Security Crossover
Collaboration Barriers from Security Practices
Tension
Security Concerns from Collaborative Practices
Information-Sharing Difficulties
Information-Security Concerns
Inability to Access Information
Stakeholders Under Sharing Information
Over-Restrictive / Ineffective Security Procedures
Involved Actors
Client / Owner
Partnering Organisations
Supply-Chain
Internal Actors
Process & Technological Shortcomings
Security-Risk, Sensitivity & Commercial Issues
Stakeholder Oversharing [Data Management & Exchanges Issues]
Too Open or Inappropriate BIM Application
B. Current Security Practices
Key security factors
Practices
Mindsets
Principle
Application of Standards
Security Concerns & Risks
Project
Industry
Security-Risk Management
Types of Sensitivity
Assessment & Classification Process
Technical
Workflow
Role
Governance Process
Current Process
Ideal Process
Technologies
Current Technologies
Ideal Technologies
Roles
Current Roles
Ideal Roles
Policies
Policy-Setting
Ideal Environments
Collaboration
Ideal Governance Approach for Secure Collaboration
Security

Figure 3.7: Research Interview Design

The aforementioned **Figure 3.7** depicts the overlap between the four section of the interview design. This being the individual/independent, overlapping and governance and management themes noted in **Sections 3.4.1.2, 3.4.1.3,** and **3.4.1.4** respectively.

In describing the interview design in view of all factors, the upper-lens of 'current collaborative practices' (column A) is the first section of the interview structure and the 'current security practices' (column B) is the second section. Both these upper-lens detail the lower-lens themes also depicted in **Figure 3.7** under their respective columns.

These themes, both at the upper and lower levels feed into the third section of the design as Section C: 'collaboration and security crossover'. As noted in **Section 3.4.1.3**, this section explores tensions arising between collaboration and security practices. The independent exploration is able to thereby feed into the overlapping perspective whenever necessary.

The final aspect of the design is to explore how tensions, and more broadly, collaboration and security barriers align to BIM governance and management limitations. This is also in exploring how overlapping issues, arising from process and technological shortcomings are barriers. Accordingly, section d also explores the ideal approaches in enabling secure collaboration. The high-level themes depicted within **Figure 3.7** are detailed in the following tables.

Independent Exploration of Collaboration Themes (Section A):

Table 3.2: Exploration of Current Collaborative Practices

Relevant Dimensions	Theme
Socio-Organisational and Stakeholders	Expert's view on key collaborative principles, values, and mindsets. • Whether, or what particular collaborative approaches may be applied to achieve collaborative working (Oraee et al., 2019).
Standards and Process	How standards such as the PAS 1192-2 are applied to support collaborative working (British Standards Institution, 2013).
Process, Technology and Stakeholders	How BIM is applied within workflows to support collaborative workflows. • How effectively BIM information is managed and shared with internal and external stakeholders throughout the project life cycle (Winfield and Rock, 2018). • How effectively BIM information-technology solutions support collaborative workflows via effective information-management and information-sharing (for both internal and external stakeholders) (Ford & Shana'a, 2020a, 2020b).
All	Expert's views on any other barriers and enablers in improving collaborative practices. • These comprise (a) stakeholder; (b) workflow; (c) technical; (d) cultural and behavioural perspectives. (Rezgui et al., 2005)

Independent Exploration of Security Themes (Section B):

Table 3.3: Exploration of Current Security Practices

Dimensions	Theme
Socio-Organisational and Stakeholders	Expert's views on key security-minded principles, values and mindsets. • How these are applied within project practices. • This included the principle of 'least privilege' /the 'need to know' (Cabinet Office, 2018).
Process	Application of standards (PAS 1192-5) to promote security and support security-risk management (British Standards Institution, 2015).
Process, Stakeholder and Technology	Significant security concerns and threats faced by experts' practices and the wider industry. • Concerns presented of technologies, digital workflows, and data-aggregation (Boyes, 2015).
Process and Stakeholder	Effectiveness of security-risk management approaches which include risk assessment and mitigation approaches (Boyes, 2015). • Assessing and classifying sensitive information and detailing mitigation of security-risk. What roles are involved of these processes.
Technology	CDE capability in securely managing sensitive BIM information. This included whether only those who 'need to know' about sensitive aspects are aware of them (Best, 2011).
All	Expert's views on any other barriers and requirements for security practices.

Exploration of Overlapping Collaboration and Security Themes (Section C):

Table 3.4: Collaboration and Security Overlap Themes

Dimensions	Theme
Socio-Organisational	Exploration of tensions between collaboration and security. This comprises contrasting principles of BIM openness, and security principles of 'least privilege' (British Standards Institution, 2015).
Process, Technology and Stakeholder	Overly rigorous security practices presenting difficulties in collaborating internally and externally. E.g. under-sharing information. • Tensions arising between security-measures and information-sharing (Eadie et al., 2015). • Influence of high security-risk / sensitivity on the effectiveness of information-sharing and information-management (Best, 2011).
Process, Technology and Stakeholder	Shortcomings in internal and external aspects of BIM collaborative practices adversely influencing security-risk (Redmond et al., 2012). • Significant security-risks arising through the application of ineffective BIM and digital workflows. • Concerns of oversharing information during exchanges and how to remediate these concerns.
Process and Technology	Shortcomings of technologies in facilitating collaborative and secure BIM information-flows (Afsari, Eastman, and Shelden, 2016).
All	Expert's beliefs on the key barriers and approaches necessary to enabling secure collaboration, within security-minded environments and the wider AEC industry.

Exploration of BIM Governance and Management Themes (Section D)

Table 3.5: BIM Governance and Management Themes

Dimensions	Theme
Process (Standards)	The application / applicability of standards in the governance and management of information. (British Standards Institution, 2015)
Process	BIM governance and management processes and their limitations; including limited precision and granularity of: • Information-management and sharing BIM processes. • Governance procedures and control over these processes.
Process (Policies)	Application of project-specific / organisational information-governance or information-management policies (Alreshidi et al., 2017).
Stakeholders (Roles)	Stakeholders and roles involved in governing, managing, and making decisions over information. • Governance decisions over what stakeholders need to know and share (C. B Sanders., 2014). • Security specific roles involved in decision-making (British Standards Institution, 2015). • The current and future responsibilities of such roles (Boyes 2014).
Technology	CDE capabilities and limitations in leveraging access-control based on: • Roles and sensitivity of information in question (Cabinet Office, 2018). • Precise access of BIM data within a model-file vs just file-level access (Afsari et al., 2016).

	• The context of professional's task work i.e., in addition to: (a) role-based-access-control and (b) high-level BIM project-stages (Adamu et al., 2015).
Process and Technology	Process and technology requirements for: • Limitations and requirements of BIM workflows and CDEs in enabling these ideas. • Precise and granular information-sharing / exchanges vs file-level information-sharing. • Enabling precise and granular governance of information-flows • Beliefs whether these would be beneficial for secure collaboration.

3.5 Sampling Approach

A sample of participants should fairly represent an entire population (Denscombe 2010; Bashir et al., 2015). In the context of this specific research however, the broader population of practitioners do not possess in-depth knowledge of the following factors.

- Security concerns and issues.
- Concerns and issues arising from the overlap between security and collaboration.

This lack of in-depth of knowledge within the broader population of practitioners led to the choice of non-probability purposive sampling which was appropriate to select participants most relevant to the problem domain (Bashir et al., 2015). Expert sampling in particular was adopted to strategically choose practitioners who possess expertise not held by the average BIM practitioner (Bashir et al., 2015).

As requirements for this research, experts must possess knowledge and expertise representative of the overlapping security and collaboration themes and issues that are applicable to security-conscious environments. Ideally, they should also possess knowledge of how such themes are applicable to the wider AEC industry to thereby capture the progression of recent industry AEC BIM security trends (CPNI, 2015) The core requirements for interviewee participants being that they held expert knowledge and / or expertise of:

1. Security-conscious environments and BIM projects.
2. Knowledge of both BIM and security specific concepts.
3. How collaborative and security focuses overlap within BIM projects.

Ideally participants were selected if their operations areas related to sectors that involved experience with critical national infrastructure (CNI). This is due to the knowledge gleaned from the literature search that projects handling CNI have dealt with the need to apply security-minded procedures longer than the broader AEC Industry (CPNI, 2015). On the other hand, some experts may have experience of security-conscious BIM projects pertaining to sensitive built-assets that fall outside of a CNI operation area or may simply possess expert knowledge of overlapping BIM and security topics. Such types of experts are also valid participants as they provide equally valid knowledge and are a more representative range of primary data sources (Denscombe 2010).

3.5.1 The Sample

Potential interviewees were identified from help from supervisors and individual identification of current experts within industry from exploration of whitepapers and journals. A total of 20 potential participants were invited to be interviewed, of which 13 took part and contributed specifically to the semi-structured interviews. Majority of the participants represented a specific organisation or BIM project. The breakdown of participants is categorised in **Section 3.5.2.** This includes participants invited to validate findings and the problem-environment which includes 3 new participants, bringing the total experts involved to 16. Expert-based sampling was utilised here also with additional criteria that participants are able to contrast current approaches, to the framework's concepts in validating utility, correctness / completeness and viability.

3.5.2 Expert Operations Area

Majority of the of interviewees held experiences of handling security-conscious BIM projects and thus held specialised knowledge for high-profile sectors; many of the interviewees were however also able to use their experiences within high-profile sectors to compare and contrast the current security and collaboration trends with the wider AEC industry. Some participants such as A6 and A11 however, acted as advisory roles to high-profile projects as they held expert knowledge of BIM and security. Additionally, many participants e.g. A1, A6, A7, A9, A10 and A11 contributed to development of BIM standards for the wider industry to varying degrees.

The aforementioned factors resulted in richer discussions and provided insight to the industry-trends of high-profile sectors in comparison to the wider industry; this factor in turn is reflected within analysis and discussion. The involved participants and a generic breakdown of their experience is provided in the following **Table 3.6.**

Table 3.6: Expert Breakdown

ID	Involved Sector(s)	Position	Experience	Interview Method
A1	CNI	Security and BIM Strategy Developer	Involved in the development of a client organisation's digital BIM strategy on security-minded projects. Also involved with standards development.	Teleconference and in person
A2	CNI	BIM Project Manager	BIM project manager as part of clients internal BIM implementation team. Was involved in defining BIM implementation for project.	In person
A3	CNI	BIM Project Manager	BIM project manager and engineer within a CNI project. Was working on behalf of a lead-organisation and held experiences managing supply-chains.	Teleconference
A4	CNI	BIM and Information Security Professional	Information security professional within a client organisation. Handled governance and assurance	Teleconference

			activities internally and externally.	
A5	Built-Environment and Defence	BIM Project Manager	BIM project manager of multi-national lead-organisation handling security-minded projects. Involved with the organisation's internal security strategy.	Teleconference
A6	Built-Environment	BIM and Security Consultant	A BIM and security specialist with extensive experience in guiding clients and developing standards around a range of AEC areas.	Teleconference
A7	CNI	BIM Project Manager	BIM project manager with extensive experience in defining and managing a client organisations BIM and security requirements. Also involved with standards development.	Teleconference
A8	Built-Environment and CNI	BIM and ICT Engineer	An ICT engineer and information security specialist within a large lead-organisation with BIM	Teleconference

			experience. Is acting as BIM and security consultant for a CNI project.	
A9	Built-Environment and Defence	BIM and Security Professional	BIM professional with extensive experience of security-minded projects and collaboration. Also involved with standards development.	Teleconference and in person
A10	Built-Environment and Defence	BIM and Security Professional	BIM security consultant for a large lead-organisation. Also involved with standards development.	Teleconference
A11	Built-Environment and CNI	BIM and Security Consultant	A BIM and security specialist with extensive experience in guiding organisations and developing standards around a range of AEC areas.	Teleconference and in person
A12	Construction Software Developer	Developer	Representing a CDE vendor. Held technical knowledge and experience interfacing with users over BIM and security features.	Teleconference

A13	CNI	Engineer	An engineer involved within a security-minded project. Held practitioner experiences of dealing with security and collaboration tensions.	In person (Interviewed alongside A2)

A11 and A12 did not wish to be recorded; as such, interview transcriptions are not possible for these participants. However, numerous follow-up conversations were undertaken to question and clarify the discussed ideas and ensure a rigorous and correct data-capture. In addition, validation consisted of A1, A6, A8, A9, A11 alongside a further three experts who were approached due to need to broaden findings applicability and limited availability for initial experts. A further **Table 3.7** distinguishes experts involved in data-capture with those involved in validation. It therefore also comprises the initial experts who took part in the validation who are given a new code for validation. The code number reflects the order in which experts took part.

Table 3.7: Expert Breakdown (Validation)

ID	Involved Sector(s)	Position	Experience	Interview Method
B1	Built-Environment and Defence	BIM and Security Professional	A9 in Table 3.6.	1st Workshop (In-Person).
B2	CNI	Engineer	An engineer involved within a security-minded project. Held significant digital and knowledge management experience.	1st Workshop (In person).
B3	Built Environment	Engineer and Digital Specialist	Engineer having moved to a digital specialisation in exploring blockchain technologies. Held practitioner and intra-organisational competence in determining BIM and Security approaches.	2nd Workshop (In person).
B4	Built Environment	Digital Specialist	Digital and automation specialist involved in implementing solutions for BIM information-systems and	2nd Workshop (In person).

			other related technologies for AEC needs.	
B5	Built-Environment and CNI	BIM and Security Consultant	A11 in Table 3.6.	Interview (In person).
B6	CNI	Security and BIM Strategy Developer	A1 in Table 3.6.	Interview (Teleconference)
B7	Built-Environment	BIM and Security Consultant	A6 in Table 3.6.	Interview (Teleconference)
B8	Built-Environment and CNI	BIM and ICT Engineer	A8 in Table 3.6.	Interview (Teleconference)

3.6 Interview Analysis Approach

Thematic content analysis was considered suitable for capturing and making connections of ideas captured within interviews (Boyatzis, 1998). It also enables the researcher to identify and make associations amongst emerging patterns (Boyatzis, 1998; Bashir et al., 2015). Thematic content analysis was therefore chosen to identify recurrent themes and issues that could be indicative of issues or gaps to still be filled within industry. This was, of course, based against responses captured from interviewees in response to questions of the semi-structured interview design. The thematic content analysis approach based upon Boyatzis (1998) and utilised by Bashir et al. (2015) comprised a multi-step process of the following steps.

a. Transcription of interviews and re-reading of transcriptions.

b. Identifying and coding crucial ideas.

c. Generation, structuring and organising of themes from coding.

d. Identification of patterns and connections between related themes.

e. Triangulation with secondary sources where applicable.

For instance, if interviewees were asked of questions of collaboration issues, they should in turn have communicated issues from different lower-tier thematic perspectives. These ideas were then coded and may in some instances be categorised to the theme originally related to the question e.g. collaboration and associated lower-tier theme e.g. digital working needs.

Ideas categorised were then further analysed and coded to determine more specific factors and associated sub-themes. As such, initially captured ideas were more appropriately structured and organised. This may be-line with the actual findings where the researcher was aware their pre-conceived structured allocation of a thematic breakdown may change during analysis.

Following this, the identified sub-themes are explored in more detail, and connections made between sub-themes as part of research-analysis in deriving further gaps. For example, the security-concern sub-themes are captured and then connections are made between them. Finally, further detailed analysis inter-related and contrasted factors across different categories where relevant. This broader level of research-analysis provided the researcher the necessary knowledge in providing critical discussion of issues captured. Overarching or sub-themes captured should also be related with secondary sources to contrast the identified findings with relevant sources (Bashir et al., 2015).

3.6.1 Approach to Structure Analysis Exploration

As mentioned of the interview design, themes pertaining to collaboration and security were isolated where appropriate. This was to capture detailed primary-data, for the purpose of identifying connections between themes from each respective section. This thereby provides extensive insight into the problem environment (Hevner et al., 2004).

Research-analysis of the independently explored themes will therefore inevitably overlap. These factors are expected as BIM projects are complex, and themes and issues are inter-related (Succar 2009). As such, whilst the design-approach enables the researcher to isolate upper lenses of collaboration and security perspectives in capturing issues, this may not however always be appropriate for analysis and in representation of said issues. In other words, for the purposes of exploring the research-interview analysis, it is sometimes unsuitable to isolate exploration of analysis to a single area of collaboration or security. This is where themes and issues related to these upper tiers overlap simultaneously and correspond to multiple dimensions. Such analysis-inferences may also come about via the thematic content-analysis approach.

In response to the aforementioned complexities, an appropriate method to explore the analysis of upper-tier issues, including BIM governance and management is via the ‘overlap of security and collaboration' represented as 'barriers to secure collaboration'. Accordingly, enablers to secure collaboration are also represented throughout the sections of analysis. Barriers to secure collaboration are additionally explored in view of patterns between BIM project dimensions, which allows exploration of patterns between multiple lower-tier themes such as relations between information-sharing and BIM standards. This in turn reflects the nature of cross-analysis of coded themes.

This approach provides freedom of analysis, and thereby exploration of individual issues, but also in making connections between overlapping problems if closely related (Bashir et al., 2015). More broadly, it enables the researcher to feed in themes captured from the independent lens into the bigger picture of how themes overlap as part of a multi-dimensional perspective.

Summary: In summary, emerging themes which overlap the upper-tiers and correspond to multiple themes within the lower tiers will be explored as 'barriers to secure collaboration' via the overlap between BIM project dimensions. The key areas of analysis are to be explored within the following **Chapter 4**. These structures are in turn derived via the rigorous analysis approach detailed.

4 Expert Interview Analysis and Findings

4.1 Introduction

The purpose of this chapter is to explore and analyse the findings from the semi-structured interviews. This includes exploration of identified themes and issues which have been structured into a number of core sections and sub-sections. The relation to themes explored as part of the interview design will be noted in sections where appropriate. In addition, key themes will be summarised in tables after each core section of analysis. Each core section of analysis also features a section-specific discussion which ultimately feeds into an overall discussion within **Section 4.6** to discuss the overarching findings of analysis with respect to enablers and barriers to secure collaboration. The key participants that provided relevant, novel and impactful insights into the issues will be referenced with links to the appendices.

4.2 Outline and Structure of Findings to be Discussed

The areas of analysis will now be outlined. The first section of findings to explore is the 'Socio-Organisational Barriers to Secure Collaboration' **(Section 4.3)**. This section pertains to a socio-organisational dimension (Rezgui et al., 2005) which captures mindset and behavioural barriers that influence the security and collaborative readiness of projects, as well as cultural issues of the built-environment as a whole.

The mindset, behavioural and cultural issues identified from the socio-organisational Section 4.3 feeds into the next area of analysis exploration as 'Barriers to Implementation of Secure and Collaborative Projects' **(Section 4.4)**. This section is in relation to core factors to consider when implementing a project in secure and collaborative fashion. Shortcomings identified of these areas are analysed and discussed.

The final core research analysis to explore is as 'BIM Governance and Management Issues and Limitations' (**Section 4.5**). This section comprises the following sub-sections of analysis. This section will explore information-governance for security and collaborative purposes whilst attempting to discern limitations of current processes and technologies. It will also discuss any directly identified requirements proposed by experts to improve the status-quo of secure collaboration.

4.3 Socio-Organisational Barriers to Secure Collaboration

The socio-organisational concept denotes socio-technical research which is further complicated via norms of BIM projects involving multiple organisations, contained within different appointment structures. Socio-organisational concepts also comprises factors of mindset and behavioural barriers to secure collaboration which are present as shortcomings in how project stakeholders interact socially amongst each other within a project setting, or through the digital environment and technologies in place. It was identified from experts that shortcomings correspond to three types of mindset and behavioural issues:

1. Non-Collaborative: Mindsets and behaviours that impede collectivism within the project ecosystem which further blocks secure and effective collaborative information-sharing (IS).

2. Non-Digital: Mindsets and behaviours that impede effectively utilising digital BIM processes and environments. They also impeded the effective management of information (IM).

3. Security-Incognisance: Mindsets and behaviours pertaining to a lack of knowledge, awareness, and competence of security related factors. This results in unsecure stakeholder behaviours and security-incognisant project initiatives.

The choice to explore such issues from a socio-organisational perspective is based upon the identification that this perspective also encompasses socio-technical shortcomings (Rezgui et al., 2005). This perspective which is adapted from Rezgui et al. (2005) also better captures the nature of shortcomings arising at distinct yet interacting levels of stakeholder collaboration. These are delineated as the following levels of the stakeholder dimension.

Intra-Organisational Lens: The internal lens captures the mindsets and behaviours of individuals and teams which guide their social interactions with others at this level, or their socio-technical interactions. These behaviours and interactions usually occur intra-organisationally. Their interactions may also occur intra-organisationally with individuals and teams as part of cross-organisational interactions. Additionally, the mentalities and behaviours of individuals and teams appear to be representative of a organisations internal culture. It is also noted that the terms individual and professional are inter-changeable within the broader scope of project work.

Inter-Organisational Lens: The inter-organisational lens captures mental and behavioural shortcomings in inter-organisational interactions. This level also captures socio-technical barriers from the perspective of how organisations interact with each other through the shared systems in place to facilitate inter-organisational collaboration within the project. Additionally, the culture of individual organisations is fed into a shared project culture.

Industry Level Cultural Lens: The socio-organisational concept also extends to the culture of the industry, where identified socio-organisational issues reflect upon the industries culture as a whole. Conversely, it was also identified that cultural issues at an industry level feed into issues found within project settings amongst collaborating organisations, individual organisations and individuals and teams.

4.3.1 Non-Collaborative Mindsets and Behaviours

Relation to themes explored within interview design:

- Expert's views on key collaborative and security principles, values and mind-sets.

- Application of PAS Standard Suites to support collaborative and secure working.

- Significant security concerns and threats faced.

Whilst discussing themes of collaborative principles, values and mindset during interviews, a number of socio-organisational issues were identified that factor into impeding collaboration within both security-minded settings and the broader industry. There was also a level of overlap with security-centric themes such as ineffective application of security principles. Security-centric themes were therefore identified to add an additional layer to collaboration averse factors. Accordingly, this section will explore the following core themes of:

1. Aversion and fear of blame (**Section 4.3.1.1**).

2. Self-Interest, over-protectiveness, and isolationism (**Section 4.3.1.2**).

3. Lack of / limited transparency, openness, and trust (**Section 4.3.1.3**).

4.3.1.1 Aversion and Fear of Blame

A2, A3, A4, A7, A9 and A11 believed the aversion and fear of blame within stakeholder interactions was a common issue within high-profile settings. A3 and A9 believed individuals or organisations fear blame from mistakenly under-classifying potentially sensitive information, thereby inadvertently raising potential for exposure. A2, A3, A9 and A11 believed such mindsets lead to behaviours of overprotecting information to avoid potential blame. This occurs when actors tasked with security-classification lack knowledge of the actual security-risk information-sets represent, or simply lack care to the information-needs of other stakeholders. Please see Appendix A.3.1 and A.3.2 for A3s supporting statements on such issues.

As such information is 'over-classified' in respect to actual security-risk present. A3 believed these mentalities and behaviours were representative of A1, A3 and A4s specific nuclear sector and its culture. A3 perceived that there exists a culture of using 'the risk of exposure' as an excuse to avoid improving collaborative information-sharing (IS) behaviours and procedures. A3 believed that cultural changes were required such that stakeholders appropriately share more information, whilst keeping in line with the *actual* security-risk posed. A9 and A11 believe these issues extend to other security-minded sectors as well.

A2, A3, A4, A5, A6, A7, A9 and A11 posed another perspective of an aversion and fear of blame common to both security-minded settings and the broader AEC industry where individuals fear blame for shortcomings within their design-work. This leads to them withholding and potentially hiding design information. The aforementioned experts believed such behaviours can further lead to design errors as a result of a lack of information when other actors require it, and design re-work when information has been identified as missing. It also leads to a general project-level unawareness of what information exists, or who possesses it.

4.3.1.2 Attitudes of Self-Interest, Over-Protectiveness, and Isolationism

A2, A3, A5, A6, A7 and A9 believed self-centeredness and isolationism underline attitudes of individuals perceiving they do not require help, or that supporting the needs of others is insignificant to their own responsibilities. These common mindset and cultural issues within security-minded environments and the broader sector can result in behaviours of not effectively engaging with others, such as withholding information or not attempting to support the design-work of other actors. The aforementioned experts believed attitudes of self-centeredness and isolationism are deep-rooted within the psyches of some individuals, as well as deficient cultures of some partnering organisations, thereby negatively impacting inter-organisational interactions.

A2, A3, A7, A9 and A12 further posed similar issues of system-appointees and information-owners displaying overprotectiveness over their systems and information respectively; these attitudes result in behaviourally formed information-siloes which undermine the effectiveness of both intra and inter-organisational shared digital environments. A2, A3, A6, A7, A9, A11 and A12 believed ensuring effective shared digital environments requires alignment with collectivist mindsets amongst stakeholders; this appears to still be a significant challenge within the built environment as a whole.

Furthermore, according to A2, A3, A6, A7, A9 and A13 a combination of (a) isolationist, overprotective and self-centred mindsets and (b) erroneously defined and ill-communicated BIM responsibilities factor into the following overlapping issues, at both an intra and inter-organisational level. These issues are noted via the following **Points 1, 2** and **3**.

1. Reduction in visibility over numerous activities and information-flows occurring.
2. Actors' awareness on existence and location of relevant information is also decreased.
3. Actors not fully aware of who is obligated to support them and when. This is also corroborated by Winfield and Rock (2018).

Additionally, according to A3, A5, A6, A7 and A9, a lack of mechanisms to address non-compliant actors provides them opportunities to isolate themselves; this issue contributes to beliefs that such negative behaviours are inconsequential. Please see **Appendix A.3.3** for A3s statements on non-collaborative issues and resulting implications of information-unawareness.

4.3.1.3 Lack of Transparency, Openness and Trust in Collaborating Organisations

According to A1, A2, A3, A4, A7, A9 and A10, achieving as-open-as-possible information-sharing (IS) procedures is especially difficult within security-minded settings without transparency, openness and trust amongst collaborating organisations that information is appropriately secured and utilised for mutually agreed purposes.

A1, A2, A3, A4, A7, A9 and A11 perceived that sustained, bi-directional values of transparency and openness leads to gaining of mutual trust that sensitive asset information and intellectual property (IP) is protected by partners. This includes upholding partners data-privacy requirements. A1 also believed collaborators being 'as-open-as-possible' creates a self-reinforcing virtuous circle of open IS where partners are assured that information will be shared and utilised for collective benefit, as opposed to sole gain. A1 believed these factors drive further openness and collaboration whereas stakeholders may otherwise be more apprehensive if a culture of openness had not been embedded initially (Please see Appendix A.1.1 and A.1.2).

With respect to A1s statements on trust within high-profile settings, A1 perceived the level of trust within their specific security-minded setting was a result of themselves as a client and their appointed organisations engendering bidirectional practices of openness and transparency. This was achieved over an extended period of time such that their appointees were transparent and comfortable in engaging with their client or other collaborators to rectify gaps presented by themselves or others.

On the other hand, A1, A2, A3, A4, A7 and A9 believed the high-impact nature of exposure within security-minded sectors more commonly influences cultures of apprehension and distrust in other collaborators. A1, A2, A3, A4 and A7 additionally perceived that achieving transparency, openness, and trust to be difficult to achieve with newly partnering organisation. This may be new appointees or temporary project initiatives.

A3 and A7 also believed there was limited communication and transparency amongst collaborating organisations in ensuring that information is being utilised appropriately and securely in their practices. A3 posed an example of clients and lead-appointees possessing little transparency, visibility, and governance of the IS practices of SMEs within supply-chains. A7 also provided an example of an appointee not ensuring their employees were upholding their obligations to accessing collaborating organisations information in an auditable and secure manner via adherence to rigorous procedures. Scenarios such as these decrease transparency, openness and trust can therefore lead to apprehension amongst collaborators. This can in turn lead to tensions in achieving open IS and collaboration.

A1, A2, A3, A4, A7, A9 and A10 perceived that limited stakeholder transparency and openness results in the following issues which are also relevant to the built environment as a whole. These are noted as the following **Points 1, 2 and 3.**

1. Lack of transparency, openness, and visibility over intra or inter organisational information-sharing procedures and information-flows.
2. Lack of trust and assurance that information shared is used in line with information-owners wishes, towards common commercial goals and not towards sole gain.
3. Lack of trust and assurance that collaborators uphold information-security and privacy requirements for sensitive information and IP of other stakeholders.

According to A1, A2, A5, A7 and A9, the correct form of contract and procurement approach can to some extent align collaborator goals and incentivise project cultures of transparency, openness and trust. A1, A2 and A7 noted shared risk and reward approaches to be of importance. These experts further believed the correct contractual mechanisms to enforce accountability in the event of exposure, or information-misuse can embed trust and assurances that information is secured and utilised correctly.

A1, A2 and A7 also believed appropriate contractual approaches can also alleviate adversarial 'winner and loser', long-term attitudes present within inter-organisational interactions of high-profile environments and the wider industry. Appropriate contractual approaches also however appear necessary to negate the liability culture within high security-risk environments.

4.3.1.4 Summary and Discussion of Non-Collaborative Mindsets and Behaviours

Socio-organisational issues limit efficacy of secure collaboration within high-profile settings and the wider industry. Firstly, transparency and openness appear to be core enablers of secure collaboration via trust being gained amongst collaborators; the absence of these factors can however present tensions in effective IS due to information-owners not possessing assurance that collaborators utilise and secure information in line with their wishes. Avoiding this tension is especially pertinent for achieving open IS within high security-risk settings and appears to be a factor that could still be improved within such settings and the wider-industry. For example, A1 and A4's practices appeared to achieve this, but this does not seem common.

It is also questionable whether collaborators within security-minded settings and the broader industry possess sufficient visibility over their workflows. For example, A3 posed that there was little transparency and visibility over appointment-chain activities. A3 also perceived technologies provided little in terms of governance to alleviate these issues which is further expanded upon in **Section 4.5**.

Additionally, a lack of transparency, openness and trust is closely linked to mindsets of an: (a) aversion and fear of blame and (b) self-interest, isolationism, overprotectiveness. These unfavourable attitudes lead to a lack of visibility over information-flows at the level of both intra and inter-organisational relationships. Another contributing factor was ineffective communication of multi-organisational BIM responsibilities; additionally, intra-organisationally originating information-siloes result in a lack of intra-organisational awareness of information existence and location which may cascade inter-organisationally. The collective implications being that actors do not always know (a) where or what information exists or (b) which actor is required to support other actors and when.

Finally, A1, A4, A6, A9, A10, A11 and A12 proposed the wider industry may face security and collaboration overlapping tensions (such as lack of transparency in collaborators security), after the value and necessity of security-minded procedures is more readily understood. Currently, non-collaborative issues may manifest more broadly such as cultures of distrust based upon ineffective contractual mechanisms or hiding of information. The following **Table 4.1** summarises the themes discussed and which experts they were captured from.

Table 4.1: Non-Collaborative Themes

Concept #	Non-Collaborative Themes	Expert Occurrences	Total
1.	Overclassifying information due to fear of blame / limited knowledge.	A2, A3, A4, A7, A9 and A11.	6
2.	Under-classifying information due to limited knowledge / lack of care.	A2, A3, A4, A7, A9, A10 and A11.	6
3.	Security-risks as excuse to not improving collaborative focuses / potential.	A3, A4, A8, A10 and A11.	5
4.	Behavioural data siloes (overprotectiveness).	A2, A3, A7, A9 and A12.	5
5.	Limited visibility of stakeholder responsibilities (via self-centeredness / isolationism).	A2, A3, A5, A6, A7 and A9.	6
6.	Withholding / hiding information (fear, self-interest and poor requirements).	A2, A3, A4, A5, A6, A7, A9 and A11.	8
7.	Information unawareness – 'what', 'where' and 'who'. Due to *fear*, *self-interest* or *poor requirements*.	A2, A3, A4, A5, A6, A7, A9, A11 and A13.	9
8.	Not supporting other's needs / sharing information (self-centred perceptions of non-consequence).	A2, A3, A7, A9 and A12.	5
9.	Longstanding culture of distrust due to risk of exposure.	A1, A2, A3, A4, A7 and A9.	6
10.	Difficult to embed trust short-term in security-minded projects.	A1, A2, A3, A4, A7 and A9.	6
11.	Limited stakeholder transparency, openness and trust:		
11a	Unaware if information protected by and utilised in-line with stakeholder's requirements and visions.	A1, A2, A3, A4, A7, A9 and A10.	7
11b.	Leads to IS tensions within security-minded sectors.	A1, A2, A3, A4, A7, A9 and A10.	7
12.	Need for values of trust and transparency to resolve cultural causes of IS tensions / apprehensions.	A1, A2, A3, A4, A7, A9 and A11.	7

4.3.2 Non-Digital Mindsets and Behaviours

Relation to themes explored within interview design:

- Expert's views on key collaborative and security principles, values and mind-sets.
- Application of PAS standard-suites to support collaborative and secure working.
- Significant security concerns and threats faced.

Previously discussed within **Section 4.3.1** were inhibitors to collaboration from the perspective of non-collaborative mindsets that adversely influence interrelationships of stakeholders, and their socio-technical interactions. This section however explores socio-organisational shortcomings from the perspective of mindset-gaps towards the requirement-setting, and implementation of the following digital procedures of BIM workflows.

- Information-Generation (IG) procedures and processes.
- Information-Management (IM) procedures and processes.
- Information-Sharing (IS) procedures and processes.

This section will discuss these non-digital mindset and cultural issues which are the focus of this section. These factors are the following.

1. Limited Recognition and Knowledge of Digital BIM Requirements and Procedures **(Section 4.3.2.1).**
2. Avoidance of Planning and Adherence to Digital Procedures **(Section 4.3.2.2).**
3. Need for Education, Innovation and Incentivisation of Digital BIM approaches **(Section 4.3.2.3).**
4. Disconnect between Software Users and Software Vendors **(Section 4.3.2.4).**

More detailed process-centric issues in defining and implementing such requirements are however noted in **Section 4.4.3** and **4.4.4** whilst the limitations of current BIM process protocols and technologies are discussed in **Sections 4.5.2** and **4.5.3**.

4.3.2.1 Limited Recognition and Knowledge of Digital BIM Requirements and Procedures

According to A2, A3, A5, A6, A7, A8 and A9, misconceptions and lack of recognition and knowledge surrounding digital BIM procedures is representative of mental, cultural and knowledge barriers to be overcome at the board-level roles within inexperienced clients and suppliers. For example, A2, A6, A7, A8 and A9 perceived that senior-roles misperceive BIM as simply digital BIM models / modelling, or associated technologies. This also appears to be the case from a practitioner perspective.

Senior roles appear also yet to fully recognise how defining detailed and accurate requirements over digital BIM procedures is crucial in implementing digital technologies and workflows to bring about significant cost, optimisation, and security benefits. Correspondingly, senior roles possess limited cognisance of the consequences of ineffective digital approaches as a mental connection appears to be lacking between: (a) ineffective BIM requirements and (b) a project's resulting limited digital readiness. A2, A6, A7, A8 and A9 believed that bridging such mental gaps amongst senior roles requires recognition and understanding of the following.

1. Collaborative and digital mindsets as well as effective IG, IM and IS procedures, are the main focuses and benefits of BIM approaches.

2. BIM projects will only be as effective as the business requirements and digital procedures underpinning them.

3. Digital BIM workflows, technologies and software must be underpinned by the correct BIM requirements to achieve effective IG, IM and IS.

A2, A6, A7 and A9 further believed that senior and project-management roles need to perceive that the implementation of effective digital **IG** and **IM** procedures is essential in deriving high-quality, structured and secured data. A6 further believed senior-roles do not understand the business benefits of information as a resource to effectively drive **BIM** workflows such as via informed decision making. A6 also believed more awareness is required that high-quality data should be cultivated via effective **IM** and policies and procedures as opposed to sole reliance of **IM** focuses to software-vendor tools.

A1, A2, A6, A7 and A9 additionally believed that the significance of defining and employing effective asset information management procedures prior to set-up of new projects is not well understood or overlooked. As such, inexperienced clients and suppliers forego their opportunity to leverage relevant information on completed projects / assets towards the commercial and efficiency optimisation of new projects. Recognition must therefore be embedded within senior and project-management roles on the business benefits effective digital procedures bring when underpinned by the correct requirements. Please see **Appendix A.6.1** for further insight via A6s statement on both the need and difficulty to embed digital mindsets at the board-level of organisations.

4.3.2.2 Avoidance of Planning and Adherence to Digital Procedures

A7 and A9 posed that project and team-managers do not usually effectively plan and define the IG, IM and IS aspects of BIM work they are responsible unless forced by the client's BIM requirements. They believed this issue was common across the built-environment. A2, A5, A6, A7 and A9 indicated that even if requirements are defined, project / team managers, and professionals also underestimate the consequences of not adhering to these requirements.

As such, A2, A5, A6, A7 and A9 found that adherence to BIM requirements is commonly perceived as inconsequential at an individual and team level up until the 'last-minute' where the scale of information generated grows beyond the ability of stakeholder to govern effectively. A2, A5, A6, A7, and A11 also proposed impacts are more pronounced within projects with more stakeholders, where there is significant difficulty in understanding what information exists once generated and who possesses and owns it. A2 for example perceived such issues on a large infrastructure project (See Appendix A.2.1 and A.2.2).

4.3.2.3 Need for Education, Innovation, and Incentivisation of Digital BIM Approaches

According to A2, A3, A6, A7, A9 and A12 a significant level of education and incentivisation is required for both clients and appointees within the broader sector. A2 believed this included conveying to board level roles the financial, security, efficiency and competitive advantages that effective and innovative digital approaches bring to their practices. A2 and A6 however found that conveying benefit to senior roles within digitally immature organisations such as SMEs is more difficult, and significant barriers appear to be an aversion to change and limited knowledge.

Please see Appendix A.2.3 for A2's perceptions that it is therefore especially pertinent for appointing organisations to provide incentives for SMEs for them to fully embrace and leverage digital BIM approaches. Likewise, increased education and passing of viability tests is essential for senior-roles to prove the value in investing in improving digital competencies and capabilities.

Lead appointees within industry also however appear to possess limited recognition of their obligations in properly guiding inexperienced clients, or simply limited cognisance that they possess such obligations. On the contrary, it was identified via A6 that some negligent suppliers may misrepresent their BIM competencies to inexperienced potential clients to achieve selection during bidding processes.

4.3.2.4 Disconnect between Software Users and Software Vendors

This section overlaps with security and digital considerations. Firstly, as users of both design and information-management software, A3 and A9 proposed a disconnect between the perceptions of the user and software developers in respect to system-usability. A3 and A9 believed that practitioners may not know exactly what software features would improve their operations or are not able to effectively communicate their system needs and requirements. They also believed more effort required by vendors to effectively interface with their users.

Whilst these are typical software implementation issues, A3 and A9 felt they were exemplified within the AEC software industry and were especially important in terms of whether AEC vendors could meet the necessary efficacy and security requirements of users. Likewise, A3 proposed software that lacked usability can contribute to unsecure usage of technologies (See Appendix A.3.4). An additional factor A6 believed was that many organisations, especially board-level roles fall into a trap in believing IM issues can be solved solely via implementation of software. This issue is linked to limited digital knowledge but A6 also believed that software-vendor marketing contributed to this issue by the overly simplistic promotion that organisations can achieve effective asset-management via a technology alone (See Appendix A.6.2).

4.3.2.5 Summary and Discussion of Non-Digital Mindsets

There are a number of cultural and mindset gaps in how senior-roles within security-minded sectors and the broader industry of how they perceive digital IG, IM and IS procedures. Senior roles appear to not fully understand or may underestimate the impact of ineffective digital BIM requirements on the digital appropriateness and readiness of their workflows and technologies.

Similarly, individual, team and project-manager roles may perceive avoidance of BIM requirements as inconsequential which results in erroneous and uncontrollable IM. Senior roles may also misperceive BIM as being simply linked to modelling or technologies. Additionally, effective IM on existing assets appears to be an afterthought. This is as opposed to applying effective asset IM procedures prior to the start of new projects.

It appears there is therefore a significant need for education and incentivisation within both clients and appointed organisations. These factors are especially pertinent as senior-roles seem to be misinformed of the benefits digital BIM procedures can bring about in the form of high-quality, structured and secured data for their digital processes. There does, however, appear to be a degree of push-back or aversion to change from senior-roles at this level; it is also even more difficult for SMEs to understand the benefits which may limit the capabilities of supply-chains. If senior-roles within the client and appointed organisations do not understand the cost, efficiency, and security benefits of effective, IG, IM and IS, then this can lead to not defining appropriate plans for a project's information-flows. This will inevitably impact on their effectiveness and security. As such, either not defining or not adhering to effective digital procedures can have debilitating impacts on the effectiveness of information-flows.

Table 4.2: Non-Digital Themes

Concept #	Non-Digital Themes	Expert Occurrences	Total
1.	Misperceiving need and background of BIM.	A2, A3, A5, A6, A7, A8 and A9.	7
2.	Misperception of BIM as models / technology driven.	A2, A6, A7 and A9	4
3.	Limited understanding of implications of ineffective BIM on project's limited digital readiness.	A2, A6, A7, A8 and A9	5
4.	Limited understanding of need to define IM policy for effective digital project outcomes.	A2, A6, A7 and A9	4
5.	Senior-roles must understand effective IM focuses underpin effective project outcomes (time, cost and quality).	A2, A3, A4, A5, A6, A7, A8 and A9.	7
6.	Need to understand effective AIM should underpin new project IM initiatives.	A1, A2, A6, A7 and A9	5
7.	Managers and practitioners underestimate consequences of not adhering to IM requirements.	A2, A5, A6, A7 and A9	5
8.	Need for significant education and incentivisation of BIM for SMEs / organisations with lesser digital maturity.	A2, A3, A6, A7, A9 and A12	6
9.	Disconnect between AEC / BIM software users and vendors.	A3 and A9.	2

4.3.3 Security Incognisant Mindsets and Behaviours

As a brief background to security-centric socio-organisational factors, the ISO 19650-5 standard denotes that security-risk broadly refers to the potential of the following types of damages:

a. Financial or reputational damages to project stakeholders.

b. Damage to asset related information, or the built asset itself (in whole, or in part).

c. Health and safety hazards to occupants.

Moreover, the standard sought to increase awareness of the risks posed to built-assets within the increasingly open and digital backdrop of BIM workflows. The general consensus from experts however was that the broader industry still possesses limited aptitude in:

- Recognising when and *why* a security-minded approach is necessary, based upon the initial **awareness** of risks present.
- Possessing **knowledge** and **competencies** on how to effectively implement secure, yet still effective and collaborative approaches.

Issues surrounding this lack of awareness, knowledge and competencies are explored under the umbrella of *security incognisance*. Security incognisance is also relevant to some instances of high-profile projects which are required by regulatory bodies to implement security-conscious approaches. As explored as part of the interview-design, the security-centric *mindsets and behaviours* of actors involved with such projects may however run counter to security-minded motives. This section will expand these collective issues via the following factors.

1. Security-Incognisant Attitudes and Behaviours Amongst Individuals and Teams:
2. Security Incognisance Amongst Clients and Asset Owners.
3. Security Negligence and Need for Accountability Mechanisms.
4. Need for Security-Minded Education and Training.

4.3.3.1 Security Incognisance Amongst Individuals and Teams

A pertinent security-incognisance issue at the team-level is an aversion to adherence of prescribed and secured avenues for IM and IS. This primarily pertains to avoidance of secured network infrastructure within which the CDE resides. This issue was identified in respect to some of the security-minded practices interviewed and experts' opinions of projects within the wider industry. A2, A3, A4, A7 and A9 were of the opinion these negligent behaviours are guided via security-incognisant perceptions. Such perceptions include beliefs that adherence to prescribed procedures and technologies are lengthier and more restrictive than other less secure avenues. In some instances, such perceptions are proved true as noted in **Section 4.3.1.1** due to the liability culture present in some security-minded projects.

A2 and A3 believed the other side to this issue was the presence of 'user-unfriendly' technologies which A2 believed may lead to: "*People jumping through hoops because the processes and the systems aren't working for them*". Other compounding, and deep-rooted attitudes displayed by negligent individuals and teams are:

a. Not understanding the need or importance of adhering to security procedures (**Experts:** A2, A3, A4, A5, A6, A7, A9, A10, A11 and A12).

b. Misperceptions and short-sighted beliefs that their behaviours are insignificant in the contribution to security-risk; this also points to misplaced overconfidence (**Experts**: A3, A6, A7, A9, A10, A11 and A12).

c. Rigidity, indifference, and aversion to change when confronted with new or changing requirements to employ security-conscious procedures (**Experts**: A1, A3, A4, A6, A7, A9, A10, A11 and A12).

The aforementioned attitudes lead to negligent behaviours. A2, A3, A4, A7, A9, A10 and A12 believed that individuals and teams may for example bypass the prescribed CDEs in favour of utilising less secure file-hosting-services and email. A3 posed an example that underlines all three types of aforementioned attitudes based around incognisance and usage of unsecure IM systems in critical environments (See Appendix A.3.5).

According to the aforementioned experts, using unsecured methods also results in an inability to track and govern information-flows. From a security perspective, this leads to a lack of visibility over who possesses what information, whether information is held by the appropriate parties, or if it has been exposed to threat-actors with malicious intent. A3 and A9 additionally perceived that individual lack understanding of the need for consistent security-minded behaviours in respect to usage of information and system assets throughout the project process. On this point, A9 perceived individuals are not able to make the mental connection that the correct behaviours should apply regardless of physical presence and instead perceive the need for security-minded behaviours to be limited to presence within secured physical environments. Please see Appendix A.9.1 for A9s statement which provides context as to why behavioural issues are faced.

4.3.3.2 Client and Asset Owners Security Incognisance

The high-profile projects interviewed held relatively fewer gaps in their security-cognisance when contrasted with interviewees opinions towards the rest of the industry. A3, A4, A5, A6, A7, A8, A9, A10 and A11 however perceived that CNI sectors still possess cognisance issues due to the gaps in mindsets of senior-roles within high-profile projects. According to A1, A2, A3, A4, A5, A6, A7, A9, A10 and A11 however, client organisations within the broader industry lack security-cognisance to an even greater extent.

Inexperienced clients within the wider industry and high-profile sectors lack holistic awareness of security-risks, competencies, and knowledge on how they should be effectively managed. This is concerning as clients ultimately make decisions over the security readiness of their project (CPNI 2020). A2, A4, A5, A6, A7, A8, A9, A10 and A11 believed the security-incognisance of senior-roles within client organisations manifests as inadequate security requirements which in turn limit a project's security readiness.

The aforementioned experts therefore proposed more focus is necessary in ensuring that senior-roles understand the necessity and importance of security in order to implement sufficient security-minded organisational values, strategies and procedures; these should filter down to attitudes and working practices to professionals and teams. This initiative is also significant for security-minded sectors but appears to be just as pressing for the broader built-environment. Please see Appendix A.6.3 and A.6.4 for A6s critical statements upon incognisance implicating clients and procurement.

4.3.3.3 Security Negligence and Need for Accountability Mechanisms

A1, A4, A5, A6, A7, A9, A10 and A11 additionally believed that the incognisance of inexperienced clients is a factor that leads to selection of security-negligent suppliers within the broader sector. This factor is compounded by cost-reduction practices of both clients and suppliers during procurement where A6, A9 and A11 believed implementing both optimised and security-minded IG, IM and IS procedures is costlier. A6 drew a parallel to the 'Grenfell Tower' disaster where focuses during operation were on reducing cladding costs. In a similar vein, A6 perceived that some especially negligent suppliers may choose to omit BIM and security requirements to be more price-competitive, and equally incognisant clients will opt for 'cheaper' bids without such procedures.

A3, A4, A5, A6, A7, A8 and A9 also believed that both the built-environment and society as a whole possess underlying attitudes that data-breaches are unavoidable. A3 and A6 drew a further parallel to the prior state of health and safety mechanisms within the AEC industry and the current trends of negligence within information-security and information-quality approaches. According to A3 and A6, the previously widespread nature of health and safety incidents was accepted as 'business as usual' due to a lack of mechanisms to hold negligent parties to account.

On the other hand, the introduction of accountability mechanisms for health and safety has resulted in responsible parties investing more focus, time and resources towards planning and implementing project-safety in order to avoid commercial and legal repercussions. A6 believed similar changes need to occur at a cultural and legal level within the built-environment in order for security-negligent suppliers to apply an appropriate level of care to their clients. This includes the following.

1. Ensuring professional care is taken to understand the security needs and requirements of clients.

2. Ensuring sufficient security-minded supplier proposals in line with security-risk faced by clients. This includes improvements of information-security procedures.

A3 and A6 believed that clients and asset-owners must *also* take a proactive role over information-quality and security. This is especially pertinent for CNI contexts, or simply where clients possess obligations towards passive stakeholders such as occupants, the public or neighbouring asset-owners. A6 in particular believed the implementation of better regulatory and accountability mechanisms for the built environment will play a significant role here. For example, A6 noted the general data protection regulation act as a high-level 'tool' that could drive security-minded culture in the AEC industry. However, bespoke regulatory approaches are necessary as corroborated by Kenny (2016). Such mechanisms must capture and enforce the legal and commercial implications for both clients and appointed parties not proactively ensuring information-security and information-privacy. Please see **Appendix A.6.5** for A6s statements on cultural issues of negligence, exposure and accountability that must be overcome.

4.3.3.4 Need for Security-Minded Education and Training

It was identified via A2, A3, A4, A6, A7, A8, A9 and A10 that more education and assurance is necessary amongst actors as part of settings of elevated risk and the broader sector. For example, in respect to the necessity for senior-roles to understand the necessity for security-minded procedures so that they become part of internal organisational culture. A6 further believed that even if the full-breadth of holistic security-cognisance is not currently possessed by organisations, a positive step forward is simply having in place designated security-centric roles promoting the recognition and need for holistic security (British Standards Institution, 2015).

A4 believed it was especially important for clients to undertake security-assurance activities in order to fill security-cognisance gaps existing at multiple levels within the hierarchy of appointed organisations and team-level actors. A4 believed that even simple assurance activities such as checking understanding of procedures was important in creating dialogue and awareness. A4 and A10 further believed the importance of security-assurance initiatives would become increasingly apparent for the broader sector once implications of insufficient security are better understood.

A6 on the other hand believed whilst education / training were important, certain negligent actors would still manifest behavioural issues linked to their psyches and past working experience. Similarly, A3, A9 and A10 held experiences and concerns of individuals and teams within high-profile settings exhibiting security-incognisant behaviours despite that such settings should be held to higher levels of scrutiny. This point is related to A6, A9 and A10's belief that individuals and organisations of lesser maturity are a weakest link. Please see Appendix A.6.6 for A6's statements on the benefits of promoting awareness.

4.3.3.5 Summary and Discussion of Security Incognisance

Security-incognisance appears to be a pertinent issue within the wider industry and to a lesser extent, high-profile sectors. At a professional and team-level, there appear to be multi-faceted security-incognisance gaps of: (a) a lack of awareness, knowledge, understanding and competencies; (b) security misperceptions and indifference; (c) overconfidence and (d) rigidity / aversion to change.

These mindsets manifest as behaviours of not utilising the prescribed and secured avenues for IM and IS which leads to difficulty tracking information-flows or knowing whether information has been exposed due to unsecure behaviours, i.e., a lack of information-flow visibility and provenance. These factors in turn appear to limit the effective governance of information-flows intra-organisationally which will also cascade to affect inter-organisational interactions.

Another central factor identified is in respect to whether senior-roles within clients and appointed organisations are aware of the importance of sufficient business-governance over security-minded organisational-level values, strategies, and procedures. Currently, however, it appears questionable whether senior-roles within the built-environment possess the necessary security-cognisance to understand the implications of ineffective security measures and thereby the pertinence of proactively structuring their organisations security-readiness. This gap by extension negatively influences the security-cognisance of team and individual level actors.

Experts also believed client-driven focus is the determining factor of whether a project is implemented securely. Presently however, if clients are incognisant of the need for and importance of security-minded BIM, then this will factor into the selection of incompetent and negligent parties; it also appears that cost-reduction approaches are a significant factor here.

Whilst security-minded BIM may be costlier, it is altogether necessary for suppliers to provide the necessary level of care tailored to the client’s specific needs. Moving past this issue is difficult due to an apparent prevailing lack of focus and care towards security-minded BIM within the broader industry. There therefore appears to be a need for cultural changes alongside improved accountability and regulatory mechanisms within the built environment as a whole such that clients and suppliers approach security and privacy with more pertinence. Moving past these issues may also require a paradigm-shift in the current procurement approaches. More broadly, there also appears to be a need to carry out an in-depth exploration to the degree of security negligence within the BIM marketplace. Finally, in view of this section's analysis undertaken, another factor of a lack of security meta-cognition was identified via synthesis of expert's opinions towards security-cognisance and is discussed within the following section.

4.3.3.6 Limited Security Meta-Cognition

A1, A2, A3, A4, A6, A7, A9, A10 and A11 all posed their beliefs in respect to how project actors perceive security-centric aspects of the project. These beliefs were analysed to identify that overconfidence of security knowledge and competencies, correspond to a lack of meta-cognitive capability to perceive gaps within one's own security-cognisance. In other words, a degree of critical self-awareness displayed by any given actor (organisational or individual), of the gaps that they must still fill of their present degree of knowledge and competencies.

Individual and teams for example may potentially lack the meta-cognitive capability to understand that no resulting exposure from previous negligent activities does not equal an absence of *present* security-risk, and therefore an excuse to ignore security procedures on live projects. A lack of meta-cognition at a team-level is therefore compounded by attitudes of short-sightedness, indifference, and misperceptions towards security exposure.

A1, A3, A4, A6, A7, A10 and A11 believed that organisations and senior-roles may also lack the meta-cognitive capability to understand that there are gaps present within their security-procedures. A10 posed an example of a client organisation within a high-profile sector believing their security-procedures to be inviolable. In reality, the client was incognisant of how digital approaches expose their organisation and assets to vulnerabilities of a cyber and information nature and therefore require corresponding safeguards. **Figure 4.1** provides a visual depiction of limited or lack of security meta-cognition.

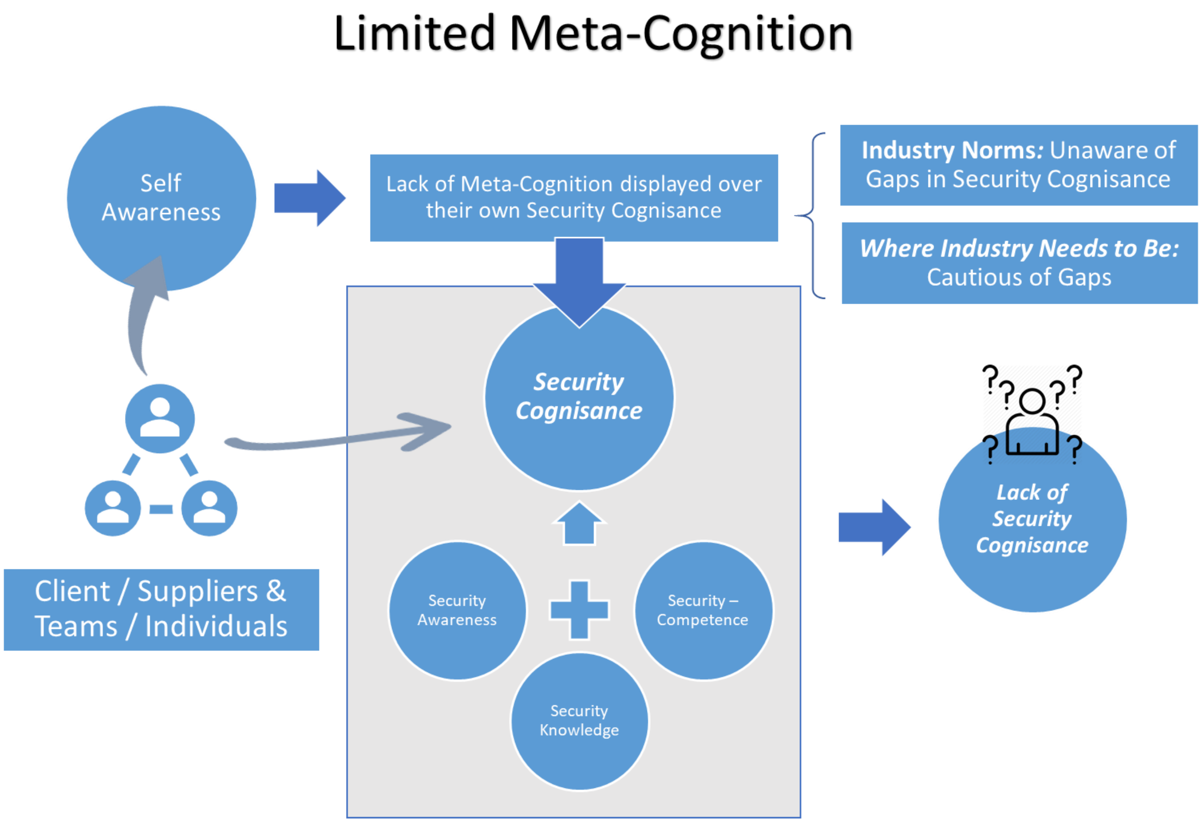

Limited Meta-Cognition
Self Awareness
Lack of Meta-Cognition displayed over their own Security Cognisance
Industry Norms: Unaware of Gaps in Security Cognisance
Where Industry Needs to Be: Cautious of Gaps
Security Cognisance
Security Awareness
Security – Competence
Security Knowledge
Lack of Security Cognisance
Client / Suppliers & Teams / Individuals

Figure 4.1: Security Meta-Cognition

Table 4.3: Security-Incognisance Themes

Concept #	Security-Incognisance Theme	Expert Occurrences	Total
1.	Non-adherence to secure avenues for IM / IS e.g. bypassing CDEs and using email.	A2, A3, A4, A6, A7, A8, A9, A10, A11 and A12.	10
2.	Misperceiving security consequences of behaviours as inconsequential.	A3, A6, A7, A9, A10, A11 and A12	7
3.	Aversion to change when introduced to security-requirements / procedure.	A1, A3, A4, A6, A7, A9, A10, A11 and A12	9
4.	Limited visibility over exposures and 'who' has 'what' information and 'where' due to behaviours.	A2, A3, A4, A6, A7, A8, A9, A10 and A11.	9
5.	Clients within broader industry are security-incognisant to greater extent.	A1, A2, A3, A4, A5, A6, A7, A9, A10 and A11.	10
6.	Board-level / senior-role incognisance within client organisations.	A2, A4, A5, A6, A7, A8, A9, A10 and A11	9
7.	Incognisance manifests as inadequate security-requirements – implicating ineffective project security-readiness.	A4, A5, A6, A7, A8, A9, A10 and A11.	8
8.	Client incognisance influences ineffectual project security practices / choices (e.g. 'cost-reduction' implicating selection).	A1, A4, A5, A6, A7, A9, A10 and A11	8
9.	Incognisant appointees (potential or appointed) do not include, or may omit security-requirements.	A2, A5, A6, A7, A9, A10 and A11.	8
10.	Incognisant / negligent bidders (no secure IM proposals) win projects on cost-basis.	A6, A7, A9, A10 and A11.	5
11.	Lack of and need for accountability / repercussion mechanisms for ineffectual security-risk.	A2, A3, A4, A6, A8, A9, A10 and A11.	8
12.	More security-minded education and assurance / guidance resources are necessary.	A2, A3, A4, A6, A7, A8, A9 and A10	8

4.3.4 Socio-Organisational Discussion

Themes were analysed pertaining to principles, values and mindsets that underpin collaboration, security, and their overlap. Accordingly, an analysis of patterns between non-collaborative, non-digital and security-incognisant factors exposes underlying themes which appear common across the board, and the following areas are the core part of this discussion.

1. Implications to Industry Culture and Implementation of Secure and Collaborative Projects.
2. Socio-Technical Implications to Secure Collaboration for Project Information Flows.

The core themes for both of these sections being a number of cultural and project-level issues that are common across security-minded settings interviewed and expert perceptions of the BIM and security maturity for broader industry. Additionally, issues explored in respect to collaboration-averse, non-digital and security-incognisant areas overlap significantly and must be interrelated.

4.3.4.1 Implications to Industry Culture and Implementation of Projects

Socio-organisational issues captured appear representative, or inductive of issues faced at a cultural level within security-minded sectors and the built-environment as a whole. Additionally, many issues appear to factor into ineffective implementation of projects in their combined security and collaborative readiness.

Firstly, values of transparency, openness and trust are common factors previously associated with enabling effective collaboration (Patel et al., 2012). The exploration of **Section 4.3.1.3** has however posed these values are essential for enabling as-open-as-possible collaboration within security-minded environments. This is where concerns of exposure of sensitivities, and associated indemnities are present. Likewise, factors of transparency, openness and trust are also pertinent to alleviate potential, and thereby concerns of exposure of personal and commercial information. These factors are also therefore pertinent for broader practice.

Inter-organisational relationships however appear to possess limited values of openness, transparency, and trust. This presents barriers to effective interactions and secure collaboration. Furthermore, projects within broader industry may face this tension at a lesser scale wherein concerns of exposure of commercial or privacy sensitivities are present. The lesser scale of tensions is likely however a reflection of limited security focuses within the built environment. As noted of security negligence (**Section 4.3.3**), there will likely be increasing requirement for stakeholders to also apply security procedures in managing built-asset information to a degree of sufficient security. Such factors are further expanded upon within **Section 4.4.4.2** from the lens of security-risk governance in the broader sector.

Addressing such cultural and mindset concerns in ensuring transparency and openness in facilitating trust between organisational-level stakeholders, with security-centric concerns of indemnities, will likely require industry-level initiatives. Another overlapping theme was the need for further education. It was identified inexperienced clients and appointees require further acquisition of competencies of digital, and security focuses throughout their organisations. However, it appears more education is required from a security standpoint. This is based upon perspectives captured of concerning levels of security-incognisance arising from many types of project stakeholders, and at all hierarchal levels. It was also noted that secure and digital BIM competence is further constrained at the lower spectrum of appointment-chains. This points to significant need to motivate, incentivise, and educate SMEs of the need for security-minded BIM.

This being said, concerns of deficient attitudes and competencies of appointees as a whole were captured. Correspondingly, this throws into question their ability to support clients with effective security-minded approaches. This concern is exemplified for the built environment; A6, A7, A9, A10 and A11 believed very few lead-appointees and their appointment-chains possess comprehensive and holistic security competencies. In actuality, A6 believed there is a significant level of supplier inattention to provision of secure BIM.

Issues of negligent stakeholder attitudes, behaviours and project structuring approaches must be rectified at overlapping cultural, educational and legal dimensions. Part of addressing such issues appears to require improved regulatory mechanisms within the built environment as a whole to capture and administer the repercussions of exposure of stakeholder's assets due to negligent information security and privacy approaches. Correspondingly, the competitive benefits for appointees, at whichever tier, in being able to provide a security-minded BIM competence to their appointer, must be further explored and thereby communicated within industry. Similar such mechanisms also appear necessary at the level of BIM project governance and management in addressing ineffective actors' inter-relationships and isolationist type behaviours.

There are also cultural concerns of adoption of negligent suppliers by security-incognisant clients on a cost-basis. These issues correspond to clients not understanding the importance and benefits of defining and applying appropriate, effective and secure approaches for BIM IG, IM and IS.

Furthermore, cultural issues of security-cognisance gaps appeared more pertinent when contrasting awareness of (a) digital BIM and (b) security-minded approaches.

Client security-incognisance in particular appears to be a determining factor in whether projects are implemented with appropriate readiness for secure collaboration. Experts therefore agreed more focus is required such that senior-level roles within client and asset-owner organisations take the initiative in terms of digital BIM collaborative and security-readiness of their projects when initiating them. This, of course, is a factor that overlaps whether a project is 'high-profile' in nature or not.

4.3.4.2 Socio-Technical Implications to Secure and Collaborative Information Flows

Actor's mindsets and behaviours appear to result in socio-technical barriers to secure collaboration which overlap non-collaborative, non-digital and security-incognisance areas. These factors and associated implications will be progressively related. Firstly, shared implications were identified from the perspective of non-collaborative mindsets of: (a) aversion and fear of blame (influenced by liability cultures); (b) non-engagement, including self-interest, isolationism and overprotectiveness and also themes of (c) limited transparency, openness and trust.

These mindsets collectively result in behaviours of hiding / withholding information and not requesting and supporting the needs of others. This presents further visibility and discoverability issues of not knowing: ***'what, where or who possesses information of relevance to them?'***, in enabling optimal work or ***'who should support the needs of others and when?'.*** Similarly, the attitudes of: (a) 'aversion of blame and isolationism' lead to (b) behaviours of 'overclassifying and overprotecting' information. This is availability to information in general, access to information within systems, or access to the systems themselves. The shared implication being that actors may be unable to access information when necessary, to the appropriate degree required.

Moving on to the implications of non-digital mindsets and behaviours, it was noted these are also closely related to non-collaborative and security-incognisant behaviours. Non-digital mindsets identified were: (a) unawareness of significance digital BIM approaches; (b) underestimating the significance of timely, effective, and consistent IM and (c) aversion to digital change. These mindsets lead to behaviours and practices of not defining or adhering to the digital BIM requirements and procedures, further leading to last-minute and erroneous IM procedures. This may also be caused by individual and team aversion to procedures and change posed via digital approaches more broadly. The implications of these mindsets appear in turn to limit actors' abilities in managing the large volumes of information generated. This can then also present discoverability issues, limited effectiveness of decision-making and thereby negative implications to effective project progression.

Implications of non-digital mindsets and behaviours also appear mirrored from a security-incognisance perspective where there were significant implications to the security of information-flows at an individual and team-level based upon gaps in security-cognisance. These security-cognisance gaps were: (a) a lack of knowledge; (b) security-misperceptions and overconfidence and (c) rigidity, indifference, aversion to change and push-back. Security-incognisance leads to behaviours of bypassing prescribed, secured avenues for IS and not consistently employing security-minded behaviours regardless of factors such as a professionals physical work context. The collective implications of the aforementioned gaps in security-cognisance appear to be: (a) limited ability in effectively tracking and managing actors work, which includes IG, IM and IS components of project-work; (b) not knowing who possess what information and (c) unawareness and lack of visibility of whether information has been exposed.

Furthermore, cultural issues of limited transparency, openness and trust in partnering organisations coincide with limited transparency and openness over information-flows between partnering organisations. Non-engagement type attitudes in turn represents a tension in ensuring effective and secure collaboration at an inter-organisational scale. Likewise, the mindsets and behaviours of intra-organisational level actors also pose issues of a similar nature in respect to internal socio-technical features. This is whereby limited visibility over project-work and information-flows may also be presented by isolationism and limited transparency and openness by intra-organisational actors.

These behaviours extend to whichever systems are in place. This is whereby the BIM marketplace for system-vendors overlap that of the broader industry. More so, the typical implementation of systems and the systems themselves appear misaligned to needs of users in effectively, easily but securely transacting amongst others at whichever hierarchal level. This is without additional erroneous procedures whilst it also ensuring information-security features are upheld. Rather, customers as suppliers or clients are in essence 'mis-sold' a belief implementation of certain systems will ensure security. This appears particularly noteworthy issue of socio-technical considerations within domains presently security-minded or aiming to be so.

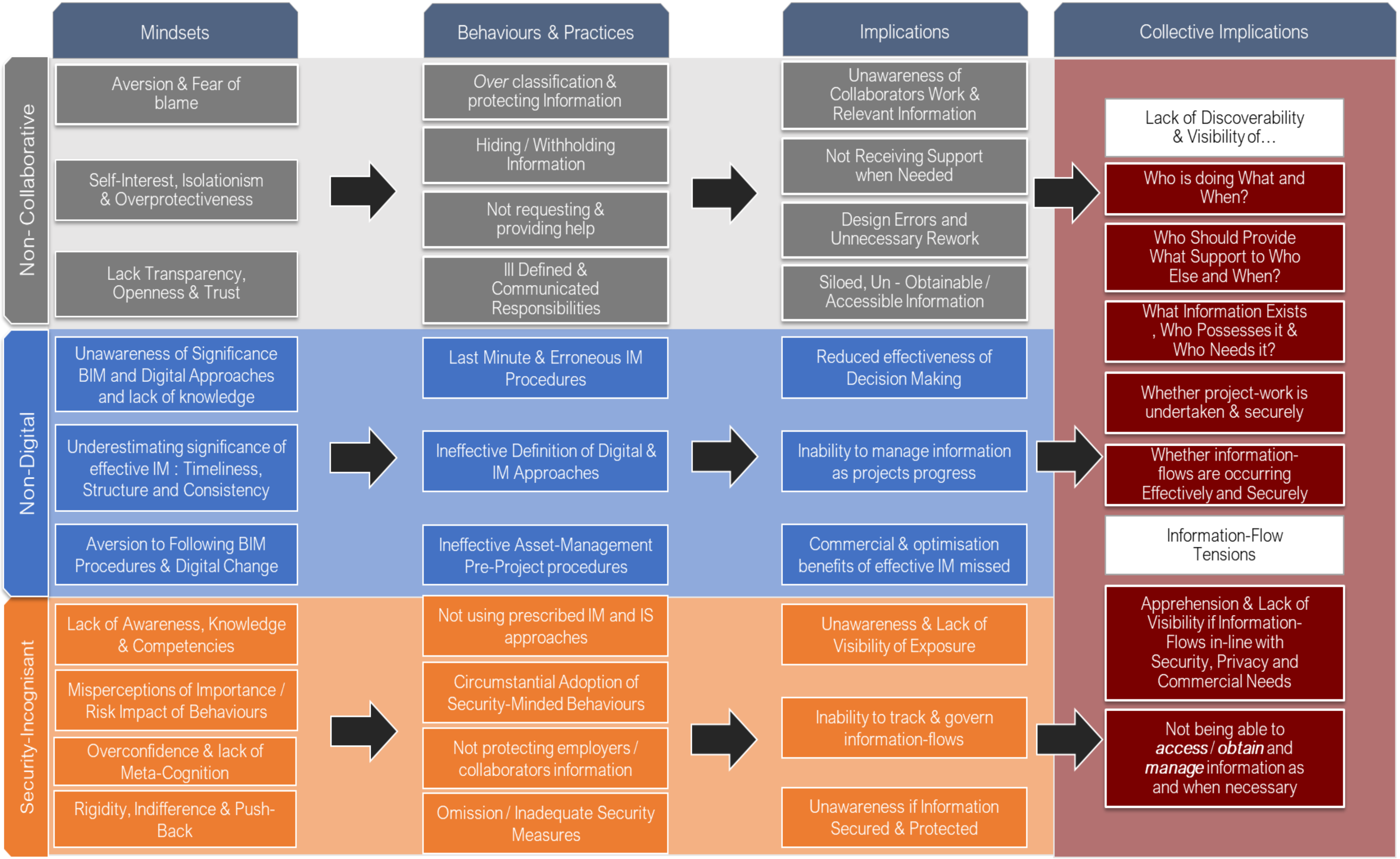
In summary, the implications to secure and collaborative information-flows identified via these three areas are similar; however, the causes originate from different types of attitudes and behaviours. For example, a lack of visibility over information-flows originated from both collaboration averse, and security-incognisant areas.

The collective implications from these three areas are 'confusion, limited visibility, discoverability and awareness' of the following factors of project information-flows (internal and external), and security and collaboration arising therein.

1. What information exists within projects and its workflows?
2. Which actors are working on what aspects of project work?
3. Who possesses, has access to, or has originated what information?
4. Who is able to provide what information?
5. Which actors are obligated to support which other actors, and when?
6. Whether IG, IM and IS aspects of project-work as 'information-responsibilities' are being undertaken effectively and securely?
    a) Whether information-flows as a whole are occurring as necessary for effective and secure collaboration?
    b) Whether information is utilised appropriately in line with the originator's requirements and needs. This includes whether it is secured effectively and appropriately to manage security-risk, privacy and intellectual property concerns?

7. Whether information is being overclassified and if so, is information being overprotected, or intentionally withheld from actors?
8. Actors are not able to access the necessary information when needed. Leading to design errors and unnecessary rework that may have been avoidable.

Figure 4.2 (following page) provides a diagrammatic representation of the issues inter-related within this section.



	Mindsets	Behaviours & Practices	Implications
Non- Collaborative	Aversion & Fear of blame Self-Interest, Isolationism & Overprotectiveness Lack Transparency, Openness & Trust	*Over* classification & protecting Information Hiding / Withholding Information Not requesting & providing help Ill Defined & Communicated Responsibilities	Unawareness of Collaborators Work & Relevant Information Not Receiving Support when Needed Design Errors and Unnecessary Rework Siloed, Un - Obtainable / Accessible Information
Non-Digital	Unawareness of Significance BIM and Digital Approaches and lack of knowledge Underestimating significance of effective IM : Timeliness, Structure and Consistency Aversion to Following BIM Procedures & Digital Change	Last Minute & Erroneous IM Procedures Ineffective Definition of Digital & IM Approaches Ineffective Asset-Management Pre-Project procedures	Reduced effectiveness of Decision Making Inability to manage information as projects progress Commercial & optimisation benefits of effective IM missed
Security-Incognisant	Lack of Awareness, Knowledge & Competencies Misperceptions of Importance / Risk Impact of Behaviours Overconfidence & lack of Meta-Cognition Rigidity, Indifference & Push-Back	Not using prescribed IM and IS approaches Circumstantial Adoption of Security-Minded Behaviours Not protecting employers / collaborators information Omission / Inadequate Security Measures	Unawareness & Lack of Visibility of Exposure Inability to track & govern information-flows Unawareness if Information Secured & Protected

Collective Implications

Lack of Discoverability & Visibility of…

- Who is doing What and When?
- Who Should Provide What Support to Who Else and When?
- What Information Exists , Who Possesses it & Who Needs it?
- Whether project-work is undertaken & securely
- Whether information-flows are occurring Effectively and Securely

Information-Flow Tensions

- Apprehension & Lack of Visibility if Information-Flows in-line with Security, Privacy and Commercial Needs
- Not being able to ***access*** / ***obtain*** and ***manage*** information as and when necessary

Figure 4.2: Socio-Organisational and Technical Barriers

4.4 Barriers to Implementation of Secure and Collaborative Projects

A project is structured upon many different dimensions that represent its security and collaborative readiness. These dimensions are decided upon during the strategic definition and preparation and brief stages ("Building design process," 2021). There appear however to be a number of challenges relevant across different projects at their implementation stages which will be explored during this section of the thesis, pertaining to the following sub-sections.

1. Challenges pertaining to Effective Assessment and Management (Governance) of Security-Risk.
2. Challenges pertaining to Supplier Accreditation and Selection.
3. Challenges pertaining to BIM Requirements Documentation and Planning.
4. Challenges pertaining to Implementation and Governance of Digital Environment and Technologies.

Issues within these areas affect both security-minded projects and those within the broader industry. This involves projects being set-up in manner unrepresentative of its actual needs for secure collaboration. The aforementioned factors also represent barriers common across the board within industry. Furthermore, problems in these areas also contribute to security and collaboration tensions, this may be particularly relevant for security-minded projects or those aiming to be security-minded. The first section to be explored is challenges pertaining to effective security-risk governance.

4.4.1 Challenges to Effective Security-Risk Governance

Relation to themes explored within interview design:

- Security concerns faced and effectiveness of security-risk governance approaches - including assessing and classifying sensitive information and mitigation of security-risk.
- Application and applicability of standards in the governance and management of information, including security-risk governance.
- Tensions of high security-risk / sensitivity on effectiveness of information-sharing and information-management.
- Overly rigorous security practices, and shortcomings in internal and external aspects of BIM collaborative practice.

It is firstly noted that the awareness of security-risk should be more commonly present within security-critical settings as sensitive assets must be protected in line with policies set by regulatory bodies (H. Boyes., 2005). These policies are enforced due to the severity of potential exposure (H. Boyes., 2005). As such, low levels of security-risk appetite are present within such settings. It is therefore pertinent that effective security-risk assessment takes place such that appropriate mitigation and management measures are employed, which align to a project's collaborative needs and requirements. This is the ideal however, and the following sections will explore these factors of security-risk governance (as a combination of assessment and management) within the context of interview findings.

1. Security-Risk Governance Approaches within Security-Minded Projects.
2. Security-Risk Governance Approaches within the Broader AEC Industry.

The first sub-section will explore variances in assessment and management of security-risk in the practices interviewed. This will be followed by exploration of security-risk governance concerns for the broader industry and exploration of baseline-security initiatives. This corresponds to the interview design themes of expert's perception of broader AEC industry security focuses. At an overarching level, the exploration also corresponds to issues identified in **Section 4.3** of security-incognisance.

4.4.1.1 Security-Risk Governance Approaches within Security-Minded Projects

This section explores security-risk governance approaches. Firstly, A6 and A10 noted gaps in the holistic security-risk governance within projects of elevated security-risk. They posed that prior to their guidance within certain projects, security-risk governance was constrained to a sole dimension of security-risk e.g. physical security. Contrastingly, A1, A2, A4, A9 and A10 suggested that projects with elevated security-risk for their built-assets are more focused upon holistic governance, as compared to the broader industry. They did however note other facets of erroneous governance procedures still exist within projects of elevated security-risk, and such issues were faced within the following experts' practices.

1) Large volumes of built-asset information were grouped under a single, overarching security-classification and stored separately within individual information-containers (i.e., BIM Models). (**Experts**: A1, A2, A3, A4, A7 and A8).

2) Information that presented little or no security-risk was incorrectly given an elevated security-classification. (**Experts**: A1, A2, A3, A4, A7 and A8).

3) Information that presented elevated levels of security-risk had not been effectively and appropriately governed. The appropriate security-risk assessment / classification had been overlooked. (**Experts**: A3, A5, A7 and A9, A10).

Points 1 and **2** are expanded upon within the context of A2, A3 and A7's projects wherein entire structures had been assigned a single security-classification tier during early project stages. A3 believed this representative of a 'globalised' security-risk governance approach. A3 further perceived that **Point 2** compounds **Point 1** wherein erroneous decisions may be made for the classification of large volumes of information. This overlaps with issues explored within **Section 4.3.1.1** of actors possessing limited knowledge of security-implications.

High-level governance policies also appear to compound issues of over-classification. Entire **BIM** models within A3's practices were assigned a classification at the level of the most sensitive design-aspect of models as project-level policy dictated. A3 believed these policies were detached from efficiency and sharing motives as only certain aspects of information within their models presented elevated levels of security-risk. Conversely, A4 noted concerns of classified information which may be benign, but which must still be governed in accordance with the classification-level to avoid reputational damages from exposure (See Appendix A.4.1 and A.4.2). The issue is double-sided as information may in some instances be erroneously classified; conversely, actors wishing to access or further share information may not be aware of the reasoning behind classifications.

In contrast to A1, A4 and A4's practices, A2 and A7's practices employed a less nuanced approach where A7 believed: *"It's a case that it's either classified or not, either you can't share the information with anyone or it's not under any sort of restriction".* In other words, A2 and A7's classification approach was not specific to the level of security-risk posed by assets. This factor could in turn limit **IS** potential between collaborators. It also limits assessment as to the degree of security-risk that may be present.

In addition, A2, A3, A4, A9, A10 and A11 posed issues identified via A2, A3 and A7's practices may also be illustrative of other security-critical projects overlapping the built-environment. A1, A2, A3, A4, A6, A7, A7, A9, A10 and A11 thus agreed that asset-information should be classified and separated accordingly to avoid unnecessary reclassification and thus aid IS potential amongst collaborators, as opposed to impeding it. A1 and A4 similarly proposed their approaches now employ in-depth security-risk assessment. A1 stated the following of granular assessment of built assets.

A1: "Rather than project by project, or structure by structure, we try to classify each piece of data individually because it's really onerous if we classify everything at the highest level because of the restrictions in place. We need to make sure we can work reasonably efficiently so we need to understand what data is sensitive and what isn't so sensitive."

A1 believed the aforementioned approach enables (a) precise capture of security-risk and thus (b) separation of information into files of the same sensitivity-tier. Effective separation was crucial for multi-organisational IS as their policies dictated that information of higher sensitivity must be protected on separate network infrastructure. Previously, classification did not represent the actual security-risk posed. This constrained collaboration as they were (a) unable to share information that was actually lower risk or (b) collaborators were required to gain higher levels of security-clearance to access; this issue is further noted in **Section 4.5.1.**

Finally, expanding upon the aforementioned **Point 3** of 'overlooking of sensitives', A7 posed past experiences wherein non-classified information was commonly shared, which actually presented significant levels of security-risk due to a lack of appropriate assessment. A7 provides an example scenario of this having been encountered in A7s practice (See Appendix A.7.1). In contrasting A7's example, A5 similarly believed there was previously little governance over their management procedures even though A5's practices were now aiming to improve their effectiveness and consistency.

Moreover, A7's issues were a clear example of data-aggregation (i.e., security-risk aggregation) issues. A1, A3, A4, A6, A8, A9 and A11 similarly posed it was difficult to understand the wealth of scenarios where aggregated or cross-referenced information may pose inadvertent security-risk. A11 similarly posed attempting to identify all scenarios wherein security-risk aggregation may occur, may in-fact lead to over-cautiousness. These perceptions acting as preliminary considerations of this idea are reflected upon in **Section 6.2.2.5.**

Summary: In summary, experts in the majority perceived that granular security-risk assessment and information separation prior to and throughout the project, is required for precise tailoring of information-security measures in line with actual level of security-risk posed. A1, A2, A3 and A4 perceived these factors especially important to improve their collaborative capacity. A1, A2, A3, A4, A6, A9, A10 and A11 also believed accurately carrying out security-risk assessment practices at project-onset limits the need for reassessment at a later time. Addressing ineffective procedures and ensuring more accurate security-risk governance may however require change in project-policy such that continuous governance occurs throughout projects.

Table 4.4: Security-Risk Governance Themes (Security-Minded Projects including CNI)

Concept #	Key Theme: Security-Risk Governance (CNI)	Expert Occurrences	Total
1.	Information erroneously designated sensitive / higher than appropriate.	A3, A5, A7 and A9, A10.	5
2.	Sensitive information inaccurately classified, or not classified at all.	A3, A5, A7 and A9, A10.	5
3.	Large volumes of BIM data grouped in files given high-level security-classification.	A1, A2, A3, A4, A7 and A8.	6
4.	Security-risk policies detached from operational, efficiency and IS needs.	A3, A4, A7, A8, A9 and A13.	6
5.	Erroneous risk governance impairs secure & collaborative IS (*increasing IS tensions*).	A2, A3, A4, A9, A10 and A11.	6
6.	Resolving tensions requires granular and holistic assessment / classification (project-onset).	A1, A2, A3, A4, A6, A7, A8, A9, A10 and A11.	10
7.	BIM data (within files / groupings) should be assessed / classified independently + atomically.	A1, A2, A3, A4, A6, A7, A8, A9, A10 and A11.	10
8.	Information should be stored in separate BIM models according to sensitivity-tiers.	A1, A2, A3, A4, A7, A9, A10 and A11.	8
9.	Complexities understanding what information represents higher risks (on own / in aggregation), why and in what contexts.	A1, A3, A4, A6, A8, A9 and A11.	7
10.	Information erroneously designated sensitive / higher than appropriate.	A3, A5, A7 and A9, A10.	5

4.4.1.2 Security-Risk Governance within the Broader AEC Industry

It was established in **Section 4.3.3.2** that clients within the broader industry commonly see security-minded approaches as lesser or of non-applicability. This section expands upon issues of client security-incognisance within a project-implementation context. According to A3, A5, A6, A8, A9, A10 and A11, security-incognisance leads to clients not seeking initial security-risk awareness and appetite assessment via specialist guidance. A6, A9 and A11 posed such core issues influence limited stakeholder security-cognisance in day-to-day project-operations. According to A4, A5, A6, A8, A10 and A11, the lack of client-driven assessments also results in potential for project security-risks to exist that neither clients or suppliers are aware of nor prepared to manage.

In particular, A1, A4, A6, A9 and A10 perceived that clients in the broader sector lack in-depth holistic awareness of what particular aspects of their asset's present elevated security-risk, and which associated work and information-flows thus require increased governance. This includes appropriate procurement and governance of appointees to manage these aspects **(Section 4.4.2)**. They further perceived such gaps can influence inadequate set-up of projects to manage the level of security-risk a client may unknowingly, yet in actuality face. A10 also proposed client incognisance of the level of security-risk faced is reflected upon within employer's project information requirement documents (EIRs) discussed within **Section 4.4.3** of what clients ask of their appointees in terms of information-deliverables at project-onset, and ideally throughout the project.

A6, A8, A9, A10 and A11 thereby posited it is essential for inexperienced clients to seek advice from advisory sources to help achieve an initial understanding of security-risk appetite and at least *baseline* capacity in governing security-risk. The aforementioned experts believed a baseline level of security-mindedness is necessary for the broader sector. This is as assets are not required to fall under a CNI or high-profile context to present security-risks to stakeholders such as occupants. For example, A9 stated the following in respect to the need for a baseline level of security-risk governance capacity.

A9: "It's not that all buildings are highly sensitive or require high-security, but we do all occupy buildings and are therefore potentially target. Any building can be a vehicle to create problems - so we do have to be more careful about how we manage our building data".

A9 thus posed the pertinence of baseline security which ties into A6, A9 and A11's beliefs that even owners of assets (e.g. schools, hotels, offices etc) should still be aware of threats posed to their occupants. As identified through analysis of A6's responses, this viewpoint is compounded by increasing security-risks from smart assets / cities perspective of the following factors.

- Increasingly larger numbers of building-systems are interconnected and centrally accessible via advancing technological means such as building management systems (BMSs) and internet-of-things (IoT) (British Standards Institution, 2017).
- Larger volumes of BIM information are accumulated in general, and may be interconnected, and accessible via advancing technological-means (British Standards Institution, 2017).

According to A6 and A10, trends of increasing information interconnectivity, aggregation and accessibility is exploitable by malicious parties to cause harm to occupants if appropriate security-risk governance is not in place. As an example of accumulation, A6 raised concerns of datasets such as 'pattern-of-life' commonly captured for projects with publicly accessible spaces, and that such types of datasets represented vulnerabilities for stakeholders as members of public.

A1, A6, A7, A8, A9, A10 and A11 believed clients are commonly not aware how / what asset-information such as this represents vulnerabilities that should be appropriately governed to limit potential for threat actors in appropriating such information as part of their attack vectors. A7 gave an example of information-sets of fire-safety plans were not appropriately governed in a high-profile project. They also however represented vulnerabilities to broader types of assets. Please refer to Appendix A.7.2 for this example.

These information-sets which whilst generated within the context of a CNI project, also represented vulnerabilities that are also however applicable to other types of assets, and thereby projects that may not necessarily have been considered by stakeholders as elevated security-risk. As such, examples garnered from A1, A6, A7 and A9 represent the security-implications for projects within the broader sector that are not captured, and thereby appropriately percolated as part of security-requirements for the project.

In other words, a project does not need to be within 'high-profile' environments to possess missed security-implications. In respect to growing threats posed within the wider-industry, A6, A7, A8, A9, A10 and A11 believed that future security guidance documentation should convey to less experienced organisations as to *why* a baseline approach (British Standards Institution, 2015) is necessary. A9 and A10 also believed that guidance information must be presented such that senior-roles can easily understand *how* they can implement baseline approaches within their practices with clear procedures to follow. Accordingly, it appears further research is needed as to what a 'baseline' competence entails for the sector as a whole, and of its numerous different types, and tiers of stakeholders (Mamun et al., 2020).

In summary, A6, A7, A9 and A10 therefore believed that regardless of whether a project within the wider industry will face heightened security-risks, clients and suppliers must recognise their obligations to themselves and other stakeholders. This includes upholding information-security and information-privacy. Moreover, clients within the broader industry will not understand the risks posed to them, and the degree of security-minded approach necessary until they have initially sought guidance. As such, the same security-minded principles should guide project-setup regardless of whether a given project has been deemed to be of a prolific nature.

4.4.1 Summary: Section 4.4.1 has explored factors of security-risk governance within the context of both high-profile sectors and the broader AEC industry. Firstly, the analysis from the perspective of projects considered to be high-profile explored differences identified in respect to experts' security-risk governance approaches, and their perceptions thereof. This section of the analysis uncovered specific factors of security-risk governance of built-asset information that represent erroneous or ineffectual approaches that ultimately lead to security-concerns or tension. Of the practices interviewed, there was a significant degree of difference in the effectiveness of the approaches utilised.

On the other hand, the latter section explored the perspective garnered from experts in view of either direct projects they possessed experience / knowledge of within the broader sector, or simply posed concerns of the broader industry given their positions as experts within the field of security-risk governance. Moreover, the purposes of this sub-section of analysis were to capture, abstract and contrast these concerns which had not been fully considered at research-onset. Accordingly, later sub-sectors will explore methods and barriers that have been captured in implementing security-minded projects. This starts with **Section 4.4.2** as supplier accreditation and selection.

Table 4.5: Security-Risk Governance (Broader Industry)

Concept #	Key Theme: Security-Risk Governance (Broader Industry)	Expert Occurrences	Total
1.	Many clients in broader industry do not undergo initial security-risk assessment.	A1, A3, A5, A6, A7, A8, A9, A10 and A11.	9
2.	Many organisations do not appear to possess baseline degrees of competence.	A1, A3, A4, A5, A6, A7, A8, A9, A10 and A11.	10
3.	Clients should seek specialist guidance for risk appetite awareness or baseline competencies (Currently Limited).	A3, A5, A6, A8, A9, A10 and A11.	7
4.	Issues lead to project-environments and asset-operations inappropriate to effectively govern risks presented.	A4, A5, A6, A9, A10 and A11.	6
5.	Clients lack holistic awareness of risks (including vulnerabilities / threats) their projects and assets may face.	A1, A6, A7, A8, A9, A10 and A11.	7
6.	Clients possess limited understanding of corresponding sensitive work / information-flows to focus governance.	A1, A6, A7, A8, A9, A10 and A11.	8
7.	Baseline security-competences required to govern risks for general assets e.g. schools.	A2, A6, A9, A10 and A11.	5
8.	Need to further provide detailed and appropriate guidance document and processes for baseline security.	A6, A7, A8, A9, A10 and A11.	6

4.4.2 Supplier Accreditation and Selection Challenges

Relation to themes explored within interview design:

- Experts view on security-minded principles, values, and mindsets and these are applied.
- Shortcomings in internal and external aspects of BIM collaborative practices adversely influencing security-risk.
- Tensions arising between security-measures and information-sharing.
- Security concerns of oversharing and exposing information and how to remediate these concerns.

This section relates to digital and security mindset gaps of clients discussed in section x and y. Issues captured include clients possessing limited understanding of the competencies they require of appointees and thus not effectively assessing them. This section however discusses enablers, and corresponding barriers in clients utilising awareness of their required competencies to structure their contractual arrangements with suppliers for effective and secure project implementation from a stakeholder perspective. The sections to be discussed are the following

1. Issues Pertaining to Inadequate Supplier Competencies **(Section 4.4.2.1)**.
2. Supplier Selection and Contractual Structuring **(Section 4.4.2.2).**

4.4.2.1 Issues Pertaining to Inadequate Supplier Competencies

All experts believed it crucial for clients to have ensured their suppliers possess appropriate competencies in securely managing information, within both their physical and digital work-environments. This should occur prior to project onset. A2, A4, A5, A6, A7, A9, A10 and A11, however, believed more focus is required of clients in determining the correct overlap they require of appointees Security and Digital BIM competencies. This lack of focus appears linked to gaps of both: (a) holistic client security-cognisance **(Section 4.3.3.2)** and (b) digital BIM knowledge **(Section 4.3.2.1)**. This is especially within the broader industry. As such, A6, A7, A9 and A10 indicated that inexperienced clients face difficulty in properly gauging digital competencies due to insufficient frame of reference of following factors.

a. Limited client understanding over their own role in the management of BIM projects.

b. Limited client knowledge of what effective suppliers' IG, IM and IS procedures 'look like'.

c. Limited client understanding of what constitutes the delivery of high-quality information.

Furthermore, in respect to industry-trends of increased requirements to employ effective and secure digital collaboration, A9, A10 and A11 that prospective suppliers may avoid projects of higher security-requirements due to concerns of (a) personal risks and indemnities associated with data loss, exposure or (b) difficulties in facilitating effective digital operations whilst simultaneously upholding security-requirements. In addition A5 provided that at present, the appointees do not possess any liabilities for exposures (See Appendix A.5.1).

A1, A4, A5, A9, A10 and A11 further proposed that few lead-appointees and their appointment-chains possess long-term experience of managing projects with elevated security requirements. A10 for example stated that the growing need for the broader sector to effectively govern security-risk has caused a 'kneejerk reaction' from organisations over their ability to effectively operate whilst upholding security-requirements (See Appendix A.10.1).

This is in contrast to certain security-minded practices and organisations with long-standing competencies (inclusive of their supply-chains), which are limited in the sector as a whole. According to A6, A9 and A10, this issue factors into the scarcity of overlapping BIM and security competencies within the marketplace for clients to reliably choose from. This in turn influences potential for clients to choose inexperienced / negligent suppliers. The following section will discuss approaches identified from interviews that could be utilised by clients in securely and effectively structuring their contractual landscape of suppliers.

4.4.2.2 Supplier Selection and Contractual Structuring

A3, A4, A5, A7, A9, A10 and A11 posed projects face difficulties in remediating inadequate supplier / appointee competencies as projects are progressing. This is as opposed to detailing appropriate appointments at project-onset. A10 in particular posed that tensions in attempting to introduce already appointed organisations and their teams to new security policies and procedures for physical and digital working (See **Appendix A.10.2**). This is as opposed to ensuring the following factors are accounted for.

a. The necessary policies and procedures are correctly identified and defined at the project-onset in-line with security-risk appetite.

b. Suppliers, individuals, and teams are chosen that are both capable of and will adhere to security policy and procedures.

In regard to approaches clients could utilise to assess and manage security-competencies, A10 posed that client-led definition of security-centric, pre-qualification questionnaires (PQQ's) (Designing Buildings, 2021) were an especially important mechanism to enable clients to achieve the following.

1. Select suppliers who can provide evidence they have completed security-minded BIM projects.
2. Eliminate potential suppliers without the appropriate overlap of BIM and security competencies.

A10 however believed that leveraging security centric PQQs is not common within the wider industry as clients do not fully recognise why and how PQQs should be leveraged in the aforementioned manner. Examples of PQQs identified were requirements for suppliers to possess ISO27001 and 'Cyber Essentials' accreditations (National Cyber Security Centre, 2020a, 2020b).

For example, A9's practices had recently leveraged the cyber essentials accreditation to gather an overarching understanding of: (a) what competencies appointees possessed (previously appointed or tendering), and (b) an understanding of the security-risk that prospective suppliers may themselves present. A6, A8, A9, A10 and A11 believed that whilst numerous accreditations exist that clients can request from potential suppliers, a limiting factor is a lack of client security-cognisance. Simply put, if clients lack knowledge, then they will not know what competencies and accreditations to ask of potential suppliers and why.

Accreditation mechanisms tie into a potential security-risk governance approach at the project-level. This is by splitting procurement between separate lead-appointees to handle different workflows, representative of their level of sensitivity. A10 proposed organisations with specialised capabilities could be assigned to aspects of project-work of a more sensitive nature. Split project-work may pertain to wholly sensitive assets, or specific sensitive aspects of otherwise low risk built-assets. Specific organisations would abide by more stringent security accreditation and working practices. This however allows more open working practices for other appointees and can partially alleviate tensions.

Conversely, A1, A6, A10 and A11 believed they can result in confusion and difficulty in coordinating information-flows of varying sensitivity amongst collaborators. A1, A6 and A10 further believed split procurement approaches are not common with inexperienced clients as they may not be fully aware of their applicability to their practices or lack the overlapping digital and security-knowledge to know how to effectively structure their projects in such a manner. The applicability of this method of stakeholder structuring may also be dependent upon whether the criticality and volume of sensitive project-work necessary to be undertaken can be reconciled with business-cases and costs in designating separate lead-organisations.

Discussion: Finally, it was identified via analysis of A3, A5, A6, A9, A10 and A11 that as different supplier / contractor organisations are employed at different project-stages, their respective levels of security competencies and rigour may differ. Gaps in security may thus exist throughout the project-lifecycle. To address potential gaps posed by varying supplier competencies, A6 proposed clients should perceive their ultimate aim is to secure their asset information in line with operational risks which requires their assets remain unexposed operation. Meeting the aforementioned aim in turn requires clients to think slightly differently by working backwards to identify the necessary security rigour that must be applied by project-actors within each stage, and the appropriate stakeholders that must be employed as the information pertaining to an asset throughout its lifecycle scales over time and actors that have had access to information (See Appendix A.5.2).

Table 4.6: Accreditation and Selection Challenges Themes

Concept #	Key Theme: Accreditation and Selection Challenges	Expert Occurrences	Total
1.	Inexperienced clients face difficulty gauging competencies due to limited understanding / knowledge.	A6, A7, A9 and A10.	4
2.	Few suppliers / contractors w. combined security and digital maturity (supply-chain inclusive) in broader industry.	A1, A4, A5, A9, A10 and A11.	6
3.	Limited competencies in marketplace increases potential for negligent / incognisant appointees.	A6, A9 and A10.	3
4.	Lack of client focus in selecting appointees with competencies to securely deliver quality information.	A2, A4, A5, A6, A7, A9, A10 and A11	8
5.	More client focus needed in determining overlap required of appointee's competencies.	A2, A4, A5, A6, A7, A9, A10 and A11	8
6.	Supplier avoidance of secure projects due to financial / legal risks (exposure), financial viability and difficulties in working.	A9, A10, and A11.	3
7.	Difficulties in remediating inadequate appointee competencies after appointment.	A3, A4, A5, A7, A9, A10 and A11.	7
8.	Clients do not leverage security-minded 'qualification' mechanisms e.g. PQQs.	A6, A8, A9, A10 and A11.	5
9.	Tensions in introducing already appointed actors to need for security-measures.	A2, A3, A4, A6, A7, A8, A9, A10 and A11	9
10.	Split procurement approaches can lead to confusion / difficulty in coordinating information-flows of various sensitivity.	A1, A6, A10 and A11	4

4.4.3 BIM Requirement Documentation and Project Planning Challenges

Relation to themes explored within interview design:

- Applications of standards to promote collaborative working, security, and support security-risk management and information governance.
- How BIM is applied within workflows to support collaborative workflows; how effectively information is managed and shared with stakeholders throughout the project lifecycle.
- Key barriers and approaches and necessary to enabling secure collaboration within security-minded environments and the broader industry.

The ISO 19650 standard-suite (ISO, 2018a, 2018b) guides the development of a project specific BIM strategy that aims to shape an on-time, cost-efficient and value-driven process over the design, construction, and operation of an asset (British Standards Institution, 2013). Accordingly, the client's definition of employer's information requirement (EIR) documentation provides them an opportunity to establish to their appointees the following factors.

1. How they envision their BIM workflows to be structured and how appointees should operate.
2. How they expect appointees to generate, manage and share the project-information that the client requires.
3. The rules and procedures appointees must adhere to throughout the project process.

According to A2 and A7, the EIR creates a project-specific requirement structure that suppliers must meet through their BIM Execution Plan (BEP) which captures more detailed information on how suppliers intend to do so. Linking **to Section 4.3.2**, clients appear to display limited appreciation and knowledge of digital BIM requirements. This section will expand from the perspective of project-level issues of the definition of BIM documentation and requirements.

4.4.3.1 Ineffective Definition of Employer's Information Requirements

Firstly, A2, A6, A7, A9, A10 and A11 believed clients do not proactively define how they wish suppliers to carry out BIM project-processes. They had likewise encountered many EIRs that lacked sufficient detail, clarity and overall project-suitability. These information-planning issues appear pertinent for projects irrespective of security-risk profile. A5, A6, A7, A9 and A10 did however note client security-incognisance within the broader sector implicates ineffective / non-existent security and privacy centric requirements. A6, A9 and A10 noted requirements lack detail of which aspects of the built-asset present elevated security-risks, thus requiring elevated security measures and governance for associated exchanges.

They believed BIM requirements possess gaps of (a) who should do what; (b) how they should do it; (c) why is it important and (d) when do requirements need to be met. These factors also do not reconcile collaboration, efficiency and security project-motives. For example, A6, A7, A9 and A10 believed clients omit crucial detail over information-delivery, simply from an efficiency perspective. A9 for example perceived a common industry issue was the lack of detail for how stakeholders should work and manage information. (See Appendix A.9.2). Expanding on A9s beliefs, erroneous information-requirements results in clients possessing limited visibility of what appointees need to deliver, when and how. This in turn limits clarity of what information collaborators need to generate and share to fit the client's question, whilst achieving the following motives. This is in remaining effective and secure by providing just enough information to appointers and other collaborators, whilst avoiding over generation and sharing of information.

In other words, information-planning that balances a pragmatic view of 'too much vs too little', thereby limiting ineffectiveness, waste or security-risk. A9 indicated clients overlooked a related enabling mechanism to achieve such a motive. This was of Plain-Language-Questions (PLQs) which simultaneously define (a) responsibilities and (b) 'reflection-points' to direct and remind suppliers of the suitability of their planned deliverables based against requirements such as costing, performance and adherence to security-measures. It was also identified clients do not continuously govern their PLQs throughout the project. This should ideally occur however to ensure that appointees fully understand the questions they must answer at each stage and uphold them so that appointees provide answers to them in a sufficient manner. Clients should also work with appointees to adapt PLQs where necessary.

Finally, A2, A6, A7 and A9 also posited significant lack of detail over (a) information-quality; (b) information-validation; (c) accurate project-scheduling and (d) assignees necessary competencies (organisational / professional). This also comprises those professionals assigned without the appropriate overlap between security and disciplinary competence. In A7s practices, such issues led to task work being assigned to unskilled individuals, which actually required extensive experience to accurately capture and validate complex datasets for specific aspects of infrastructure assets, dealing with sensitive variables. In this instance, their inexperience led to the 'last-minute', flawed generation and verification of asset-information which impaired the efficacy and quality of A7s IG and IM procedures. This impeded the client's ability to make informed decisions relevant to the broader project which incurred significant additional costs and delays. It is also questionable whether the security-competence of the assigned individuals was appropriate with respect to the sensitivity of information being managed.

Summary: In summary, erroneous information-planning negatively impact upon the following factors. Firstly, strategic project business cases and governance associated with what information is needed, when and for what purposes. This includes estimated costs and delivery timescales associated with information-planning activities. Correspondingly this impedes: (a) decisions clients and appointees make in progressing processes throughout project stages; (b) the definition of appropriate IG, IM and IS responsibilities and (c) the necessary competencies prospective actors should meet. This includes ineffective capture of what information should be generated and shared amongst stakeholder and to what specific detail.

4.4.3.2 Insufficient Supplier BIM Plans and Limited BIM Regulation

A5, A6, A7 and A9 believed erroneous EIRs are mirrored by similarly ineffectual suppliers BEPs. A6 gave the following example of an EIR of a specialised facility which possessed significant gaps for how information should be generated and managed (See Appendix A.6.7). According to A6s example, such scenarios are representative of clients and appointees being out of sync. On one hand, appointees perceive difficulty in understanding how they can adequately undertake BIM processes and deliver information in line with a client's indefinite needs. Likewise, clients possess limited awareness what information appointees intend to deliver and if it is what they will actually require. Similarly, A2, A6, A7 and A9 indicated the quality of BEPs provided by suppliers was often poor, inaccurate, and not in the correct format. A2, A5, A6, A7, A8, A9, A10 and A11 posed plans possessed the following issues:

1. Devoid of a link between their own appointment-chain capability assessment and how this directs who needs to produce what information, when and how.

2. Unfeasible, not matching the actual time and costs needed to produce information or undergo activities based upon design and management of information, or construction.

Points 1 and 2 further lead to the following issues noted by **Points 3 and 4**:

3. Clients' confusion in managing the flow of the project-schedule and information coordination between themselves and appointees.

4. Not possessing accurate information on *who* is going to be working on *what* and *when* to understand how to effectively structure access to CDEs.

Scenarios that A6 and A7 posed also lead to clients possessing little frame of reference over how suppliers will operate and whether they will manage and share information securely. A6 and A9 were also aware of cases where information within a single BEP was copied across several projects. Copied or non-project specific BIM documentation appears to be a rising concern within the built environment as a whole, still to be addressed. Some cases may be due to negligent suppliers exploiting the lack of knowledge displayed within client EIRs by providing similarly erroneous BEPs. A6 and A9 believed the compounding issues to be limited regulation over the standard of quality and care provided within suppliers BEPs and limited, easy to understand, and relatable BIM educational pieces for clients.

Table 4.7: BIM Requirement Documentation and Planning Themes

Concept #	BIM Requirement Documentation and Planning Themes	Expert Occurrences	Total
1.	Clients do not proactively define how suppliers should undertake BIM processes.	A2, A6, A7, A9, A10 and A11.	6
2.	Client-defined EIRs lacking detail, clarity, accuracy and meaningfulness.	A2, A6, A7, A9 and A11.	5
3.	EIRs – Gaps of 'who', 'what', 'why', 'when' and 'how' over IM and information-delivery.	A2, A6, A7, A9, A10 and A11.	6
4.	EIRs – Gaps over information-quality, validity, project-scheduling and organisational / professional competencies.	A2, A6, A7 and A9.	4
5.	Limited client security-cognisance results in lack of appropriate security-requirements.	A5, A6, A7, A9 and A10.	5
6.	EIRs lacked assessment of what aspect of built-asset / activities present elevated risks.	A6, A9, A10 and A11.	4
7.	Poor supplier's BEPs (pre / post selection) reflect poor client EIRs.	A5, A6, A7 and A9.	4
8.	BEPs – Inaccurate budgets (time / cost) not matching reality to procure / generate information and undergo activities.	A2, A6, A7 and A9	4

9.	Limited shared client - supplier understanding for secure and efficient governance over information-delivery (due to ineffectual planning).	A2, A5, A6, A7, A8, A9, A10 and A11	8
10.	Limited supplier understanding of how to securely undertake BIM processes and deliver information (gaps in client needs).	A2, A6, A7, A8, A9, A10 and A11.	7
11.	Limited client - supplier understanding of: project-scheduling, information-coordination.	A2, A6, A7 and A9.	4
12.	Negligent suppliers may take advantage of gaps in client's EIRs / Project Requirements.	A6, A7, A9 and A10.	4

4.4.4 Challenges to Implementation and Governance of Digital Environment and Technologies

Relation to themes explored within interview design:

- BIM governance and management - project and organisational level digital implementation.
- Efficacy of ICT solutions in supporting collaborative workflows; security concerns of technologies and digital workflows.
- Shortcomings of technologies in facilitating collaborative and secure BIM information-flows.
- CDE capability in securely managing sensitive BIM information. This included whether only those who 'need to know' about sensitive aspects are aware of them.

A project's digital environment includes its technologies and network-infrastructures which facilitate collaborative usage of numerous connected hardware, software, and other technologies. A project's network infrastructure also comprises infrastructure-level security mechanisms such as firewalls (Mahamadu et al., 2013).

Project requirements and policies direct the implementation of the digital environment. This includes the centre of a project's digital environment as the CDE. This should ideally act as a common source of project-information (Eastman., et al 2018). This section will explore a number of factors that limit the secure and collaborative implementation of digital environments. These are the following sub-sections.

1. Limited Project Governance over Digital Suitability of Technologies **(Section 4.4.4.1).**

2. Limited Security Governance over Network Infrastructures and Technologies **(Section 4.4.4.2).**

3. Limited Security Governance over Procurement and Implementation of CDE **(Section 4.4.4.3).**

4. Implications of Unsuitable Contractual Arrangements for CDE Data Hostage **(Section 4.4.4.4).**

Sections 1 through **4** are tightly inter-related and explore different perspective of digital environments. The core perspective explored of the digital environment however is the CDE as a project's lynchpin in facilitating BIM IM and IS.

4.4.4.1 Limited Project Governance over Digital Suitability of Technologies

This section explores issues of the suitability of the digital environment and its technologies where a project's digital suitability is strongly linked to its effective IM and collaboration. Firstly, A2, A4, A6, A7, A9 and A12 believed that requirements do not direct the appropriate implementation of digital environments in line with project-specific needs. A6 and A9 for example believed projects lacked effective business governance over requirements of technological implementation. This can result in unsuitable implementation of BIM IM software. A4 and A6 also believed that some project-practices may however focus on digital capabilities but may side-line corresponding security-requirements of technologies as explored in **Section 4.4.4.3.**

A4 and A7's practices in particular posed previous issues of minimalistic client-side business-cases over what they required their systems and technologies to accomplish which led to appointees adopting inadequate systems; this was also previously noted of A1 and A4s practices.

A7 believed such issues limited their ability to effectively manage and share information. For example, A7 perceived they were previously fairly limited in their approaches to both visualise built-asset information in order to support enhanced design-processes, included the utilisation of information for decision-making.

A2 and A7 believed remediating issues of inadequate technologies required an overhaul of their practice's requirement-capture strategy to instead focus on the optimal implementation of their digital environments. A2 and A7 further believed that supplier incentivisation schemes were necessary so that virtual, augmented and mixed reality technologies were deployed by suppliers to optimise their visualisation and interpretation capabilities of the built-asset data generated. Moreover, it appears that whilst such progressive changes were necessary, they were difficult to achieve in ensuring appropriate consideration of the business-cases behind the utilisation of such technologies. Rather, until the business-cases had been effectively defined, either limited digital incentivisation was seen, or the implementations did not meet the real complex needs of their environments.

4.4.4.2 Limited Security Governance in Implementing IT Infrastructures and Technologies

A3, A4, A7 and A10 posed projects require more focus and governance over the definition of policies to direct secure implementation of network infrastructures. A10 for example was aware of a client within a high-profile sector who possessed inadequate network infrastructure security. This enabled a path of unauthorised access to their entire internal network. A10 believed if this weakness had not been treated then attackers would have been able to compromise their network and by proxy, their **BIM IM** systems and their digital assets.

This was a result of the organisation not implementing sufficient policies over its cyber and information-security programmes due to incognisance of the pertinence of alleviating such risks in their operations. A10 believed such issues were representative of limited focus within industry on the definition of appropriate governance policies for digital environments. A4, A9, A10 and A11 further proposed many organisations are unaware of the security-risks of implementing new technologies within their digital environments and the extra costs associated with implementing technologies securely.

A4 suggested **GIS** software as an example of a technology which possessed a strong business case in their practices to enable improved **IM** and visualisation functions (See **Appendix A.4.3**). A4 however posed it may require significant added costs to implement layers of governance and security to avoid non-authorised access to sensitive **GIS** data. The underlying point A4 raised was that senior-roles and project-managers are more cautious of implementing new technologies once they are aware of costs associated with security-requirements. A4 as an information-security professional was required to make A4's internal practices aware of such requirements. This was in line with regulatory requirements specific to A1, A3 and A4s sector.

A4 noted the key factor is that both the business and security motives are reconciled. Conversely, A3, A4, A6 and A10 perceived engendering such awareness of secure implementation to be difficult where regulation, or at least governance via the client and / or lead-appointees is not present, and many digital environments are set-up without these layers of overlapping, and integrated security and efficacy motives.

4.4.4.3 Limited of Security Governance over Implementation of CDE

Expanding upon security-governance within the context of CDEs, A7, A9, A10 and A12 had experiences of interfacing with clients who were unaware of factors pertaining to the procurement and implementation of their CDEs. Commonly faced issues were limited client direction and governance at project-onset over the CDEs security requirements. A9 and A10 also posed many clients and suppliers were commonly unaware of data-centric conditions for their CDE. This included factors of: (a) physical data storage location, (b) physical data security requirements, (c) physical data backup, recovery and redundancy requirements and (d) cloud data hosting tiers.

A10 for example, believed organisations do not fully understand the concept of cloud data hosting. A basic tenant of 'cloud' hosting is that data is still physically stored within a datacentre and thus subject to security-risks of a physical nature and need for appropriate treatment. A10 suggested some organisations are unaware of such basic concepts which leads to misplaced assurances. Far fewer understand technical and contract-oriented nuances. e.g. what clients service level agreement with their data supplier entails them to, or the tier-level of their chosen data host and corresponding assurances.

A3, A4, A9, A10 and A12 thus believed it is common for both clients and suppliers to be unaware of technicalities of how and where data is being stored. A3 and A4 posed this issue is exacerbated for appointees lower in the supply-chain. A10 believed that this lack of lack of client and supplier awareness of data governance is where malicious parties have or may further exploit in the future.

4.4.4.4 Impact of Ineffective or Unsuitable Contractual Arrangements Pertaining to CDEs

This section explores broader requirements pertaining to CDEs which collate project-information and IPR belonging to multiple stakeholders. Careful contractual consideration is thus required in hosting and configuring the CDE to best accommodate the needs of all stakeholders in view of a project's specific context. The practices interviewed chose distinct approaches as to who was appointed CDE 'gatekeeper'. Within some experts' practices such as A1 and A4, CDEs were hosted and configured by their appointees. Other client-side practices such as A2 and A7s hosted and governed the CDE themselves due to concerns of appointee gatekeeping. A7 linked these concerns to issues leading to injunction of Trant (Client) vs Mott Macdonald (supplier) (Rock, 2017).

The injunction pertains to a project where the lead-supplier was gatekeeper to the information the client required for project progression. A fee-dispute occurred due to a lack mutual understanding between the two parties over the *scope* of project-work to be provided by the supplier. This culminated in the supplier blocking their client's access to the CDE (Rock, 2017; Winfield and Rock, 2018). The lack of mutual understanding itself appears to have arisen due to a lack of clearly defined and agreed upon obligations of the lead-suppliers scope of work and its respective value. Using this injunction as a basis, A7 believed client control and awareness over appointees IS and IM is limited when appointees are assigned gatekeeper. This includes lack of oversight over (a) where and who data is shared with and (b) who they integrate with or conversely, do not integrate with when necessary (See Appendix A.7.3).

Furthermore, A7 believed Trant did not consider the implications of their appointees holding the 'keys' to project-information, and by extension the project-schedule which in turn incurred significant delays. A7 therefore believed a client-side approach better positions clients to: (a) govern smooth adherence to the project-schedule, (b) ensure that suppliers share information effectively amongst each other and ultimately (c) deliver the correct information to the client.

Conversely, a client-side approach may not always however be practical dependent upon the clients digital and security capabilities and competencies. A1 and A4s practices for example had relatively recently adjusted to merging their evolving digital BIM competencies with their prior established security competencies. Their appointees previously appeared to be better positioned in terms of digital BIM competencies to procure and manage the CDE. As such, A1 and A4s previous competencies represents scenarios where it may not always be practical for the client to act as gatekeeper.

Overall, careful and measured consideration is thus required to identify which party is best suited gatekeeper based upon effective definition of project and contractual requirements. A6, A7, A9, A10, A11 and A12 believed that issues cascade due to unsuitable contractual CDE arrangements at project-onset. For example, the aforementioned issues of stakeholder disputes or limited collaboration and security potential. Moreover, the underlying issue appears to be due to erroneous, high-level, and untimely agreements and relatively little consideration pertaining to their appropriate definition; such issues are corroborated by (Winfield and Rock., 2019).

A1, A7 and A9 believed more focus is required in defining contractual arrangements over how project stakeholders should interface with the project's CDE. Experts believe contracts should better define at appointment who possesses the responsibility to host the CDE based on who is best suited to coordinate information and when. A9 believed this needed to be a collective 'hierarchal-tiered' approach which incorporates the considerations and requirements of all lead-suppliers and their own supply-chains. A2, A6, A7, A9 and A10 also posed it pertinent to define liability should issues of data-inconsistency, errors and exposure arise. According to Rock (2018), requirements stipulating factors of on-going localised extraction of BIM data or shared hostage amongst stakeholders should also be considered as a potential means to alleviate data-lockout issues in Trant vs Mott McDonald.

Summary: Overall, a number of factors must be considered in more detail in terms of contractual arrangements. This comprises careful consideration as to which party is legally responsible for physically hosting, managing and governing CDE data. Provisions to ensure intellectual property rights, security, privacy, data access, and data redundancy concerns should also be defined and designated to be upheld amongst partners and appointees. This should comprise arrangements in ensuring that data, for each of the involved stakeholders, is not misused or unprotected, and should comprise further arrangements to cover what occurs in the event of exposure, misuse or loss.

Table 4.8: Implementation and Governance of Digital Environments and Technologies Themes

Concept #	Implementation and Governance of Digital Environments and Technologies Themes	Expert Occurrences	Total
1.	Limited project / business governance over digital-environments based on project-needs.	A2, A4, A6, A7, A9 and A12.	6
2.	Minimalistic client-side business governance of project / stakeholder needs leading to adoption of inadequate systems.	A1, A2, A4 and A7.	4
3.	Systems requirements technologically focused – ignoring security-implications of technologies e.g. GIS.	A1, A2, A4, A6, A7 and A10.	6
4.	Limited security-governance over polices to direct secure network-infrastructure.	A3, A4, A7 and A10.	4
5.	Need to define and reconcile project motives for technology-adoption with their security-constraints / requirements.	A2, A3, A4, A6, A7, A8 and A10.	7
6.	Limited client governance over CDE procurement, implementation, management hosting and decommissioning.	A1, A2, A4, A6, A7, A9, A10, A11 and A12.	9
7.	Cascading issues arising from ineffectual consideration and governance over IM and CDEs.	A2, A3, A4, A6, A7, A9, A10, and A11	8
8.	Need for improved governance over CDE procurement, implementation, hosting and decommissioning.	A1, A2, A4, A6, A7, A9, A10, A11 and A12.	9
9.	Need for improved governance over: scope of work, data-security / privacy and usage arrangements amongst stakeholders.	A2, A4 A6, A7, A9 and A10.	6
10.	Need for legal responsibilities and liabilities / indemnities in the event of data-security / privacy risks actualising e.g. loss of IP.	A2, A6, A7, A9 and A10.	5

4.4.5 Discussion of Secure and Collaborative Set-Up of Project Ecosystems

4.4.5.1 Exploration of Project Ecosystem Concept

Prior to discussion of project-level issues, the project ecosystem concept is denoted. Primary research analysis alongside direct guidance of Simpson et al. (2019) has enabled an understanding of the project ecosystem concept, and its relevancy to this research.

The original meaning behind the concept is with reference to an industry-level lens of an evolving digital built-environment ecosystem (Simpson et al., 2019). The construct via Simpson et al. (2019) is adapted slightly for the purposes of this research to interrelate the secure-collaboration aspect of a given *project-level* ecosystem. This mental construct provides a conceptual entity which explicitly defines how BIM project dimensions are interrelated. For the purposes of this section's discussion, it serves as a visual aid to relate concepts throughout the rest of this discussion. This is depicted within **Figure 4.3,** and thereafter expanded upon.

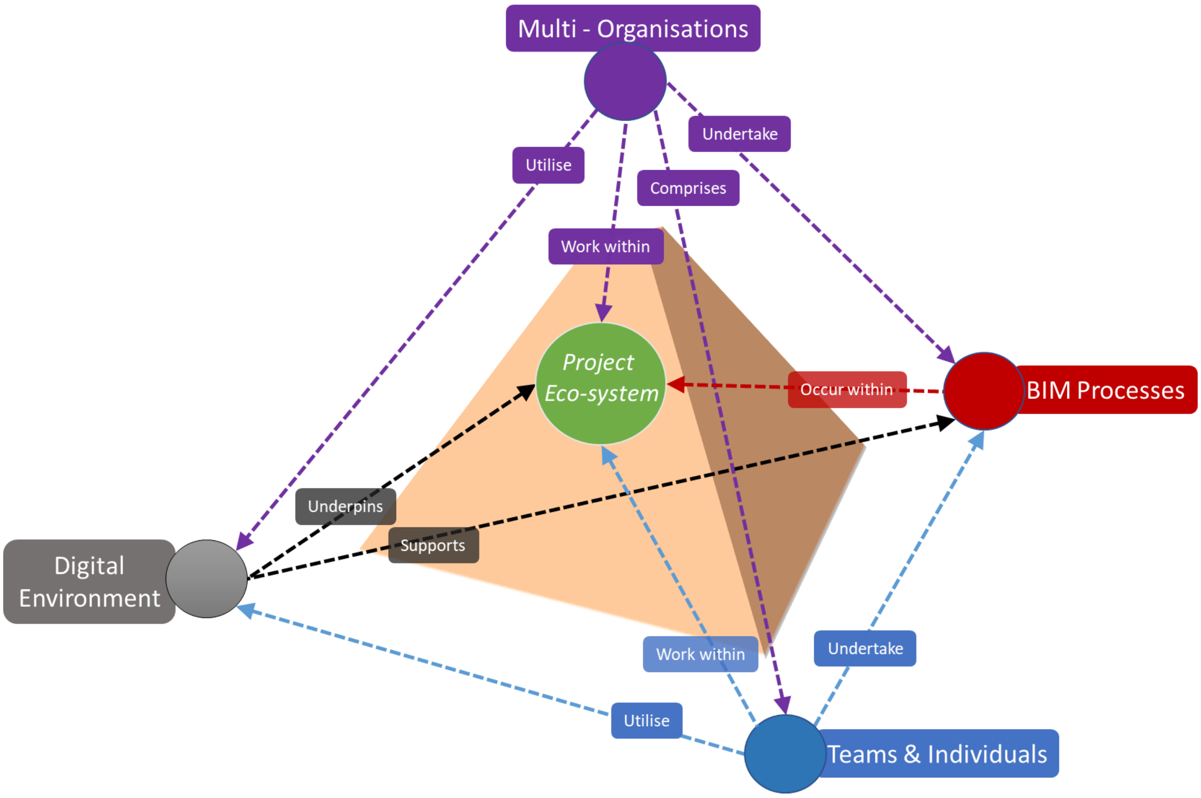


Figure 4.3: Project Ecosystem Concept

In expanding on **Figure 4.3**, a one-of-a-kind BIM project ecosystem is conceptualised as the intersection between the project's BIM dimensions which include:

a. **Multi-Organisational Stakeholders:** These consist of the client's internal project team who interact with the lead-appointee; these lead-organisations in turn possess their own appointment-chains (ISO, 2018a, 2018b). Organisations interact with each other using the ecosystems shared digital environment and technologies for multi-organisational undertaking of BIM processes (Simpson et al., 2019).

b. **Individuals and Teams (Team-Level Actors):** Professionals (within teams) and Teams as a whole work within the project ecosystem and compose an individual organisation. They also utilise an organisations *internal* shared digital environment to undertake granular BIM processes which results in work that is then coordinated at a multi-organisational level.

c. **Digital Environment and Technologies**: The ecosystems digital environment and its technologies are defined and implemented at the project onset for use at an individual, team and multi-organisational level. A digital environment and its technologies support the defined BIM processes and underpins the project ecosystem.

d. **Digital BIM Processes:** A project's digital BIM processes, or workflows are defined at a high-level at the project-onset to work in line with an ecosystem's digital environment. Individuals, teams, and organisations undertake the assigned activities, or tasks respectively.

It is noted that the ecosystem concept, and its dimensions also provides representation to the cultural issues that were identified of **Section 4.3.4.1** of socio-organisational issues as depicted in **Figure 4.4.**

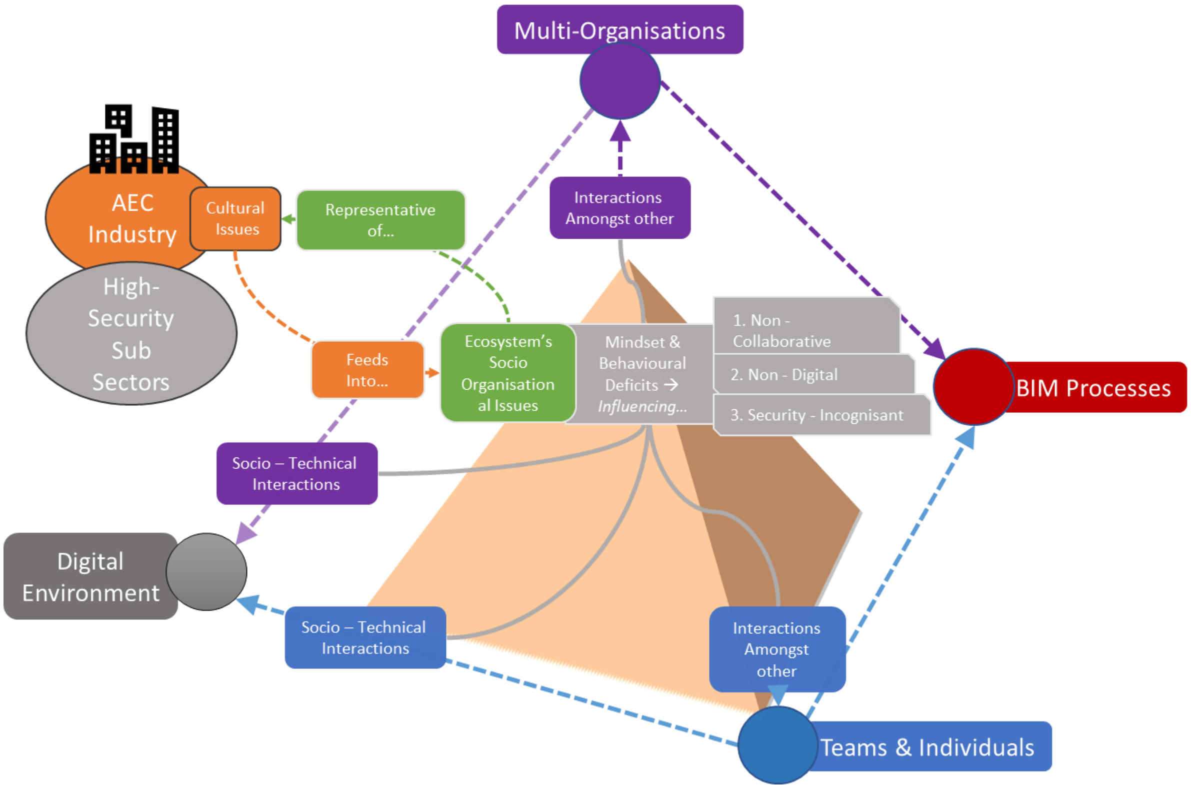

Multi-Organisations
AEC Industry
Cultural Issues
Representative of...
Interactions Amongst other
High-Security Sub Sectors
1. Non - Collaborative
Feeds Into...
Ecosystem's Socio Organisational Issues
Mindset & Behavioural Deficits → Influencing...
2. Non - Digital
BIM Processes
3. Security - Incognisant
Socio – Technical Interactions
Digital Environment
Socio – Technical Interactions
Interactions Amongst other
Teams & Individuals

Figure 4.4: Socio-Organisational Issues (Ecosystem Representation)

As depicted in **Figure 4.4,** the ecosystem also provides a conceptual construct to relate the socio-organisational factors. Similarly, this ecosystem concept will provide context to the factors discussed throughout the following sections. The first aspect is discussed in **Section 4.4.5.2** as cascading issues to the implementation of secure and collaborative project ecosystems.

4.4.5.2 Project Level Cascading Issues

The security-minded practices interviewed, and experts' experiences or perceptions of general projects within industry led to the identification that factors of erroneous or untimely security-risk assessment at project-onset lead to many cascading barriers to secure and collaborative implementation of projects and of its ecosystems. The first issues stemming from ineffective security-risk governance are the following factors:

1) Varying degrees of unawareness of **what** and **where** security-risks are presented of built-assets correspondent to project-work.
    a) This can result in the implementation of ineffective and unrepresentative security measures. **(Section 4.4.1)**
    b) Unawareness appears exemplified within the broader industry. However, projects of elevated security-risk within high-profile environments may also undertake erroneous, untimely, or non-holistic security-risk governance (**Section 4.4.1.2**).

These initial issues of ineffective security-risk awareness, alongside limited client cognisance of what is required from suppliers are linked to issues of structuring of the project, such as ineffective choice of suppliers and the definition of BIM requirements. On the part of supplier competencies and selection is a common issue of client's unawareness of the following factors.

2) What *overlapping*, holistic (a) security and (b) BIM competencies are required from suppliers (**Section 4.4.2**).
3) *Why* accreditation methods are important and *how* they can be used to (a) eliminate potential suppliers unable to effectively manage security-risks; (b) choose appropriate suppliers with the correct security competencies to target specific workflow of higher risk (**Section 4.4.2**).

Limited awareness of *holistic* security-competencies appears to be an especially pertinent issue for inexperienced clients within the broader industry who will likely be unaware of different stakeholder procurement approaches to aid governance of security-risk. Ineffective supplier assessment means clients may be unaware whether their suppliers actually possess the correct BIM and security competencies, or whether they present risks themselves. Concurrently, experts believed that information-planning activities within both high-profile and the broader sector face common issues of defining ineffectual EIRs as issues spanning **Sections 4.4.3** which oftentimes implicates BIM processes in the following manner:

4) Suppliers will possess limited awareness of their own responsibilities in working effectively and securely. They may also possess limited awareness of what their IM and IS responsibilities are to other partnering organisations **(Section 4.4.3.2).**
5) Clients will possess limited awareness of supplier activities or what information suppliers plan to deliver **(Section 4.4.3.2).**

Ineffective requirements lead to ineffective and unsecure information-flows, thereby influencing actor's inabilities to work effectively yet securely. These issues also appear to affect the definition of requirements for implementation of the digital environment technologies. On this point, a number of core issues were identified, which span **Sections 4.4.4**.

6) Lack of project and commercial governance in aligning project needs with selection of technologies results in inappropriate selection **(Section 4.4.4.1).**
7) Lack of governance towards the implementation of the digital environment as a whole (network and technologies adopted for IG) **(Section 4.4.4.2** and **4.4.4.3).**
8) Lack of governance and contractual management towards the procurement and implementation of the CDE (**Section 4.4.4.3** and **4.4.4.4**).

There is therefore questionability whether CDEs are implemented in mind of security, privacy, and collaborative requirements of all involved stakeholders. There is also questionability of whether the contractual methods for gatekeeping of CDE matches the nature and needs of involved stakeholders and their commercial and data-ownership needs but also requirements to effectively manage security-risk. Furthermore, ineffective, and unsecure choice and implementation of CDEs also implies limited transparency over and control over the CDE.

In summary, a number of project-wide tensions stem and cascade from erroneous assessment and management of security-risk which implicate effective and secure project operations. These can be seen to be displayed within **Figure 4.5.**

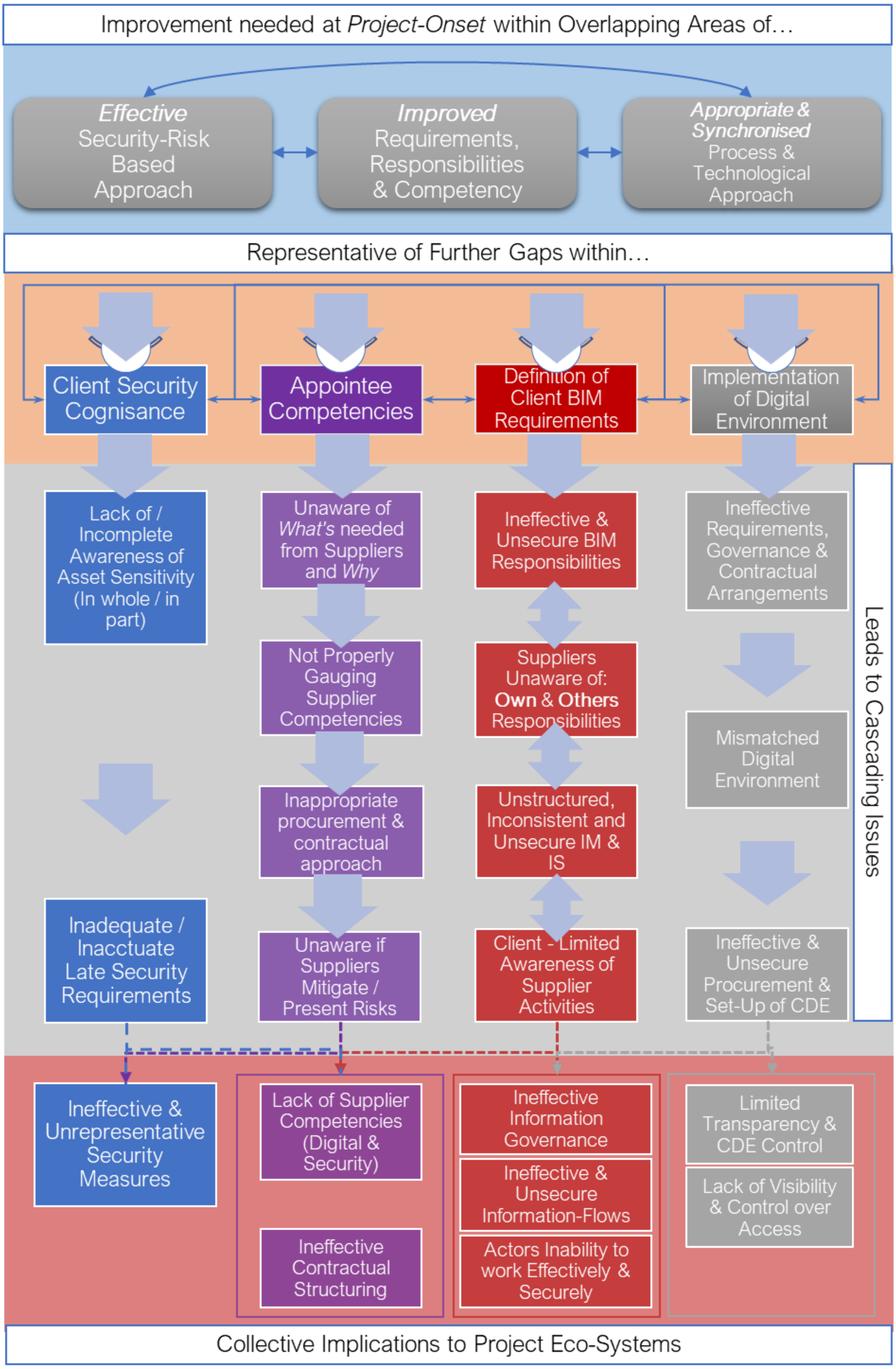

Improvement needed at *Project-Onset* within Overlapping Areas of…
Effective Security-Risk Based Approach
Improved Requirements, Responsibilities & Competency
Appropriate & Synchronised Process & Technological Approach
Representative of Further Gaps within…
Client Security Cognisance
Appointee Competencies
Definition of Client BIM Requirements
Implementation of Digital Environment
Lack of / Incomplete Awareness of Asset Sensitivity (In whole / in part)
Unaware of *What's* needed from Suppliers and *Why*
Ineffective & Unsecure BIM Responsibilities
Ineffective Requirements, Governance & Contractual Arrangements
Not Properly Gauging Supplier Competencies
Suppliers Unaware of: **Own** & **Others** Responsibilities
Mismatched Digital Environment
Inappropriate procurement & contractual approach
Unstructured, Inconsistent and Unsecure IM & IS
Inadequate / Inacctuate Late Security Requirements
Unaware if Suppliers Mitigate / Present Risks
Client - Limited Awareness of Supplier Activities
Ineffective & Unsecure Procurement & Set-Up of CDE
Leads to Cascading Issues
Ineffective & Unrepresentative Security Measures
Lack of Supplier Competencies (Digital & Security)
Ineffective Contractual Structuring
Ineffective Information Governance
Ineffective & Unsecure Information-Flows
Actors Inability to work Effectively & Securely
Limited Transparency & CDE Control
Lack of Visibility & Control over Access
Collective Implications to Project Eco-Systems

Figure 4.5: Cascading Issues to Implementation of Secure and Collaborative Project Ecosystems

In brief discussion of the aforementioned **Figure 4.5**, it appears that based upon findings of expert's practices, it is especially pertinent for high-profile projects to implement project ecosystems with integrated requirements to ensure effective and secure collaboration over the themes depicted within **Figure 4.5** that should be considered in implementing ecosystems. In other words, the full platter is required to ensure effective and secure operations to avoid tensions within security-minded environments.

In terms of the broader industry however, experts were more concerned with ability of clients to assess and govern security-risk to even baseline degrees of capability. This presents concerns of ecosystems implemented without integrated requirements for secure collaboration, or simply whether there are unknown risks left untreated.

Finally, whilst tensions between security and collaboration are more apparent within projects and environments that are security-minded presently, it appears projects within the wider industry may also face such tensions. This is presently where motives of security are hidden over other project-motives. Tensions will further arise as industry is required to move towards ensuring baseline security-readiness. Push-back already appears to be occurring and attempting to employ baseline-security measures without an understanding of the reconciliation that is required between project motives, will lead to similar integration tensions that are faced presently in security-minded environments. Accordingly, factors of project level tensions will be discussed within the next **Section 4.4.5.3**.

4.4.5.3 Project Level Security and Collaboration Tensions

Tensions arise when clients do not leverage requirements integrating collaborative, operational and security needs. These tensions are also correspondent to untimely and erroneous security-risk assessment and management. A project will likely thus face tensions if there are attempts to (a) introduce or (b) remediate security-measures whilst it is underway. In addition to erroneous and untimely security-risk assessment, the following intertwined factors are significant:

a. Untimely or erroneous identification of security-risk in respect to assets and project work.

b. Untimely or erroneous identification of necessary project work to be undertaken.

c. Untimely or erroneous identification of the appropriate stakeholders required to undertake project work and their required competencies.

A trigger for review of the project's security-risk governance approach *should* occur if the aforementioned factors are erroneously / partially captured (CPNI, 2020). For example, A3, A4, A5 and A10 believed triggers due to untimely identification of security-risk leads to back-fitting of security-requirements to project-work. This results in extra costs and delays. A3's practices also displayed high-level and uninformed sensitivity assessment which led to change management of security-classifications so actors could access the necessary information.

Conversely, A1 and A4 faced difficulty in accurately identifying the necessary project-work and corresponding appointees due to limited foresight of these factors at project-onset. Requirements pertaining to these factors influence the logistics for secure implementation of intra and inter-organisational work environments (both digital and physical).

Accordingly, A1 believed that erroneous or untimely capture of requirements may uncover digital environments are unfit for appointees' actual needs. Correspondingly, appointees may be unable to meet the security-requirements of environments and the project more broadly. These intertwined factors impact efficacy of multi-organisational collaboration. For example, A1, A4, A9 and A10 in the position of clients or lead-appointees posed that if they did not accurately identify the security-requirements that appointees (potential or otherwise) must meet to work on the project, then they may be unable to effectively collaborate with some within their supply-chains. Collectively, triggers to change also affect information-flows as it casts confusion and limited visibility over the following factors.

1. Whether the correct levels of security-risk treatment have been applied throughout planned / on-going workflows, and corresponding information-flows.
2. Whether the present implementation of the physical and digital environments can securely accommodate appointees.
3. Whether the contractual landscape of appointees *can*, *will* and *do* apply the necessary security rigour required within environment/s to undertake work effectively and securely.
4. *How*, or even *which* stakeholders should be working on what aspects of project work to effectively govern security-risk whilst remaining effective and collaborative.

In scenarios where change presents doubt, change-management is necessary to ensure security of information-flows. This may not always occur which implies limited visibility of security-risk. If change-management does however occur, it can increase collaboration difficulties such as via the following factors.

5. An increased security-rigour in policies and procedures pertaining to work environments and how stakeholders are required to enact BIM processes. Increased rigour may in turn disrupt how stakeholders are used to working and thereby their effectiveness.
6. Actors not receiving correct information as and when required, to the correct LOI and LOD.

In respect of **Point 5**, A1, A2, A3, A4 and A10 believed unnecessary change-management to cause tensions by changing how actors at all levels are used to working and may result in their push-back. For example, A3, A4, A8 and A10 all perceived tensions may manifest as remediation of policies to fill security-gaps whilst simultaneously creating issues in how effectively stakeholders can access either the digital-environment and information contained therein. This is instead of ensuring actors are introduced to these policies when joining the programme. **Figure 4.6** presents the aforementioned considerations of project-level tensions.

Point 6 on the other hand pertains to scenarios wherein actors do not receive their information and is a core gap to be discussed as part of **Section 4.5**. The following sub-section will expand upon methods of alleviating tensions at the project-level.

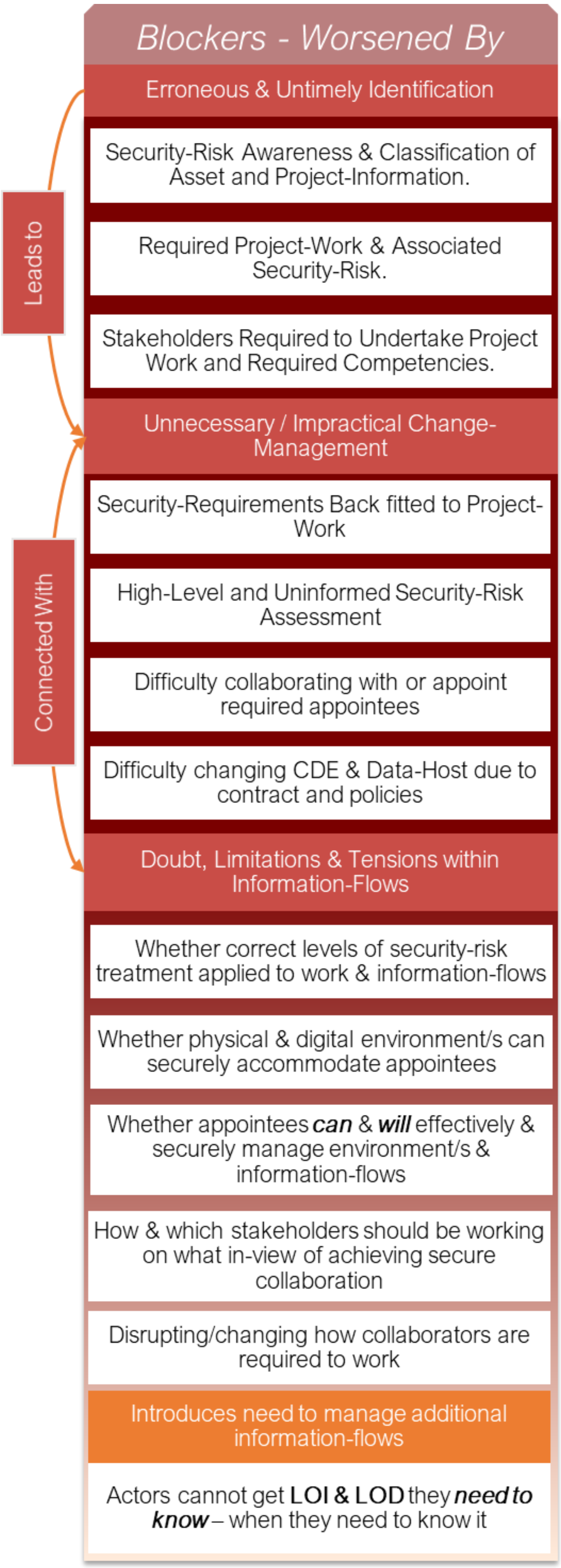

Blockers - Worsened By
Erroneous & Untimely Identification
Security-Risk Awareness & Classification of Asset and Project-Information.
Required Project-Work & Associated Security-Risk.
Stakeholders Required to Undertake Project Work and Required Competencies.
Leads to
Unnecessary / Impractical Change-Management
Security-Requirements Back fitted to Project-Work
High-Level and Uninformed Security-Risk Assessment
Difficulty collaborating with or appoint required appointees
Difficulty changing CDE & Data-Host due to contract and policies
Connected With
Doubt, Limitations & Tensions within Information-Flows
Whether correct levels of security-risk treatment applied to work & information-flows
Whether physical & digital environment/s can securely accommodate appointees
Whether appointees ***can*** & ***will*** effectively & securely manage environment/s & information-flows
How & which stakeholders should be working on what in-view of achieving secure collaboration
Disrupting/changing how collaborators are required to work
Introduces need to manage additional information-flows
Actors cannot get **LOI & LOD** they ***need to know*** – when they need to know it

Figure 4.6: Blockers to Secure Collaboration (Project Level)

4.4.5.4 Managing Project Level Security and Collaboration Tensions

Change-management can be lessened at a project-level if effective planning and security-risk governance procedures are undertaken at project-onset. For example, A10 indicated that identification of varying levels of security-risk faced in a given project, allows clients to tailor security-rigour to workflows of specific appointment-chains capable of effective work whilst effectively governing elevated sensitivities. This is with respect to different aspects of an asset, and thereby separation of work and information-flows of the project. As explored within **Section 4.4.2,** however, this introduces further tensions in needing to govern additional information-flows.

A2, A3, A6, A9, A10 and A11 further believed a core barrier in effectively managing tensions and change-management is client capability of defining proportional and integrated secure collaboration requirements for inter-related dimensions of an ecosystem at project-onset (noted in **Section 4.4.5.1**). A2, A9, A10 and A11 also believed clients require more awareness the implementation of a collaborative, functional, yet secure ecosystem requires the following factors:

1. Integrated project-requirements that overlap inter-related dimensions of project ecosystems. This is as opposed to current disconnected requirements.

Overcoming these issues requires clients to simultaneously leverage knowledge-domains of advisory stakeholders to gather initial awareness of the following intertwined factors.

2. Operational requirements of what is required of each aspect of the project ecosystem to achieve effective and collaborative processes, why and how.

3. Security-risks faced, their *severity* and *placement* respective to project work pertaining to design, construction, and operation of the built-asset.

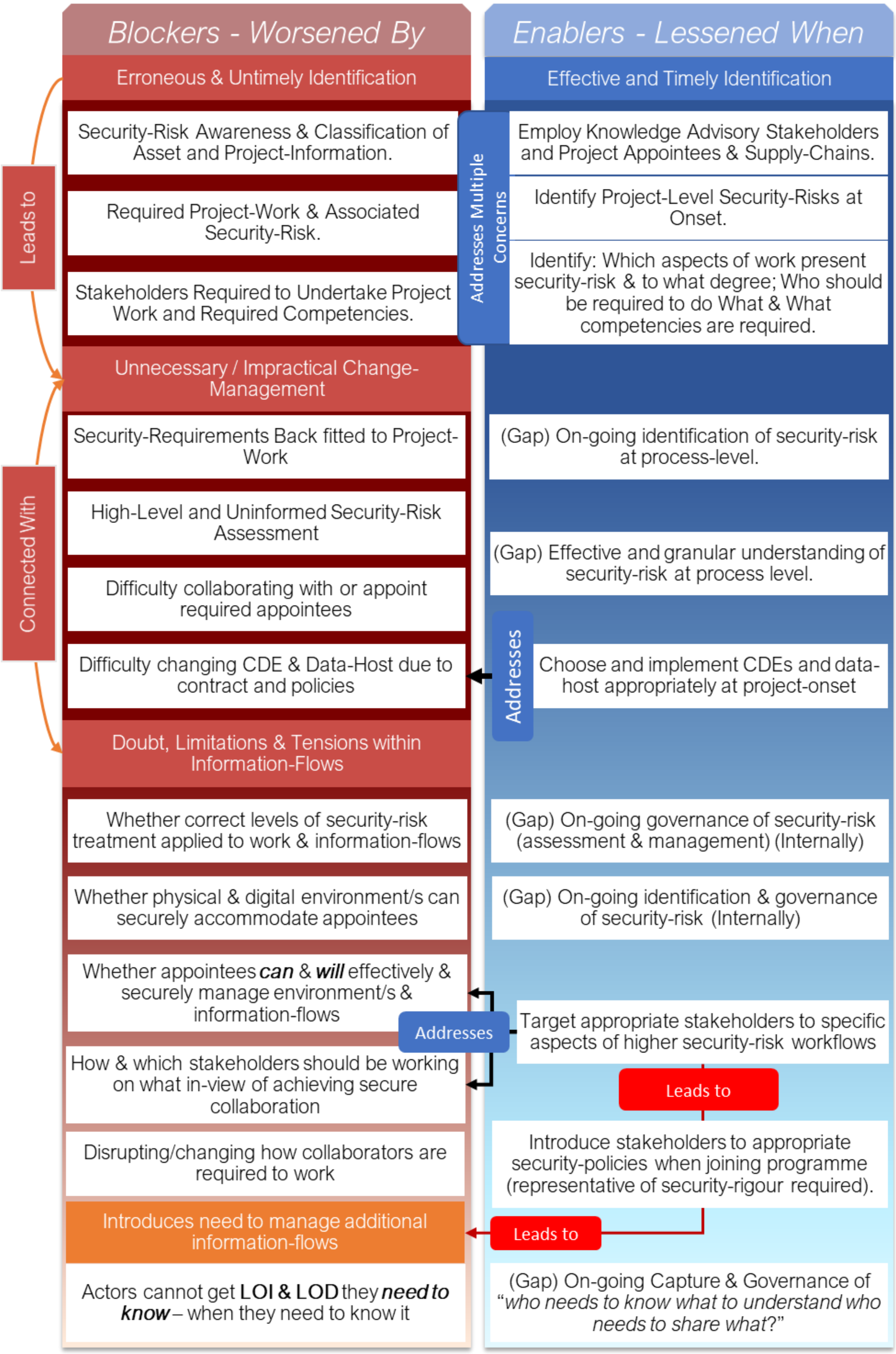
A8, A9, A10 and A11 believed simultaneous awareness of the aforementioned factors provides:

4. An initial awareness of actual security-risks *actually faced,* and the security-risk *appetite* clients are willing to accept.
5. An initial understanding where potential tensions may arise when overlaid with security-requirements.

This provides overlapping project-knowledge of how security requirements must be proportionally integrated with collaborative and operational requirements. This is for each aspect of an ecosystem. In addition, contractual arrangements, and organisational wide policies such as choice and implementation of CDEs, and their data-hosts may be difficult to alter at later stages.

6. As such, factors of an ecosystem, impractical or difficult to alter at later stages are pertinent to possess the correct requirements at project-onset.

Proportional implementation should thereby achieve a balance by ensuring the necessary measures to mitigate security-risk, whilst simultaneously limiting operational tensions accompanying mitigation measures. Based in view of the factors identified via research-analysis, **Figure 4.7** presents the enabling actions that are available to project-stakeholders. This is for both those in existing security-minded domains, or those wishing to enable such projects. Finally, to summarise all factors that were captured regarding these analyses, A10 aptly provided an informative consideration (See Appendix A.10.2).



Blockers - Worsened By

Erroneous & Untimely Identification

Security-Risk Awareness & Classification of Asset and Project-Information.

Required Project-Work & Associated Security-Risk.

Stakeholders Required to Undertake Project Work and Required Competencies.

Unnecessary / Impractical Change-Management

Security-Requirements Back fitted to Project-Work

High-Level and Uninformed Security-Risk Assessment

Difficulty collaborating with or appoint required appointees

Difficulty changing CDE & Data-Host due to contract and policies

Doubt, Limitations & Tensions within Information-Flows

Whether correct levels of security-risk treatment applied to work & information-flows

Whether physical & digital environment/s can securely accommodate appointees

Whether appointees ***can*** & ***will*** effectively & securely manage environment/s & information-flows

How & which stakeholders should be working on what in-view of achieving secure collaboration

Disrupting/changing how collaborators are required to work

Introduces need to manage additional information-flows

Actors cannot get **LOI & LOD** they ***need to know*** – when they need to know it

Enablers - Lessened When

Effective and Timely Identification

Employ Knowledge Advisory Stakeholders and Project Appointees & Supply-Chains.

Identify Project-Level Security-Risks at Onset.

Identify: Which aspects of work present security-risk & to what degree; Who should be required to do What & What competencies are required.

(Gap) On-going identification of security-risk at process-level.

(Gap) Effective and granular understanding of security-risk at process level.

Choose and implement CDEs and data-host appropriately at project-onset

(Gap) On-going governance of security-risk (assessment & management) (Internally)

(Gap) On-going identification & governance of security-risk (Internally)

Target appropriate stakeholders to specific aspects of higher security-risk workflows

Introduce stakeholders to appropriate security-policies when joining programme (representative of security-rigour required).

(Gap) On-going Capture & Governance of "*who needs to know what to understand who needs to share what?*"

Figure 4.7: Enablers & Blockers to Secure Collaboration (Project Level)

4.4.5.5 Barriers and Enablers Discussion Summary

In summary, clients must aim to recognise there are a number of overlapping contextual project factors they must account for and integrate as there is no single solution for secure collaboration. Projects may face collaboration and security tensions to varying degrees if integrated requirements are not defined. The crux of the matter therefore appears to be awareness of the need to take a holistic security-minded approach at project-onset. This should positively influence the project requirements of a number of overlapping areas of implementation of secure project ecosystems.

Alternatively, some of these factors of security-risk governance at a project-level may be difficult to achieve at a process level of information-flows. For example, it appears that changing security-risks may be identified as the project progresses of day-to-day task-work and information-flows. A3 believed this to be especially pertinent for new-build projects where security-risk rise and are identified in line with the LOI and LOD being generated as the project progresses. Where security-risks are unclear, it appears pertinent for methods to progressively identify security-risk. In addition, as discussed within **Section 4.4.5.4**, there are still many gaps at a micro-level information-flows which ties into next section of BIM governance and management.

4.5 BIM Governance and Management Issues

This section explores themes explored as part of the semi-structured interviews centred around issues and limitations of BIM governance and management (processes and technologies). This section also discusses related interview themes pertaining to the overlap between security and collaboration and collates any remaining issues identified.

Exploration of both these areas uncovered unresolved IS tensions centred upon difficulties in making governance-decisions in what actors need to share based upon what other actors need to know. These difficulties are linked to the limitations of current BIM process standards, supporting technologies and their project-specific adoptions. According to A1, A2, A3, A5, A6, A7, A8, A9 and A11, both projects of elevated and lesser security implications adopt similar underlying processes and technologies, extending from the BIM standards-suites.

It was identified through research-analysis that underlying gaps of 'Level 2' BIM methodologies implicates both types of projects. As such, there is a lesser-need to distinguish between the security-profile nature of projects during the exploration of the identified issues and gaps. It is also noted that this section focuses upon a specific theme of the information-management function (ISO, 2018a, 2018b) as a whole, in the generation, facilitation and sharing of information.

4.5.1 Difficulties in Governing the Need to Know and Need to Share

Relation to themes explored within interview design:

- Exploration of tensions between collaboration and security (process and information-flow level).
- BIM governance and management processes. Stakeholders involved in these processes in governing, managing and making decisions over information (sensitive or otherwise).
- Governance decisions over what stakeholders need to know and share. Security specific roles involved in decision-making.

Shortcomings were identified in the application of information-governance policies and procedures that directs information-sharing (IS) on projects. A1, A2, A3, A4, A6, A7, A8, A9, A10 and A11 posed a pertinent governance issue to be the difficulty in identifying and balancing what information stakeholders need to know and need to share in order to maintain effective, collaborative and secure information-flows.

According to A1, A2, A3, A4, A6, A9, A10 and A11, the need-to-know concept relates to information-governance decisions which detail: 'What specific information does a given actor need to know and should thereby receive for their assigned project-work?' The need to share concept pertains to another perspective of such decisions regarding: 'What specific information does a given actor need to share, in line with what *other* actors need to know?'

According to Jonas (2007), both of these concepts are interlinked via an 'Information-Sharing Paradox'. This paradox characterises issues in facilitating secure and optimal information-flows within intelligence-sharing. The paradox also however serves to characterise a BIM governance difficulty that A1, A2, A3, A4, A5, A6, A7, A9, A10, A11 and A13 faced in answering questions of ‘who needs to know what information?' to understand “who needs to share what information?”.

The difficulties associated with answering the aforementioned questions to ensure secure, yet effective information-flows are multi-layered, as expanded upon via the **following Points 1 and 2.**

1. Sharers may possess limited understanding of what information is relevant to any given actor to work effectively. Correspondingly, sharers may possess limited understanding of what information must remain excluded from IS instances based on security-risk profile.

In respect to aforementioned point, a sharer with deficits in knowledge may therefore face difficulty in understanding what should and should not be shared. Receivers of information also face a similar following issue.

2. Receivers possess limited understanding of what information to ask for, and whom to request it from, as they may not know what information exists, and who possesses relevant information.

In expanding upon the aforementioned factor, a receiver may possess limited visibility and discoverability of location, possession, or simply existence of relevant information (Jonas., 2007). The paradox thus represents scenarios wherein both sharer and receiver of information feature limited visibility of each other’s respective responsibilities and informational needs. This paradox also mirrors experts’ experiences of information-sharing tensions in balancing the following motives in governing what actors need to know and share.

3. Achieving effective collaboration and project-work via incentivising and directing optimal information-sharing amongst project-stakeholders.
4. Correspondingly, reducing security-risk by avoiding oversharing amongst multiple stakeholders and thereby reducing potential exposure of sensitive information.

In other words, stakeholders face difficulty in balancing the fine line in over or under sharing. A1, A2, A3, A4, A5, A7, A9 and A10 as client / lead-appointees faced this tension when attempting to plan effective information-exchange requirements. This included identifying what their appointees needed to know based against their assigned responsibilities and what information they as appointers therefore needed to share for their appointees to effectively meet these responsibilities. This is whilst simultaneously managing security, privacy, and commercial concerns. Correspondingly, A6 stated the following in respect to information-sharing tensions.

A6: "One of the interesting tensions around BIM is on one hand it is one thing for a client organisation to want to share lots of information with their supply-chains on the design, or parts of that nature, and on the other hand there's a recognition that you might be sharing a lot of stuff that might have sensitivities associated with it so you might well choose not to share all of it so I think there's an interesting tension there."

Summary: This section has set the scene for BIM governance issues of information-sharing that were identified within interviewees practices. The paradox also appears to characterise information-sharing tensions in being able to effectively 'reconcile the need to know with the need to share' within a BIM context. In respect to this tension, governing-roles (GRs) are currently given decisions-rights over day-to-day information-flows of what internal team-level actors need to know and share amongst each other. GRs are also tasked with governing exchanges at a multi-organisational level. The conceptualisation of a GR is based upon competencies information-manager, information-security and built-asset-security-manager roles should ideally aim to fulfil (Boyes, 2014). These roles arose via discussion of actor's governing roles within semi-structured interviews. They will be referred to as governing-roles (GRs) whilst noting current competencies in industry may not yet fit the ideal gap that GRs would aim to fill. The following section will expand upon specific difficulties GRs face governing information-flows.

4.5.1.1 Complexity of Information Governance Decisions

This section explores difficulties **GRs** face in making decisions pertaining to what actors need to know and share in relation to their assigned work. A secondary theme of the interviews is security-risk governance. Firstly, A1, A4, A9 and A10 believed some decisions are relatively straightforward if they are either a 'yes or no'. I.e., whether an individual meets the necessary security-clearance to access information of a given tier of sensitivity-classification.

The difficulty and complexities are however in the appropriate governance and thereby classification of information. A1 and A9 also posed it pertinent for stakeholders to appropriately identify which suitable individuals require clearances to avoid delays in their access. A9 however posed for example that it is difficult at project-onset to infer who will need what access, and what information is going to be sensitive.

A4, A5 and A9 also note some organisations within high-profile settings elevate the security-clearances of large numbers of individuals. This is to ensure they possess a sufficient number of security-cleared individuals to work on sensitive aspects of the project's workflow. A4, A5 and A9 however believed this wasteful as well as counter-intuitive to security by providing clearances to more than the minimum number of individuals necessary.

Unclear Governance Scenarios: A1, A2, A3, A4, A6, A7, A8 and A9 further believed other scenarios are more complex as it is sometimes unclear where security-risks may arise from actors combined access to information-sets. This issue compounds previously explored aggregation issues (**Section 4.4.1.1**).

A1, A2 and A4 believed the underlying governance principle to avoid such scenarios was to ensure that **IS** occurs on a need to know and share basis. Application of this principle governs security-risk by ensuring precision and relevancy, thereby avoiding over sharing / access.

Conversely, A1, A2, A3 and A9 perceived it was difficult to consistently apply the principle to mitigate security-risk whilst simultaneously ensuring optimal sharing / access. This is because it requires GRs to balance the following considerations when making decisions.

1. The minimum LOI and LOD that *needs* to be shared to allow actors (internal and external) to remain effective vs the maximum that *can* be shared to support further optimal work.

Decisions to the aforementioned question *must* also remain in line with clearances of the actor in-question, whilst ensuring relevancy to an actor's need to know. As such, decisions further comprise understanding of the following factor.

2. What LOI and LOD is (a) irrelevant and may pose security-risks if inappropriately shared whilst also considering (b) what relevant to many different actors.

In other words, A1 and A9 perceived difficulty is because GRs require deep understanding of what task specific LOI and LOD need to be shared / accessed by many actors (internal and external) to maintain security, but also ensure their effective work. As an example of balancing the aforementioned considerations, A9 posed the need to take a pragmatic atomic approach in protecting vs sharing data (See Appendix A.9.3).

Governing Irrelevant and Sensitive Information: Expanding upon the aforementioned point of irrelevant information, A1, A6, A9, A10 and A11 provided similar hypothetical examples of filtering information irrelevant to the receiving actor, which is also sensitive. A1s example was an individual responsible to install cabling within a sensitive security-wall protecting other vulnerable features of an asset (e.g. plant room).

The individual does not however need to know their work pertains to a security-wall. A1 thus posed the individual should be given the minimum relevant LOI and LOD to work effectively. In the context of this example, A1 posed this would be simple geometric and space-positioning data pertaining to the wall to enable the installation. The following points however detail technicalities of dealing with BIM data that further characterise complexities based on A1s example.

- Information serving to identify the wall as a physical security-feature such as reinforcement values or its relation to other assets being protected should be filtered from the actor's access if they do not need to know about it.

- This may include information directly pertaining to the sensitive assets or indirectly via other spatially and / or semantically related assets. Related assets such as rebar within the wall would *inherit* the security-rating of the security-wall due to its *spatial, and / or semantic relationship.*

The aforementioned is an example of a component not being sensitive in and of itself outside the spatial context of the wall. The rebar is however (a) *contained within* the spatial context of the wall, and (b) its reinforcement values may imply (i.e., semantic information) a specific wall serves a physical security-function of another sensitive facility space. In other words, information which is sensitive by association must also be identified and filtered as part of decisions. Such information may provide insight into the wall's physical security function, thereby informing actors (without a need to know) of its security-function, even if the GR has removed such labelling. A1 noted such nuanced decisions were necessary in their practices.

The aforementioned is simply an example, and other project-specific scenarios may arise in determining at an atomic level where sensitivities or factors that may imply sensitivity by association may arise. The latter subtitle however considers the second aspect of the equation in governing relevancy, and thereby suitability. This was noted in the aforementioned **Point 2b.**

Governing Relevant Information: In ensuring optimal relevancy, suitability and effectiveness of IS / access, A1, A2, A4, A9 and A11 proposed further difficulty in understanding subtleties surrounding what information may further support the optimal work of external collaborators, thus relevant to their need to know. A1 and A2 believed this pertains to providing additional information-sets pertaining to the design, or increased LOI and LOD towards information-sets already identified as necessary. A1 perceived making optimal decisions of what information to provide to internal / external actors was not straightforward, linking this to the 'need to know' principle and the degree of foresight needed to properly apply it (See Appendix A.1.3).

A1 further posed that improve the underlying decision-making processes pertaining to IS and being able to better capture a wider perspective, or mapping of the design information-needs of actors within the BIM and design fields (See Appendix A.1.4).

Summary: In summary, A1, A2, A3, A4, A5, A7, A8 and A10 believed that whilst their practices faced difficulty in governing what specific LOI and LOD on assets presents sensitivities, they also believed that organisations with less security-experiences may face far more difficulty. A1, A3, A4 and A9 further posed that even though their GRs held security-competencies to make pragmatic decisions, their sharing capabilities were limited by being required to filter and separately manage sensitive by association information as discussed within **Section 4.4.1.1** and expanded upon within **Section 4.5.2.5**.

A1 for example posed that as opposed to the rebar in the example which may indirectly be associated with reinforcement values, a light-fixture for the wall holds no security-risk but must be filtered into a distinct container alongside sensitive information. This issue however also represents joint process and technological limitations of CDEs as discussed within **Section 4.5.2.4**. Overall, there are many complex factors that require consideration in making informed and pragmatic governance-decision. The next accompanying **Section 4.5.1.2** will also introduce issues of uninformed decisions.

4.5.1.2 Issues of Uninformed Governance Decisions

As discussed within **Section 4.4.3**, erroneous BIM documentation influences difficulties in making informed governance-decisions. Moreover, GRs may be unable to freely defer to the actor in question (who requires information) as to what they need to know and thus what they should access / receive.

A1, A2, A3, A9, A10 and A11 proposed that GRs make decisions over what other actors' access in line with their own perceptions of their information-needs. A9 in particular believed these decisions may be potentially one-sided as GRs must to an extent speculate what LOI and LOD other actors will need to know and share. According to A6, A9 and A10 this is of particular concern where security clearances, and competencies are required to avoid exposure or misuse of sensitive information.

Such decisions require an additional degree of security-mindedness. Correspondingly, A9 noted the following whereby decisions are difficult due to their one-sided nature without a complete view of the information-receivers needs, whilst also having to keep in mind the clearances of actors and corresponding security-risks presented by information (See Appendix A.9.4).

A2 and A13 also posed an example of uninformed decision-making. A2 possessed experience of making governance-decisions as to whether access to design-information should be granted. A13 on the other hand spoke from the perspective as an individual requesting access on the same project as A2. During a particular instance where A13 required access to design-information, the period to decide whether access should be granted exceeded the time A13 possessed to complete the task. A2 noted in respect to A13's issue that roles within the project's upper hierarchy made decisions over granting access which A2 proposed may not necessarily be the most informed to make decisions. A2 indicated to A13, that the decision-process lacked the *localised* team knowledge over whether technical design-data is relevant for practitioners (See Appendix A.2.4).

Section 4.5.1 Discussion: Different motives must be simultaneously balanced when making decisions pertaining to instances of sharing and access instances. These should aim to be pragmatic and balance the need to share detailed information for effective collaboration, with the level of security-risk present. A9 and A10 believed there is a need to balance the minimum and maximum LOI and LOD. For example, instances of sharing sensitive information should filter any detail that is sensitive, or sensitive by association. However, the minimum that actors need to know remain effective should still identified in line with security-clearances, thereby achieving pragmatic governance-decisions of what *can* and *should* be shared / accessed.

Achieving a balance between over / under sharing through effective governance-decisions appears essential for secure-collaboration. There however appear to be difficulties in determining the precise project-specific LOI and LOD to be shared respective of both collaborators needs and management of security-risk. Furthermore, it was identified there is a link between the locality of the decision-making processes and the 'informedness' of those making decisions on behalf of other actors. This factor influences the appropriateness and accuracy of governance-decisions of what actors need to know and share.

A gap therefore appears to be the need to facilitate targeted and informed decisions by actors within the workflow with the most informed knowledge. The next section will explore process and technological limitations to making such optimal governance-decisions in terms of balancing the need to know and share and ensuring secure and collaborative information-flows.

4.5.2 BIM Processes and Technology Limitations

As discussed in **Section 4.4.3**, BIM information-planning requirements are commonly erroneous, contributing to issues of ineffective and unsecure IG, IM and IS processes. It was also identified from A1, A2, A3, A4, A5, A7 and A9's practices and cross-referencing of BIM standards that barriers exist in enacting secure collaboration which pertain to: (a) the limitations of the standards themselves; (b) how they are currently adopted and (c) the technologies underpinning BIM processes. These themes were discussed as part of the interview design.

A1, A2, A3, A4, A5, A7 and A9s project implementations of level 2 BIM approaches were analysed which included how they implemented BIM methods of information delivery plans and responsibility matrices. Other related themes from the research design to be discussed are in respect to information-governance over chains of appointed organisations, data-access and expanding upon sensitivity-issues. This section will therefore discuss the following sections.

1. Limitations in capture of requirements and responsibilities **(Section 4.5.2.1)**.
2. Need for atomic information responsibilities **(Section 4.5.2.2)**.
3. Need for interlinked responsibilities **(Section 4.5.2.3)**.
4. Need for improved information governance focuses **(Section 4.5.2.4)**.
5. Difficulties in defining and governing security access policy **(Section 4.5.2.5)**.
6. Difficulties in governance and coordination of sensitive information **(Section 4.5.2.6).**

4.5.2.1 Limitations in BIM Information Planning Capture and Enablement

Within BIM workflows, actors are both responsible to, and dependent upon others for information (Singh et al., 2011). As such, actors are simultaneously seen from the capacities of (a) relying upon the information-outputs of sharing actors and (b) fulfilling the information-needs of receiving actors. BIM information-flows are therefore tightly knitted, and implicit interdependencies are created between adjoining sequences of work (Singh et al., 2011). Correspondingly A1, A2, A3, A5, A7 and A9 indicated the following of information-planning norms.

- Information Requirements: The capture of intra-organisational responsibilities pertaining to the generation, management and sharing of high-level elements of the built-asset (e.g. MEP systems) via file-based information-containers.
- Responsibility Matrices (RACI): The capture of overlapping responsibilities in terms of which organisations have a responsibility to coordinate what high-level (Sheen, 2015) element of the design at a fairly abstract LOI and LOD.

In respect of the aforementioned norms, A2, A3, A5 and A7 believed project-knowledge resources mainly captured inter-organisational responsibilities of which organisations are required to generate and share high-level aspects of the design. A3 and A7 for example perceived their RACIs captured when their lead-appointees were required to deliver information. They perceived such norms usually mean responsibilities are high-level of which organisations are to generate and push exchanges of information-sets of high volume and complexity. These bulk exchanges also only occur at distantly spaced points in the project-schedule (Succar, 2009).

A1, A2 and A3 believed these factors mean organisations possess limited awareness whether the correct LOI and LOD is shared in line with the receiver's information-needs. A2 and A9 also believed there is a lack of visibility and governance over sharing, and corresponding uncertainty whether exchanges have resulted in exposure. It was also understood from A2 and A5's practices that organisations appear to possess vague awareness information is needed to and from them to share / federate certain types of design-model (See Appendix A.5.3).

Discussion: These factors relate to limitations of current processes that BIM standards promote, how they are implemented and also of further issues such as push and share everything mentalities / procedures. These limitations present difficulties for collaborators to make pragmatic and informed governance-decisions over what project-specific information needs to be shared. For example, responsibility matrices provide abstract approximations of the LOI and LOD required at particular stages. The following sub-sections further explores how these issues could be rectified by advancements in the underlying process and technological approaches. Such factors along with further implications of limitations are collectively discussed within the following sub-sections.

4.5.2.2 Need for Atomic Information Responsibilities

A1, A2, A3, A4, A7, A9, A10 and A11 believed there is an increasing requirement to capture atomic task-level responsibilities and corresponding information-needs in generating, sharing, and accessing atomic information-subsets. They indicated the definition of atomic information-requirements enables the capture of the precise LOI and LOD internal (team / individual) actors need to know in effectively, yet securely undertaking their atomic responsibilities. They believed this in turn would improve information-planning for effective and secure information-flows. A1 for example posed task-level planning would improve rigorous conceptualisation of information-needs in-line with security-constraints (See Appendix A.1.5).

A1, A2, A3 and A9 further believed that capturing atomic that comprise BIM workflows would allow collaborators to precisely plan which teams should generate and share what LOI and LOD and for what purposes. A1 in particular believed it would compel their internal practices and their appointees GRs to carefully consider what LOI and LOD is actually relevant for internal actors to generate, share and receive in line with captured task-level responsibilities. A1 proposed this should in turn enable GRs to identify and remove sensitive / irrelevant information (from exchange / access) more easily.

Discussion: It appear the planning of atomic information-exchanges should also provide inter-organisational collaborators deeper insight of what their partners need. The sharer of information therefore better understands, to thereby govern, what specific LOI and LOD to share in view of their partners information-needs. This however requires inter-related internal actors to firstly define and communicate their responsibilities amongst each other. This is however inhibited by a number of factors which are expanded upon within the next section.

4.5.2.3 Need for Interlinked Information Responsibilities

This section will explore the need for atomic interlinked responsibilities based upon issues captured and experts' requirements. For example, A2, A3, A5, A7, A9 and A11 perceived that capturing the interlinkages between collaborators information-responsibilities was necessary for secure collaboration. This was such that their BIM project processes captured: *'who has a responsibility to share what information, when, to who and for what purposes?'*.

Recent BIM standards (ISO 2018a, 2018b) mirror the aforementioned experts' beliefs and promote that interdependent overlaps / interdependencies (IDs) between atomic tasks of collaborators and their internal actors should be iteratively captured during the planning and enactment of BIM processes. A2, A3, A5, A7 and A9 however captured overlaps in responsibilities via static responsibility matrices which appear ill-suited for BIM flows consisting of evolving responsibilities and information-needs (Singh et al., 2011).

Similarly, A2, A7 and A9 further perceived project-knowledge of IDs of their team-level actors is generally not effectively captured amongst organisational-level collaborators. This is due in part to project-process complexity and limited BIM and digital competencies. Based upon analysis of A1, A2, A3, A4, A5, A7 and A9's project practices, this issue appears to manifest in the following manner.

1. Ineffective capture and communication of atomic responsibilities and information-needs *throughout* an appointment-chain. This also impedes the effective communication of IDs *across other* appointment-chains (where multiple lead-appointees present).
2. Collaborating organisations therefore possess limited mutual visibility and understanding of what LOI and LOD other organisations need to know and at what points in time. This in turn limits understanding of *when* and *which* of their team-level actors has a

responsibility to generate and share *what* specific LOI and LOD (in view of other collaborators needs).

The aforementioned factors contributed to difficulties in A1, A2, A3, A4, A5, A7 and A9's practices of fully understanding what collaborators 'needed to know' as much information was of potential relevancy in supporting optimal work. However, only after the presumed necessary information had been shared was it, in some instances, identified what collaborators actually required. Full alignment between collaborators also only occurred after extended periods of time. This also appeared due to norms of organisational-level responsibilities which are commonly met by exchange of large volumes of information (i.e., file-based information-containers).

A1, A2, A3, A7 and A9 also noted majority of work had to reach certain levels of internal suitability before coordination. This led to high information-sharing 'latency' before collaborators received and were made aware of the suitability of received information. Push-based norms also led to organisations providing information with a one-sided understanding of the needs of partners internal actors. According to A1, A2, A3 and A4, collaborators may make requests for information (RFIs) if information is not suitable after information is received. However, providing stakeholders may still be unaware whether oversharing has led to exposure. This is due to a lack of, or limited, effectual internal security-risk governance prior to exchanges.

Discussion: The aforementioned findings are based upon A1, A2, A3, A4, A5, A7, A9 and A10's processes which were based upon high-level interconnectivity norms. A11 as an independent specialist also provided similar insights, whereas A12 provided insight from a CDE vendor perspective. These factors influence issues in appropriately governing information-flows for security and suitability.

A1, A2, A3, A7, A9 and A11 indicated such factors and scenarios represent gaps in mutual visibility and recognition between collaborators of IDs in their work, and by extension, their respective needs and responsibilities. This links to an **IS** tension of limited mutual visibility of collaborators task-work. Correspondingly, there is limited recognition of a pragmatic **LOI** and **LOD** that should be shared (ensuring security and suitability) in view of evolving responsibilities and associated needs. As such, gaps between collaborators appear to influence under or over sharing and there is limited guarantee of relevancy and specificity.

Furthermore, it was noted interdependencies (IDs) do not appear to be effectively captured due to static / document-based norms. A2, A3, A7, A9 and A11 corroborated in perceptions that CDEs do not currently provide for digital capture of an atomic project-process resource to thereby inform team-level actors of their needs and responsibilities to others at this level (internally / externally).

A1 and A9 also noted little verification whether exchanges mitigate security-risk whilst appropriately meeting collaborators needs. Research by Beach (2019) has also posed an inherent difficulty validating the suitability of digital project-data in view of document-based requirements. Vendor's CDEs also generally do not appear to support functionalities for directed atomic exchanges between team-level professionals. This is expanded upon in **Sections 4.5.2.3**. In respect of issues and gaps characterised, A1, A2, A3, A7, A9 and A11 supported joint process and technological change via the following overarching needs. This pertains to planning, enabling, and governing, atomic and interconnected information-flows.

1. Digital methods to capture, coordinate and govern task-work IDs between team-level actors in what task-specific information professionals need to know and share (from / to who) and when.

    a) This comprises methods for tighter connectivity and visibility amongst such internally / externally related actors. Methods should in turn reduce gaps in understanding overlaps between professionals' task-work and 'bridge' their understanding quicker.

    b) Increase in IS specificity via functionality for atomic exchange and correspondingly, reduction in IS latency between collaborators.

2. Digital methods to verify whether atomic exchanges mitigate security-risk whilst meeting receivers' information-needs. It is inferred this should occur before information is shared.

    a) Digital methods to facilitate on-going governance of where accumulating LOI and LOD prior to external IS may present security-risk.

3. Methods to better identify what information is relevant in the wider context of BIM disciplinary professionals throughout project lifecycles and when.

A1, A2, A3, A4, A7 and A9 supported ideas could manifest in an evolving digital structure of ID tasks. A3 in particular noted capturing the links forms an interlinked and atomic 'tree' structure of all activities, their atomic tasks and their interrelations that evolve over time (See Appendix A.3.6). It appears such an approach could provide enhanced visibility, control, and traceability in governing complex inter-related processes. This would in turn aid understanding between collaborators of the required outputs at an atomic task-level in view of receivers needs. A2 and A3 perceived it could also enable GRs improved governance over where exchanges may present inadvertent security-risks that individual internal actors may be mutually unaware of due to specialisations. A3 provided an example of MEP engineers responsible for separately designing fire-prevention and gas systems. The respective engineers may be unaware of vulnerabilities the combined design may expose when shared externally.

A1 further believed that governing atomic exchanges should include a degree of semi-automation such that planned task-based information-exchanges are only released after validation by a GR that a receiving organisations team actually needs to know the information. This is as opposed to A1, A2, A3, A4, A6, A7, A8, A9, A10 and A11s views that sharing typically occurs without such governance and validation. A1 stated that verifying exchanges in terms of both security-risk governance and suitability for the receiver's needs, before allowing a response would ensure security. This is as opposed to issues of current methods that presuppose governance, wherein actuality thought is not provided, and exchanges made without explicit governance (See Appendix A.1.6).

In summary, experts agreed there were issues presented by the methods in which information planning and enabling occurred. Such process norms also implicate appropriate information governance. They professed high-level requirements and needs on how to alleviate issues. These factors along with those explored within the following sections pertaining to further governance-centric aspects will be collated within discussion as part of identifying further gaps and requirements.

4.5.2.4 Need for Improved Information Governance Focuses over Information Flows

A1, A2, A3, A4, A5, A7, A9 and A10's practices faced difficulties achieving effective governance over their internal / external information-flows. Notably, A5 and A7 perceived little control within their practices whether internal actors sufficiently and securely undertook project-work. A3 also perceived limited visibility and governance over what information had been generated and shared throughout their supply-chains, to who, and how. This notion applied particularly to SMEs despite BIM plans directing them to exchange via the CDE.

A5 and A9's separate practices attempted to rectify these gaps via similar governance approaches to better identify and thus govern what their appointees needed to know and share. These approaches were hierarchal in that each appointer governed: (a) security-clearances; (b) sharing and (c) access to their own appointees a tier below.

These elements of hierarchal governance were further based on what an appointer had identified their appointee needs to know. This was in turn based upon an organisation's role and their tier-position within an appointment-chain. A5 and A9's governance approach allowed each tier to better achieve the following factors:

1. Improve the identification and governance of what files their own appointees need to know and share. Correspondingly, a given tier would inform their own appointer of decisions made, thus establishing a chain of hierarchal governance.

2. Improve the identification of what files *could* be shared and accessed by their appointed organisations given the level of clearance achieved and security-risks that information.

3. Overall, ensure that this was a consistent process that would be applied throughout their different projects.

Point 1 represents hierarchal-governance throughout appointment-chains as well as decision-making rights held at an appropriate locality by those most informed to make decisions. Point 1 loosely feeds into the aforementioned **Point 2**, where A9 believed their governance approach enabled the appointers (at any given tier) to identify what could and could not be shared to tendering organisations. This is with respect to the fact that tendering organisations required a degree of information to submit their proposals, but, in order to simply tender, could not be expected to pass detailed security-competence tests in ensuring their professionals held appropriate clearances.

Furthermore, and in expanding upon the need for consistency presented in **Point 3,** A7 and A9 implemented their own digital tools as CDEs possess limited functionalities in effectively supporting governance. A9s tool guided clients through the requirement-setting process for numerous project-activities, including definition of information-requirements, ensuring factors such as contractual commitments of appointees to produce model data, inclusion of PLQs as part of the information-exchange programme, and overall definition of information and model-delivery tables had been considered. A9 perceived this improved consistency and quality of their EIRs (See Appendix A.9.5).

A7 on the other hand developed a decision-support tool to leverage information-delivery plans to improve coordination of information-delivery between lead-appointees and the client. This tool could cross-reference information present within appointee's delivery-plans to provide their client-side practices, knowledge over the required time and resources for any given appointee to undertake their cumulative organisational-level responsibility. The tool also informed decisions over which organisations should receive which files based on what and when an organisational role had been assigned to deliver. A7 however noted their governance focuses were limited to lead-appointees and themselves as client. As such, their governance capabilities possessed gaps in visibility over their lead-supplier's own tiers of appointees.

Discussion: It appears BIM standards guide the planning of processes and information but possess limited guidance for how organisations should govern their actual project's and their information-flows. A7 and A9 posed this required them to define their own approaches of how governing their project-specific BIM processes. This required development of their own information-governance policies, processes as well as supporting technologies. A7 for example utilised BIM documentation via decision-support tools for improved governance over their suppliers. A5 and A9 captured BIM plans via digital tools as well as defining their own, yet similar approaches to achieve hierarchal governance over their appointment-chains.

A limitation of their approaches appears to be that sharing or access to information between appointment tiers was driven by decision-making of organisational-level information-deliverables of model-files, occurring at distantly scheduled points in the project-schedule. Their approaches thereby possessed limited specificity. Furthermore, given the issues noted within **Section 4.5.2** so far, knowledge-centric governance issues may extend to object-level access and federation mechanisms. I.e., being able to easily, effectively and accurately reconcile the need to know with the need to share. In addition, no single practice employed all hierarchal governance tactics. I.e. A5, A7 and A9 each missed an aspect of each other's approaches, and their benefits in-turn. As such, and in line with previous atomicity-requirements in **Section 4.5.2.1.1**, benefits could be gained from a process and technological shift based around following requirements of enabling a chain of atomic hierarchal governance over appointment-chains:

1. This comprises the utilisation of digital methods to capture and enable governance of requirements, responsibilities and information-needs of appointee organisations and govern what each organisation needs to know and share.

2. This also comprises the on-going governance of the information-flows of appointee organisations. Appointer organisations should correspondingly be able to visualise and govern their appointed organisations information-flows at an atomic scale. Furthermore, clients and asset-owner organisations should be able to comprehensively visualise the entire information-flow of all project-stakeholders at an atomic scale.

4.5.2.5 Difficulties in Defining and Governing Security-Access Policy

The process of creating CDE access-structures involves defining varying levels and types of access-rights for actor roles. A common issue indicated via A1, A3, A5, A6, A7, A8, A9, A11 and A12 being the implementations of access-models such as 'role-based access control' (RBAC) commonly did not support atomic control at the level of 'BIM objects and BIM data-attributes'. Instead, the aforementioned experts believed CDE workflows, and their access control predominately operated in line with file and folder-based architecture. For example, A3 stated the granularity of CDE access control within A3's practices limited them. A3 provided the example of a groundworks contractor working on a sensitive facility who possesses a need to know that a facility is present, and that they are unable to work there. They do not however need to know the facilities inner-workings (See Appendix A.3.7).

A3 however believed current mechanisms did not enable this specificity to distinguish 'who should get to see what?' at an atomic-level, whilst also considering clearances present. A3s practices CDEs supported file-level RBAC access. This meant that actors of a given role could access all information within a given file, or not access the file at all. Similarly, A3 perceived the level of control and granularity via the shared 3D visualisation environment was visualisation to the entire model or nothing at all. A3 did note certain GRs could download files containing subsets of BIM data and provide these to internal actors. This was not however via mapping of roles, or professional's activities to certain groupings of data subsets and was instead via the manual mapping that certain BIM objects belonged to a certain aspect of the information-model e.g. a drainage-system.

On the other hand, A12 as a software-vendor proposed improved RBAC mechanisms within their products allowed for granular permissions over information at an BIM object level. Granular BIM information visualisation capabilities were also similarly being developed. A12 however did note that these mechanisms had not yet been tested within practices of their users and believed they would evolve as users work with A12 to resolve issues or make improvements.

Some issues that may be faced by A12s RBAC approach were identified via cross-referencing analysis of A5, A6, A8 and A11's beliefs. These experts indicated that CDE security-mechanisms present 'ease of use' issues which are tied to the inherent complexity in making governance-decisions over BIM data access. This was noted within **Sections 4.5.1.**

A5, A6, A9 and A11 further believed that even if access-mechanisms are granular enough to account for BIM object-level access, the complexity of BIM models requires vast administrative overhead. A6 and A8 argued this usually results to the default of access to nothing or everything. A6 noted concern over the ease of usability in governing the security-access policy for BIM data, via security-access models built-in to CDEs. A6 noted that improved methods were necessary to alleviate (a) the admin issues arising from unintuitive mechanisms and (b) security-risks present from access not being updated over time (See Appendix A.6.8) These issues appear to be tied to the systems-design principles for CDEs not being deeply embedded in the BIM stakeholder, work and information-flow context, where information-needs are fluid and change over time in-line with current activities / roles.

Discussion: As inferenced via A6 and A8, another complexity of mapping RBAC on a need-to-know basis appears to be due to BIM models representing the physical, spatial and semantic interconnections between nested design components and systems, all of which are attributed with a variety of project-specific data. Some of this may represent project-specific security-risks. More broadly, it is complex to understand what is relevant for disciplinary professionals.

Supporting this inference, A2, A3, A4 and A11 believed only those with an appropriate overlap of disciplinary and security-risk knowledge can make pragmatic decisions on permissions of such complex datasets. Furthermore, A6 and A8 perceived current access-models make this difficult even for those with informed knowledge of what actors (internal / externa) need to know. A8 in particular noted that linking which roles needs to view what sets of BIM data was inherently complex, as it is not straightforward mapping. It is further complicated if there is a lack of policy and appropriate governance to appropriately capture what different roles need to know. A8 believed such issues in practice would lead to a default of security-access policy not being appropriately defined and applied, thereby increasing security-risks greatly (See Appendix A.8).

A1, A3, A5, A6, A8 and A11 thus believed there was a need to simplify the linkage of access-rights to BIM data. A5 noted this important due to the large amounts of BIM data generated on projects and indicated there was a need in some manner to link access-rights to precise groupings of BIM objects. A1 proposed linking task-based responsibilities to access rights for internal actors. When synthesised with previously captured requirements for atomic information-sharing, it appears appropriate for internal team-level actor's task inputs, and thereby access to directly interface with the information shared via task level outputs of other related teams. In addition, access should account for clearances. A1, A2, A3, A4, A6, A7, A9 and A11 agreed in principle with the general approach and supported further exploration.

4.5.2.6 Difficulties in Coordination and Governance of Sensitive Project Information

A1, A2, A4, A6, A9 and A11 perceived issues coordinating information-flows of varying sensitivity. Sensitive and non-sensitive information was stored in separate information-containers where the concurrent development of multiple separate information-streams was required via different stakeholders. This increased IM difficulties in coordinating separate information-flows. Additionally, within A1, A2, A4 and A7s practices, coordination of sensitive and non-sensitive information occurred only under certain conditions. Increased levels of governance were thus required over what information was present within non / lesser-sensitive information-containers after coordination.

Furthermore, A6 posed that filtered sensitive information leaves gaps within lesser classified models (e.g. gap where a secure room was removed). A6 referred to such gaps as providing a 'medieval-map' for threat-actors such as malicious insiders to understand that 'here be dragons' (See Appendix A.6.9). In other words, allowing malicious actors to infer the gap left within the non-secure model represents the sensitive aspect e.g. a filtered spatial volume of the asset that may represent plantroom/s which serve a purpose in handling of sensitive equipment.

A1, A2, A3, A4 and A6 believed this presents security concerns as access to information within projects is usually via file or federated object-based information-containers. This means actors gain access to everything within a model, including such design-gaps. They believed these issues represent norms of access approaches not directing that actors gain access to only what they need to know and nothing more. A1, A2 and A3 for example perceived these issues could be alleviated via querying subsets of BIM data (BIM objects and data-attributes of BIM object) at a precise LOI and LOD. It is inferred that via such approaches, the presence of gaps would be common-place as irrelevant information would be filtered out. Actors would therefore only be aware that the gaps provided within their access were deemed irrelevant to them.

4.5.3 Discussion of BIM Governance Issues and Limitations

Industry and expert norms in capturing, enabling and governing information-flows were discussed during interviews to identify issues and limitations that impede secure collaboration. This includes requirements captured via experts that are gaps of the current norms. This section will inter-relate the extracted issues and limitations to expose further gaps, and thereby needs for secure collaboration. The following factors are categorised against theme and whether **BIM** governance issues are embedded in the problem-environment with either a focal process centric perspective **(PP)** or technological centric perspective **(TP)**.

Table 4.9: BIM Governance and Management Themes (Collated)

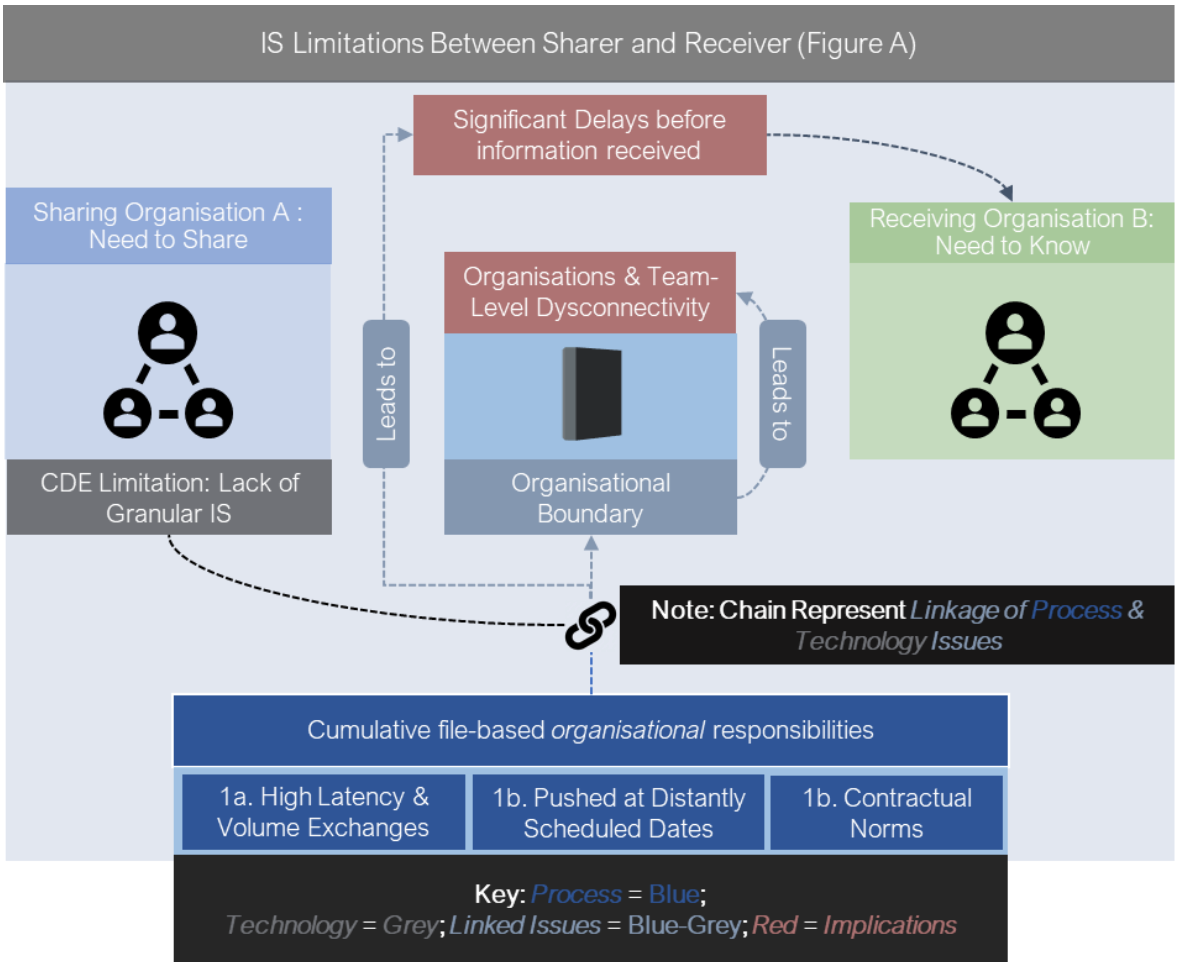
Concept # and Focus	BIM Governance and Management Themes	Expert Occurrences	Total
1.	**High-Level Organisational Responsibilities**: BIM plans mainly capture organisational and file centric responsibilities.		
1a. (PP)	BIM plans define distant dates for push-based coordination of files of high information volume. This is typically when the organisational responsibility is met.	A1, A2, A3, A5, A7, A9 and A11.	7
1b. (PP)	IS occurs mainly between appointment arrangements as opposed to more collaborative procurement forms integrating atomic actors across chains (Winfield & Rock, 2018). Mechanisms also implicates defining of BIM coordination schedules.	A1, A2, A3, A5, A7 and A9.	6
2.	**Limited Task Level responsibilities**: The capture of atomic task level responsibilities is uncommon / captured via ineffective methods.		
2a. (PP)	Not defining atomic responsibilities limits ***specificity*** of responsibilities of what teams need to generate; share and access.	A1, A2, A3, A5, A7, A9 and A11.	7

2b. (**PP**)	Responsibility capture via static document methods (e.g. RACIs) - ineffective to represent how atomic actor's responsibilities are evolving and interdependent.	A2, A3, A5, A7, A9 and A11. Corroborated by Beach (2019).	6
2c. (**TP**)	CDEs do not enable capture of an atomic digital process resource, comprising evolving information responsibilities and needs amongst collaborators, informing precise IS amongst them.	A1, A2, A3, A7, A9, A11 and A12.	7
2d. (**PP**).	Difficult to validate responses to current information-planning responsibilities (static, document and organisational based) in view of *data-centric* outputs of high volume.	A1, A7 and A9 and Beach (2019).	3
3.	Information-sharing and access difficulties are presented by CDE limitations which are linked to responsibility capture and information-governance gaps. Sub-factors are interlinked.		
3a. (**TP**)	CDE functionalities mainly support file-based exchange as opposed atomic and precise sharing of BIM data-subsets (no more / less to meet needs)	A1, A2, A3, A4, A6, A7, A9 and A11.	8
3b. (**TP**)	Technology-centric: Correspondingly, access-models support file and folder-level access as opposed to BIM object-level access. Where present, they are complex for GRs to utilise and thereby ineffectual.	A3, A5, A6, A7, A9, A11 and A12.	7
4.	Project-specific adoptions of BIM processes face difficulties governing their information-flows		
4a. (**PP**)	Stakeholders feature limited governance of their information-flows. This includes limited (a) internal security-risk governance and (b) pragmatic decisions balanced with collaborators needs.	A1, A2, A3, A4, A6, A7, A8, A9, A10 and A11.	10

4b. (PP)	Appointers face difficulty governing appointees' information-flows (ineffectual hierarchal governance). This is due to limited / ineffective focuses within projects and limited standards-led guidance.	A2, A3, A4, A5, A7, A9 and A11.	7
4c. (TP)	CDEs lack functionalities to visualise and govern atomic information-responsibility planning, exchanges and information-flows as a whole. This implicates security-risk governance difficulties.	A1, A4, A7, A8, A9 and A12.	6
4ci. (TP)	CDEs lack mechanisms for GRs to validate exchanges based on receiver's needs (Beach, 2019) and security-risk governance (before release).	A1, A4, A7, A8, A9 and A12.	6
4cii. (TP)	'Hierarchal governance' capabilities over appointees, their processes and information-flows (atomic scale) are also not present.	A1, A2, A3, A5, A7, A9, A10, A11 and A12.	9
4d. (TP)	GRs must manually filter files of sensitive and irrelevant information prior to exchange. This presents (i) inaccuracy / inconsistency of decision making and (ii) of 'sensitivity gaps'. Governing 'gaps' requires (a) additional routes for IM and IS coordination or (b) mass elevation of clearances.	A1, A2, A3, A5, A7, A9, A10, A11 and A12.	9

4.5.3.1 Interrelation of Identified Issues and Limitations

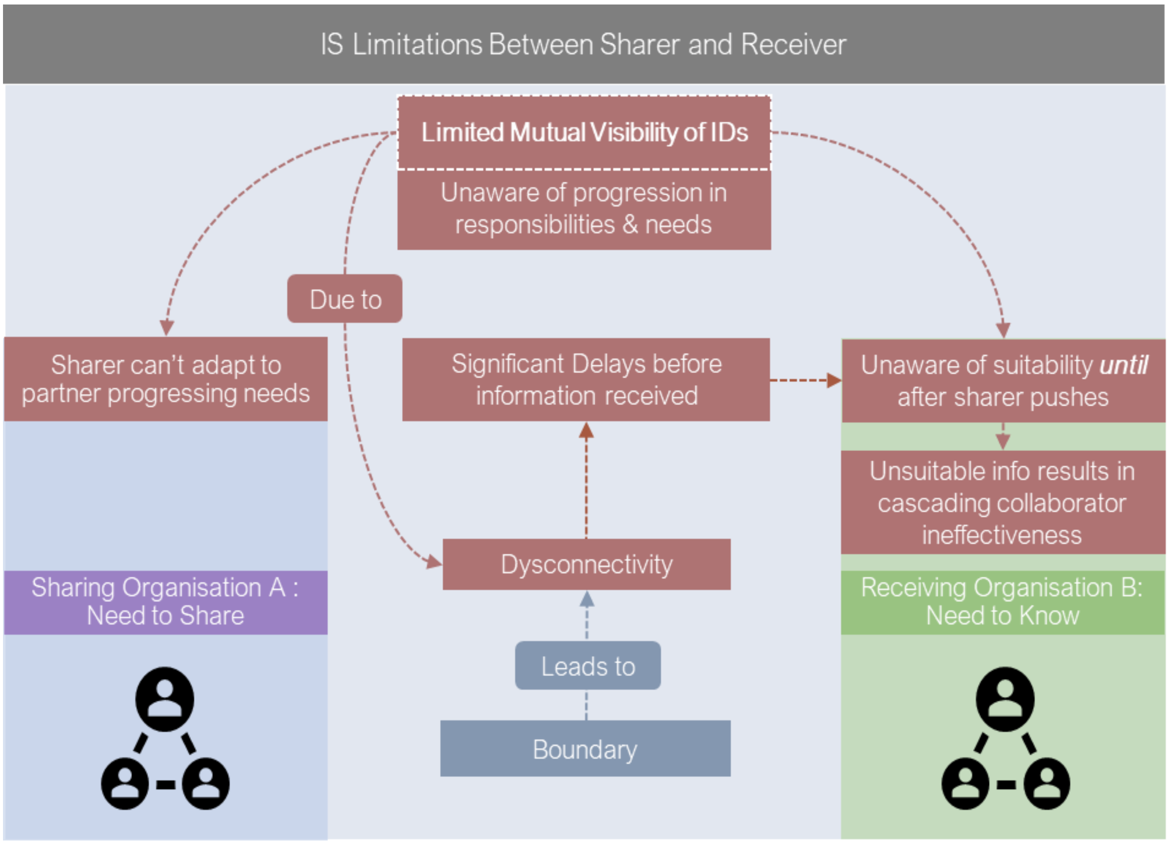
The following section will inter-relate process and technological factors to expose further gaps. Firstly, **Points 1a and 1b** link to BIM plans which capture responsibilities to push files at distantly scheduled points when an organisational-level suitability is reached. Correspondingly, **Point 3a** represents common file based CDE limitations result in collaborators lacking the technology to implement object-level federation and access. Collectively, these limitations introduce high latency and thereby delay before receiver's are provided information and learn whether information is suitable to effectively support their work. **Figure 4.8** represents these issues diagrammatically via generalisms, as organisations A and B as 'sharer' and 'receiver' respectively.



IS Limitations Between Sharer and Receiver (Figure A)
Significant Delays before information received
Sharing Organisation A : Need to Share
Receiving Organisation B: Need to Know
Organisations & Team-Level Dysconnectivity
Leads to
Leads to
CDE Limitation: Lack of Granular IS
Organisational Boundary
Note: Chain Represent Linkage of Process & Technology Issues
Cumulative file-based organisational responsibilities
1a. High Latency & Volume Exchanges
1b. Pushed at Distantly Scheduled Dates
1b. Contractual Norms
Key: Process = Blue; Technology = Grey; Linked Issues = Blue-Grey; Red = Implications

Figure 4.8: Interrelation *Analysis (1)*

The previous Figure 4.8 portrays **Points 1a, 1b,** and **3a,** resulting in boundaries between organisations which implicate dysconnectivity between team and individual level actors who are unable to directly share, especially where exchanges occur against set contractual arrangements **(Point 1b)**. This is even if certain aspects of information are ready to coordinate. Also, there is limited IS precision to ensure security in line with the need-to-know principle. Further implications of dysconnectivity are organisations A and B's internal actors possessing limited mutual visibility of task-level work and comprises the following issues (depicted in **Figure 4.9**).



IS Limitations Between Sharer and Receiver
Limited Mutual Visibility of IDs
Unaware of progression in responsibilities & needs
Due to
Sharer can't adapt to partner progressing needs
Significant Delays before information received
Unaware of suitability *until* after sharer pushes
Unsuitable info results in cascading collaborator ineffectiveness
Dysconnectivity
Sharing Organisation A : Need to Share
Receiving Organisation B: Need to Know
Leads to
Boundary

Figure 4.9: Interrelation Analysis (2)

The following points expand upon the depiction in **Figure 4.9** of implications between sharer and receiver.

Limited Awareness of Responsibilities: Actors lack live recognition of collaborator's tasks and what they 'plan to push'. They thus lack awareness of suitability until received. Unsuitable information implicates how receivers can undertake their responsibilities and cascades to affect whether their own collaborators needs can be met.

Limited Awareness of Information-Needs: Actors generating information lack recognition of the progressing needs of receiving organisations internal actors (in view of receivers' responsibilities). Organisations are thus unaware of the precise information to share to enable optimal work whilst avoiding potential exposure.

Alongside **Points 1a, 1b and 3a**, dysconnectivity is also influenced by ineffective capture of task work overlaps **(Points 2a and 2b)**. This constrains professionals of knowledge in each other's work and how to adapt their responsibilities for an appropriate response **(Point 2d)**. **Point 2c** represents a mirroring technological limitation in enabling the capture and update of task work overlaps. These factors are combined as a gap implicating dysconnectivity **(Figure 4.10).**

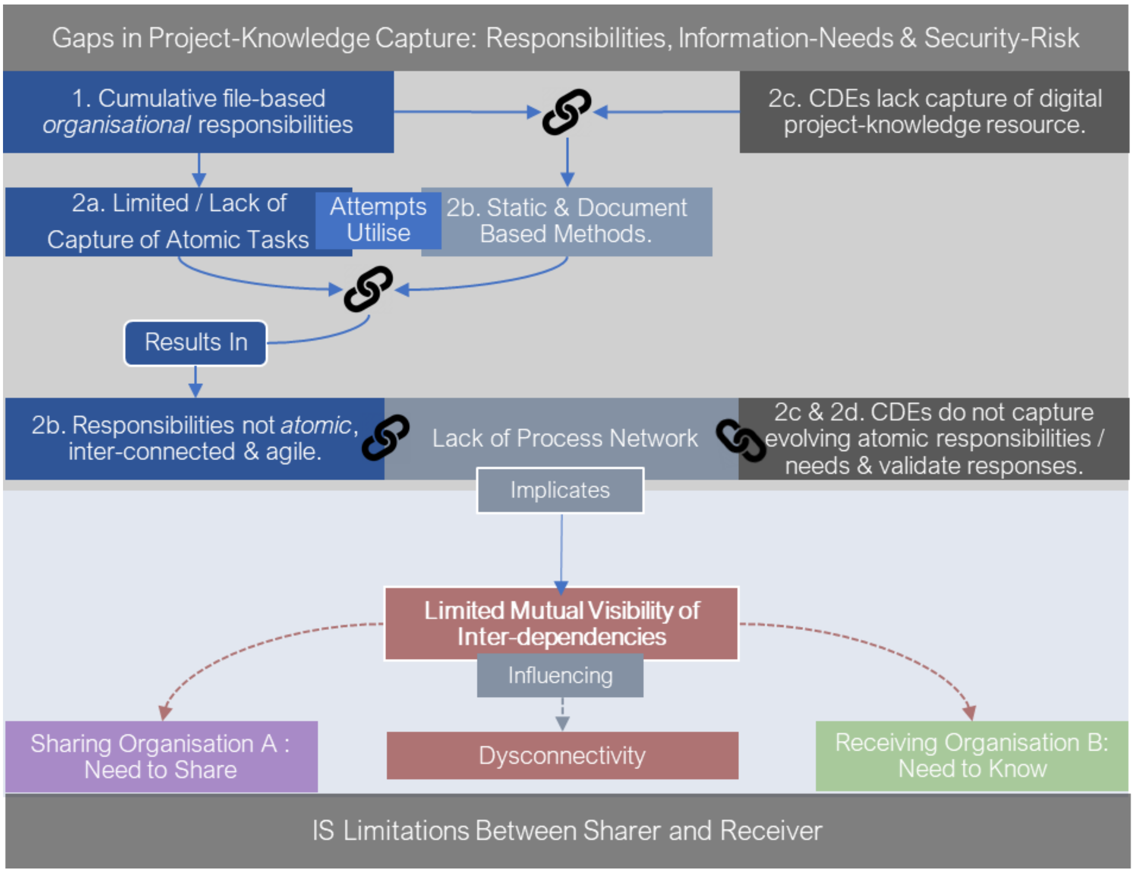

Gaps in Project-Knowledge Capture: Responsibilities, Information-Needs & Security-Risk
1. Cumulative file-based *organisational* responsibilities
2c. CDEs lack capture of digital project-knowledge resource.
2a. Limited / Lack of Capture of Atomic Tasks
Attempts Utilise
2b. Static & Document Based Methods.
Results In
2b. Responsibilities not *atomic*, inter-connected & agile.
Lack of Process Network
2c & 2d. CDEs do not capture evolving atomic responsibilities / needs & validate responses.
Implicates
Limited Mutual Visibility of Inter-dependencies
Influencing
Sharing Organisation A : Need to Share
Dysconnectivity
Receiving Organisation B: Need to Know
IS Limitations Between Sharer and Receiver

Figure 4.10: Interrelation *Analysis (3)*

The key factor that is depicted in **Figure 4.10** being that current methods lack a 'live digital process network' acting as a map of interdependencies between professional actors, their tasks and information-flows between their tasks. Such a network could interconnect related actors and enable on-going recognition of overlapping responsibilities and information-needs. They are also not conceptualised as such per BIM process norms, which extends to CDEs not typically based upon such architecture or functionalities to facilitate capture of such a network in enabling and governing atomic BIM processes (**Points 2c, 3a, 3b**).

In addition to project knowledge deficits, further joint deficits are characterised in governing security-risk whilst balancing collaborators needs in the following **Figure 4.11**.

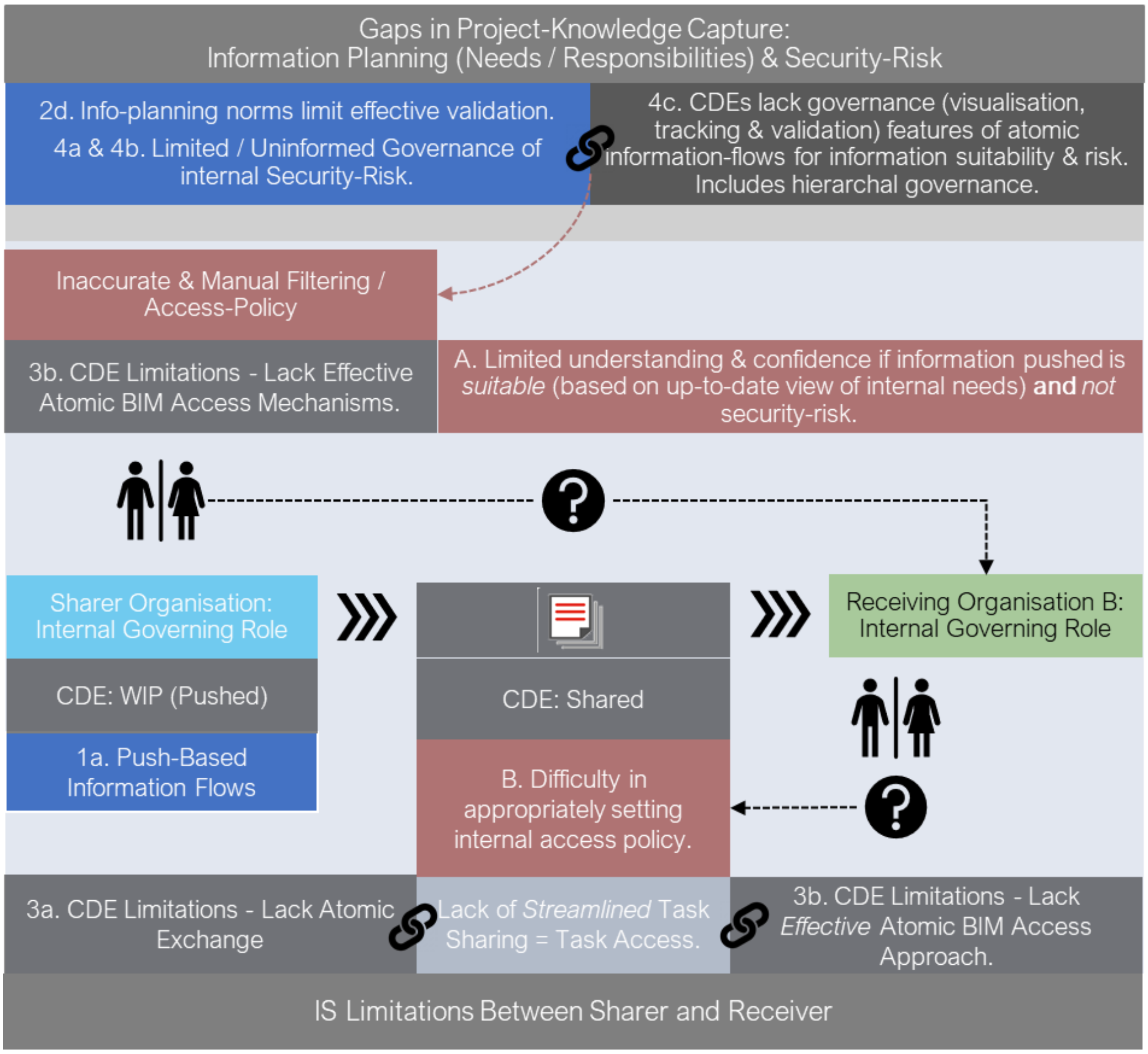

Gaps in Project-Knowledge Capture:
Information Planning (Needs / Responsibilities) & Security-Risk
2d. Info-planning norms limit effective validation.
4a & 4b. Limited / Uninformed Governance of internal Security-Risk.
4c. CDEs lack governance (visualisation, tracking & validation) features of atomic information-flows for information suitability & risk. Includes hierarchal governance.
Inaccurate & Manual Filtering / Access-Policy
3b. CDE Limitations - Lack Effective Atomic BIM Access Mechanisms.
A. Limited understanding & confidence if information pushed is *suitable* (based on up-to-date view of internal needs) **and** *not* security-risk.
Sharer Organisation: Internal Governing Role
CDE: WIP (Pushed)
1a. Push-Based Information Flows
CDE: Shared
B. Difficulty in appropriately setting internal access policy.
Receiving Organisation B: Internal Governing Role
3a. CDE Limitations - Lack Atomic Exchange
Lack of *Streamlined* Task Sharing = Task Access.
3b. CDE Limitations - Lack *Effective* Atomic BIM Access Approach.
IS Limitations Between Sharer and Receiver

Figure 4.11: Interrelation Analysis (4)

Firstly, **Figure 4.11.** depicts **Point 4a** of limited recognition of security-risk which coincides with point 1a of unsecure push-based flows. This is as GRs possess one-sided understanding of the needs of professionals within receiver organisations which limits suitability and raises potential for exposure.

Furthermore, GRs must manually govern outputs within CDEs based on static organisational requirements, not updated with either organisations or professionals evolving responsibilities / needs. These are **Points 2d** and **4ci** as depicted in **Figure 4.11.** Information planning norms generally do not provide how to effectively validate exchanges. Information planning and validation norms (process and technology) thereby appear to limit confidence that exchanges were secure and in line with receiver's requirements.

Correspondingly, also depicted in **Figure 4.11**, CDEs lack functionality in enabling atomic exchanges (**Point 3a**), and accordingly with atomic visibility of task-level information-flows in aiding governance of what needs to be shared with 'who, why, to what detail and knowing what aspects are sensitive?' (**Point 4c**). These CDE gaps also implicate difficulties GRs face in making pragmatic decisions over exchange and access-policy, which is currently a complex manual procedure (**Point 3b**). **Points 3a, 3b** and **4c** are also depicted in **Figure 4.11** and also collectively presents a gap of streamlined atomic information-flows whereby task-level exchanges serve also as access for receiver's tasks. Atomic approaches would also aid filtering of irrelevant or sensitive information as gaps representing vulnerabilities.

Currently, managing this security concern requires either (a) coordinating separate information-flows of variable sensitivity or (b) elevating clearances to many actors (**Point 4e**). This is depicted within the following **Figure 4.12.**

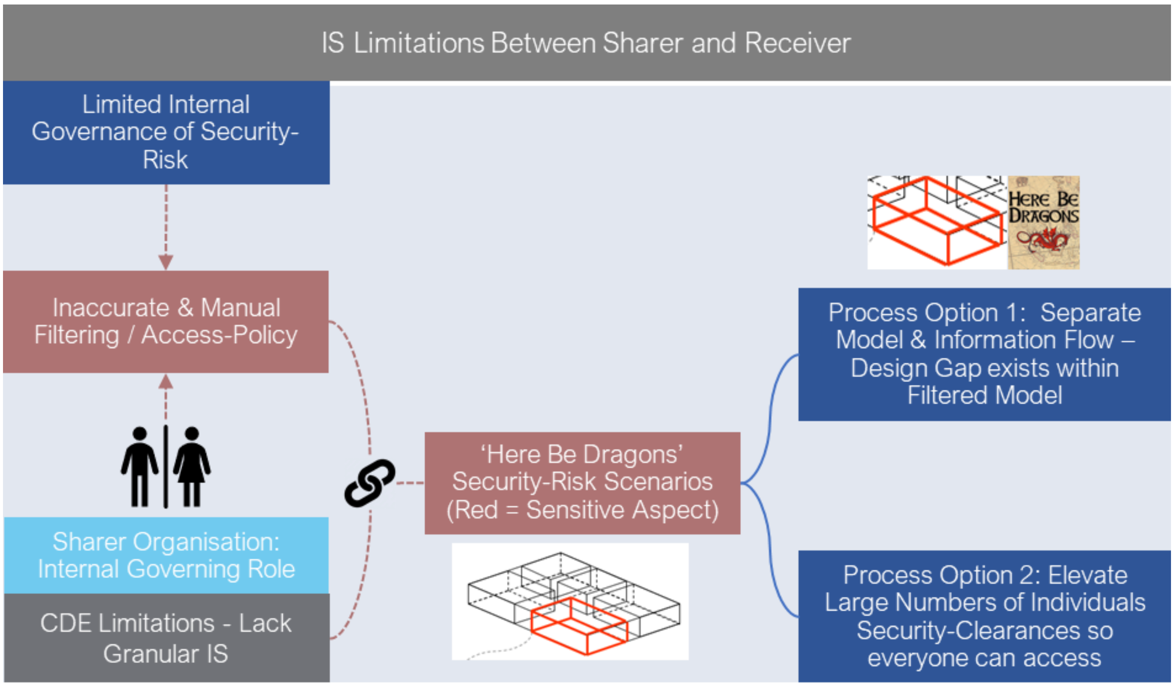

IS Limitations Between Sharer and Receiver
Limited Internal Governance of Security-Risk
Inaccurate & Manual Filtering / Access-Policy
Sharer Organisation: Internal Governing Role
CDE Limitations - Lack Granular IS
'Here Be Dragons' Security-Risk Scenarios (Red = Sensitive Aspect)
HERE BE DRAGONS
Process Option 1: Separate Model & Information Flow – Design Gap exists within Filtered Model
Process Option 2: Elevate Large Numbers of Individuals Security-Clearances so everyone can access

Figure 4.12: Interrelation Analysis (5)

Figure 4.12 depicts the default process-options available, and issues presented. This is as opposed to GRs governing atomic subsets of select security-cleared individuals with a valid 'need to know' (**Point 3a**).

Summary: In combining process and technological issues and gaps in effectively and securely governing information-flows, a further gap is uncovered which compounds the previous gap of process networks. This being a live governance overlay over such process networks as a 'governance network'. Such a concept combines both information-planning and enablement benefits of process networks but also acts as a *live* governance overlay over the overlap of atomic information-flows between partners, which includes comprehensive hierarchal atomic governance over appointees (**Points 4b and 4cii**).

4.5.3.2 Further Implications of Analysis

The analysis within **Section 4.5.3.1** represents BIM methodology norms for process and information planning, enablement and governance which are representative of difficulties faced by stakeholders in industry in ensuring both optimal security and suitability of information-flows. As analysis attempted to combine both the general issues for normal and security-minded BIM projects, they appear relevant to both. This is with additional consideration of issues for security-minded environments in reconciling sensitivity issues.

Due to these norms, it appears current methods possess limited efficacy in verifying whether appropriate degree of information was shared to meet collaborators needs and ensure security. Furthermore, current methods present dysconnectivity where prior to pushing, collaborators possess limited knowledge of what receivers' professionals actually require. Receiving organisations also possess limited knowledge and influence over what sharers intend to push.

Dysconnectivity between stakeholders thus implicates sharing tensions i.e. gaps in attaining mutual recognition of: 'who needs to know what information and when?' to understand 'who needs to generate and share what, when and to who, as the project progresses?'.

Further norms of BIM information-responsibility setting prevent atomic, low latency sharing, directly between professionals. This is even if team-level actors do possess mutual understanding. Joint issues are also present via limited governance and visibility of information-flows. This includes issues of hierarchal governance. Collectively, factors discussed implicate a lack of sharing specificity which limits effective working and presents security-risk.

Correspondingly, it is posed that projects lack governance networks as a combination of both process and governance aspects. This is in underpinning the informing, enabling, and governing of BIM information-flows. Implementing technologies should leverage the inherent interconnective of atomic information-flows in facilitating live governance capabilities over them. This includes live visibility, validation and also hierarchal governance of appointee's needs and information-flows.

Future technologies could implement such networks and functionalities also in achieving atomic pull-based information-flows (comprising atomic exchange and access). This is further linked to issues inherent to push-based methods of limited specificity. This in elevates security-risk potential and limited suitability of information received. Accordingly, it is posed atomic and pull-based information-flows would be inherently more secure and suitable when overlaid with atomic governance capabilities. The benefits pull-based transactions may present for secure collaboration are expanded on in the following section. The following **Figure 4.13** however combines the factors discussed within this and the previous section.

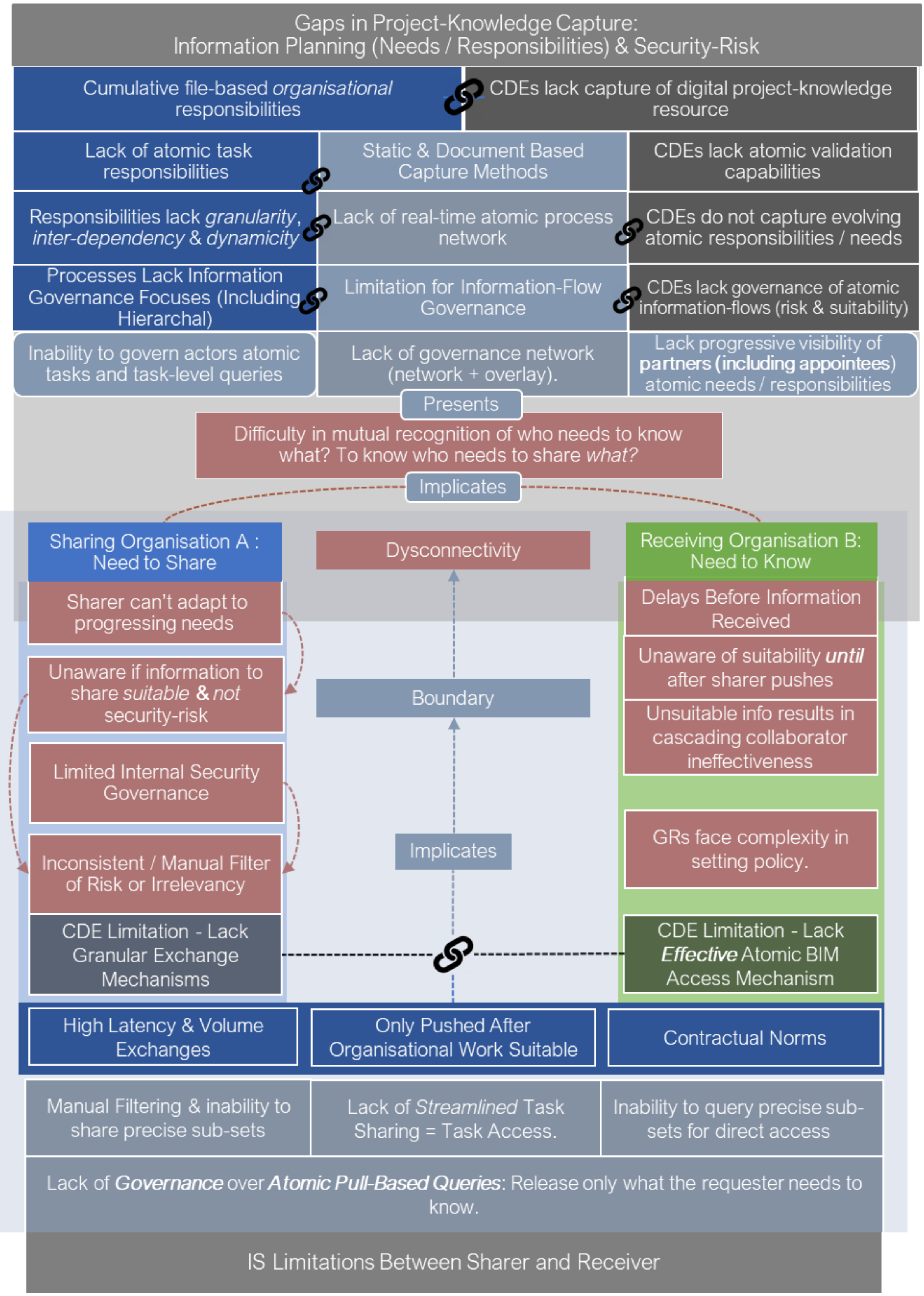

Gaps in Project-Knowledge Capture:
Information Planning (Needs / Responsibilities) & Security-Risk
Cumulative file-based *organisational* responsibilities
CDEs lack capture of digital project-knowledge resource
Lack of atomic task responsibilities
Static & Document Based Capture Methods
CDEs lack atomic validation capabilities
Responsibilities lack *granularity*, *inter-dependency* & *dynamicity*
Lack of real-time atomic process network
CDEs do not capture evolving atomic responsibilities / needs
Processes Lack Information Governance Focuses (Including Hierarchal)
Limitation for Information-Flow Governance
CDEs lack governance of atomic information-flows (risk & suitability)
Inability to govern actors atomic tasks and task-level queries
Lack of governance network (network + overlay).
Lack progressive visibility of **partners (including appointees)** atomic needs / responsibilities
Presents
Difficulty in mutual recognition of who needs to know what? To know who needs to share *what?*
Implicates
Sharing Organisation A : Need to Share
Dysconnectivity
Receiving Organisation B: Need to Know
Sharer can't adapt to progressing needs
Delays Before Information Received
Unaware if information to share *suitable* **&** *not* security-risk
Unaware of suitability ***until*** after sharer pushes
Boundary
Unsuitable info results in cascading collaborator ineffectiveness
Limited Internal Security Governance
GRs face complexity in setting policy.
Implicates
Inconsistent / Manual Filter of Risk or Irrelevancy
CDE Limitation - Lack Granular Exchange Mechanisms
CDE Limitation - Lack ***Effective*** Atomic BIM Access Mechanism
High Latency & Volume Exchanges
Only Pushed After Organisational Work Suitable
Contractual Norms
Manual Filtering & inability to share precise sub-sets
Lack of *Streamlined* Task Sharing = Task Access.
Inability to query precise sub-sets for direct access
Lack of ***Governance*** over ***Atomic Pull-Based Queries***: Release only what the requester needs to know.
IS Limitations Between Sharer and Receiver

Figure 4.13: Combined Interrelation of Issues, Gaps and Needs

4.5.3.3 Proposition of Potential Solutions

This section advocates overarching recommendations for future BIM methodologies. Firstly, expanding on the previous section, a core proposal being adoption of atomic and pull-based information-flows with governance overlaid for inherently secure-collaboration. This includes a proposal where focuses shifting to team-level actors, particularly at the individual / professional level. Such actors should be able to cut across boundaries in directly sharing information. Currently however, they lack recognition of which and what other ID actors 'need to know what?' to understand 'who needs to share what?'. They thus face difficulty in answering the aforementioned paradox and alleviating associated information-sharing tensions.

On the other hand, it is envisaged that process networks (**Section 4.5.3.1**) would help alleviate knowledge-centric issues. These would be a data-driven, industry-standardised and machine-interpretable representation of a project specific information-flows between team-level actors. In other words, a data-structure, and adjoining information-systems architecture that is built to facilitate atomic processes and captures professionals themselves, their tasks, and IDs to another actor's task.

Such inter-connected networks would be the foundation to inform currently disconnected actors whom they share IDs in their task-level work, and thereby in providing and receiving information. It also provides the basis for on-going inter-connectivity and atomic information-sharing. A network would therefore capture and enable data-centric BIM information-flows. This includes the following key points where crucial governance-centric factors are also noted as an overlay to process-network, thereby being a governance network for their governance responsibilities.

Atomic Information Planning: Information planning entails creating a secured 'lens' on to others task-work of relevancy (IDs). This is both internally, and externally. Once a lens has been created, it should facilitate interconnectivity between professionals. As an overview in creating such a lens, the requesting actor should not possess specific knowledge of what prospective upstream professionals have generated as this would indicate security-concerns. Rather, such actors should possess the minimum understanding of overlapping relevancy of responsibilities such that IDs can be identified by the professionals themselves and formalised by GRs to be added to a project's specific process network. On-going atomic collaboration and information-flows can thereafter be facilitated. Methods to generate IDs will be expanded upon within Chapter 5.

Enabling Atomic Pull-Based Information-Flows: A process network as an interconnected data-structure and its implementing systems architecture must be capable of facilitating atomic pull-based information-flows. This includes the actual management and exchange of data-subsets between actors and their tasks. Professionals would query against established IDs to retrieve inputs from other individuals via an implementing platform.

Furthermore, the currently detrimental boundaries provide benefit in a pull-based context by providing time for the GR of sharers in making informed decisions over what information to release after a request has been received. Atomic sharing also enables task outputs to directly interface with task inputs and access of a receiving actor. This enables planning, exchange, and access to be a fluid procedure. Atomic interconnectivity also implies significantly decreased latency between communication and thereby sharing between externally related teams. This should in turn increase stakeholder and project efficiency.

Governance Network Overlay: GRs lack comprehensive and atomic visibility over information requirements, information exchanges, and the information flows a whole. This is both of their own internal practices, their appointees, and how atomic overlaps (IDs) are present amongst the professionals of partners. This visibility would simultaneously enable (a) improved governance and validation of the organisational output and (b) keeping view of how task responsibilities should interface with needs of receiver's task needs.

Furthermore, and combined with knowledge and process complexity issues, manual filtering increases potential for inaccurate decisions. Rectifying this issue requires systems to provide GRs their own overlay over a project's process networks. i.e. a governance network to govern what is being exchanged and why by their professionals. Rather, they possess the potential to ensure that responses to queries meet suitability needs and uphold security. Their own decisions could also be captured when filtering sensitivity / validating outputs.

This would also increase audibility of decision-making. Atomic IS would resolve other difficulties faced by GRs in manually filtering irrelevant / sensitive information from model-files prior to exchange with external parties. This includes concerns of sensitivity-gaps which are eliminated by exchanges of precise subsets. Furthermore, an overlay would also enable ongoing capture of what is being filtered, why and when, in auditing governing sensitive / irrelevant information.

As a whole, GRs throughout the process network are thus able to govern their own organisations portion of their network of incoming and outgoing transactions, but also in aiding broader inter-organisational governance.

Hierarchal Governance: As a sub-perspective of a governance-network, GRs should also be able to achieve comprehensive hierarchal visibility and governance over appointee's information-flows at an atomic scale. In other words, hierarchal visibility which extends from the client to the lowermost organisations within a given appointment-chain. This includes governance and access-setting over what appointees can access and visualise of their own internal-workflow. As such, there is a degree of bi-directional connectivity between an upper and lower-tier organisation to ensure that appointed organisations are able to achieve effective work whilst the upper-tier maintains privacy and security by choosing what to communicate.

Summary: In summary, filling the gap of a governance network and implementing architecture presents potential to bridge dysconnectivity and direct team-level actors in facilitating information-flows of enhanced security and efficiency. An appropriate information-system architecture would underpin and facilitate networks to iteratively capture atomic task responsibilities and IDs between tasks. As such, an appropriate data-schema should be devised to represent the network. The actual sharing and management of IS as per the role of current CDEs would also be facilitated by architecture implementing a network. Low latency and volume exchanges, corresponding to atomic task responsibilities / needs should also improve ease and detail of visibility, and by extension governance and audibility of information-flows.

4.6 Discussion of Broader Research Findings

This section will detail the broader implications of **Sections 4.3** and **4.4** which explored socio-organisational and project implementation issues respectively. This section will summarise findings and provide consideration of how aforementioned proposals may help alleviate such issues. Finally, closing statements in view of initial aims of primary research will be discussed.

4.6.1 Discussion of Cultural and Project Level Barriers to Secure Collaboration

Section 4.3 explored socio-organisational themes such as limited trust amongst intra and inter-organisational actors. This research sheds new light on themes such as trust where security is of pertinence, and the nuances stakeholders must consider when adopting such values in facilitating open yet secure collaboration. It is also proposed that as the need for sufficiently security-minded approaches becomes an increasing concern for the built-environment as a whole, so will the need to identify and address how actors both at an intra and inter-organisational level should interact in facilitating secure yet effective information-flows. Correspondingly, more security-centric socio-organisational issues, and thereby tensions may become apparent in-time with increased security recognition.

Section 4.3.4.1 explored socio-organisational barriers that are applicable at a cultural-level. These include stakeholder misperceptions, security-incognisance and limited competencies associated with secure and collaborative digital **BIM** approaches. Furthermore, cognisance and competency issues were identified of internal actors within projects of varying security-criticality. This applied especially to board-level actors, despite the fact that such actors possess the highest potential to influence a projects security-readiness.

Limited cognisance was argued to adversely influence client direction of implementing projects. This feeds into project-implementation issues discussed within **Section 4.4.5** where gaps have also been identified in defining requirements that integrate a project's security and efficiency motives, and the needs of all stakeholders. These gaps in turn stem from limited awareness of security-risk within the broader industry, particularly on the part of non-experienced clients.

This being said, both socio-organisational and project-implementation tensions arise despite the security-profile and sector of a project. Moreover, the longevity of the organisations involved with security-conscious domains appears to be a stronger indicator of security-competencies at the organisational-level and reflects internal actor behaviours. Furthermore, long-standing security-minded partnerships between clients, appointees and their own appointment-chains provides distinct security benefits. For example, only A1 and A4 were identified to possess long-standing security-minded relationships with their partners.

In contrast, both security and digital competencies are required to implement appropriate project-level requirements and policies to ensure efficient secure collaboration and limit project-level tensions. It is concerning, however, that as few organisations possess long-term experiences of both security and digital BIM approaches. As such, whilst lesser experienced supplier-organisations (and their internal actors) may be able to clear mechanistic security-clearances, they may not possess the degree of security-minded culture A1 was seen to possess. This, in turn, appears to be part of causes of limited security-competencies and negligence found on such projects described by A10, which whilst falling under a 'high-profile' moniker, are not always, holistically security-minded. This, of course, extends to the broader sector as A10 also indicated.

In summary, it appears there have been fairly limited collective efforts within the AEC sector to define routes which reconcile socio-organisational and project-implementation barriers in achieving secure collaboration. This may in part reflect security-initiatives being viewed as a fringe topic within industry and also, a capacity to be developed for solely internal needs. This as opposed to also being able to deliver security competencies to potential clients within the marketplace. This is imperative considering the nature of BIM project ecosystems wherein numerous numbers of stakeholders are present and interact over an extended period of time. The following **Section 4.6.2** will discuss 'Barriers in Enabling Secure and Collaborative Information-Flows'.

4.6.2 Discussion of Barriers in Enabling Secure and Collaborative Information-Flows

Gaps were identified in enabling secure and collaborative information-flows which cannot be fully resolved solely via advancements in cultural and project implementation approaches. These gaps were explored in section 4.5, but also relate to factors noted in section 4.3.4.2 of issues encountered amongst team-level actors, alongside erroneous security-risk governance procedures.

Security-Risk Governance: **Section 4.4.5.1** explored available approaches available in managing project-level security and collaboration tensions. The following gaps were however identified in managing tensions.

- Limited on-going governance of security-risk in view of increasing generation of project information on the built-asset.
- Actors not receiving an appropriate LOI and LOD when needed. This was an implication of erroneous information-planning and change-management of security-procedures.

The former gap of limited security-risk governance has formed part of needs for improved governance of security-risk in line with atomic exchanges. The latter pertains to difficulties in governing actors need to know and share. Section 4.5.1.3 explored how proposals would aid in resolving said gaps via governance networks.

Socio-Technical Barriers: The implications of negligent mindsets and behaviours such as non-engagement being other actors may in turn possess limited visibility, awareness, discoverability of (a) project-information in and of itself; (b) who is required to support others and (c) who is working on what aspects of project-work.

Negligent mindsets and behaviours also cause cultural dysconnectivity and constrains transparency between collaborators. This by extension also leads to the information-sharing tensions, albeit induced via actors' own behaviours themselves.

Cultural causes of dysconnectivity are however distinct to causes posed via limitations of processes and technologies in enabling real-time connectivity across boundaries (internal / external). Conversely, mindsets and behaviours may in-part reflect such process and technological gaps due to the following gaps.

- Limited team-level actor interconnectivity and visibility. This provides non-compliant team-level actors an opportunity to not fully engage with needs of other team-level actors.
- Limited forward visibility of how information shared is utilised by other stakeholders. This leads to apprehension whether other collaborators utilise and secure information in line with information-owners wishes.
- Limited visibility of internal actor's activities and whether IM and IS in respect to their assigned task-work is suitable and secure. This was an issue in and of itself and also compounds inter-organisational trust issues.
- Trust issues may also be influenced by gaps of ensuring atomic visibility of inter-organisational information-flows as organisations possess limited visibility of external teams' task-work.

On the other hand, the enablers in implementing secure-collaboration requirements for project ecosystems and reducing potential for tensions were captured and explored.

Implications of Proposed Solutions: Networks would underpin atomic visibility and governance capabilities of information-flows. This would alleviate issues posed by intra-organisational actors' unsecure behaviours over IM and IS. It would also serve to provide more assurances and alleviate issues of apprehension in respect to inter-organisational collaboration. Negligent behaviours may also be deterred via adoption of networks to ensure real-time visibility between team-level actors in ensuring responsibilities to each other are met. Furthermore, process and technological advancements may serve as socio-technical enablers in improving internal actors' mindsets and behaviours. This in turn present the potential for cascading improvements at a cultural, organisational and project levels.

4.6.3 Research Analysis Summary

The analysis explored barriers and enablers to secure collaboration within projects that experts and their operations have faced during the project lifecycle. In view of research design, assumed tensions were identified, as were significant findings in differentiating and comparing issues of security-minded projects, and those with limited security focuses. At the time of the research design it was unclear to the extent of the differences faced. It has since been identified that whilst projects of elevated sensitivity face higher potential for security-collaboration tensions, it can also be said projects of lesser prolific nature face overlapping security concerns and associated tensions such as mindset and behavioural issues.

Moreover, the potential for elevated security risks is present at the onset of any project, and risk by nature is subjective to given clients and asset-owners themselves. As such, it should always be deemed necessary for such actors to proactively identify and appropriately govern security-risks, with respect to common sensitivity types as noted in **Section 4.4.4.2.** Project level governance includes choice of appointees where AEC projects are a melting pot of different types of entities, at different points in the project-lifecycle. The stakeholders can, in turn, influence the security-context of the project and whether it is appropriately mitigated.

Furthermore, a broad cross-section of potential suppliers within the sector bid for projects considered both elevated and lesser security-risk. The findings thus propose security-risk governance approaches are applicable and should be encouraged for industry at large. Moreover, this would serve to improve the baseline readiness of organisations across the AEC sector in approaching and handling projects in a security-minded manner, regardless of the level of security-risk displayed. Where projects of elevated security-risk however, the baseline readiness of the sector as a whole must be in adapted to be in a position to appropriately manage such projects in moving the built-environment forward in both digital and security-minded readiness.

Finally, it was posed as design-science research that there be a need to facilitate improved technological approaches in enabling secure and collaborative information-flows. This is true but with new-found knowledge that the industry as a whole faces broader issues that will require holistic efforts overlapping many areas of culture, mindsets, behaviours, processes and technologies. However, exploration of BIM governance and management issues has elucidated gaps that a governance-network could fill. These gaps apply for projects regardless of profile as they adopt the same underlying process and technological frameworks in many cases.

The following chapter will define necessary improvements as part of a framework for future secure and collaborative BIM processes. This framework focuses upon process and data concepts, with the implicit assumption an appropriate platform (i.e., future CDEs) would implement such concepts comprising atomic, pull-based processes. Detailed technical considerations of a proof-of-concept implementation is however beyond the scope of this research. The frameworks scope will aim to define and propose (a) the *route* the AEC industry must consider and (b) the underlying *concepts* software-vendors would appropriate and thereby expand upon within their specific software solutions.

5 Exploration of Secure BIM Collaboration Framework

5.1 Introduction

Based upon the issues and gaps extracted from analysis within Chapter 4, this chapter will outline a 'governance framework' towards securely (a) governing and (b) optimising the collaborative potential of BIM project processes and their information-flows. It is also noted the governance framework as a whole comprises the structuring and enabling aspects of information-flows, as these features must logically be present in-order for governance to occur over them.

The framework is a 'to-be' type of approach in structuring, enabling, and governing atomic, pull-based BIM information-flows. At the highest-level, the framework comprises requirements for 'what' should occur with respect to these key features of BIM projects, their processes and information-flows. The high-level requirements are explored in **Section 5.2**.

Concepts are also explored at a further layer of detail. This is from the perspective of actors involved as part of planning, enabling and governing, and their interactions in doing so. The actor's procedures are explored at a high-level throughout **Section 5.3.** Section 5.3 thus builds upon and details how requirements could be met. This is in expanding upon the conceptual 'patterns' to be considered for implementing proposed methods for inherently secure collaboration.

The framework must also consider high-level requirements of a type of data schema to support the aforementioned features of BIM projects, the types of actors involved, and their interactions. The schema and its concepts only explored to the extent that it can represent conceptual entities and underpin other requirements. It is also depicted in full in **Section 5.4.2** *only after* incremental exploration throughout **Section 5.3.** of the framework's concepts.

To summarise, the overarching focus of the governance framework is a representation of proposed type of method for capturing, enabling and governing information-flows such that its implementation at both a project and process level should achieve inherently secure and optimised collaboration and IS. The framework is firstly explored via high-level requirements from the perspective of actor's procedure types. This ties into the implicit need that in implementing the method posed, appropriate system architecture is required. This would comprise network-infrastructure architecture, functionality, and user-interfaces. It would also require specific data model implementation (in representing the concepts and a fully developed schema would cumulatively represent).

Such factors are outside of the research-scope, as these may be vendor-specific choices. Moreover, the framework as requirements, concepts and overall propositions must be further explored throughout industry in adoption from overlapping process, technological and contractual perspectives. This is necessary as the framework only represents a starting point of a potential method, which will require further research to get there. This expanded upon within **Chapter 6** as validation feedback and future work in **Chapter 7**.

5.2 Framework Requirements Introduction

This section captures the framework's requirements as needs for secure collaboration which reflect the joint-gap analysis of the current 'as-is' from **Section 4.5.3**. The requirements to be explored are positioned as proposals for change in the underlying methodology for BIM processes and considerations for BIM systems in adopting such methodological changes. Requirements are explored here from the perspective of: (a) actor's themselves and (b) their procedures / interactions in planning, enabling and governing processes and information-flows.

Actors include governing-roles (GRs) as a combination of digital BIM management and security competencies, team-managers (TM) as a localised governance and management capacity and individual disciplinary professionals as team collaborators (TCs). These actors were abstracted via research-analysis of the core *types* of actors present within the 'as-is' whilst representing future ideas of their competence, responsibilities and interactions as part of new approaches. The explored requirements are presented via a matrix of following overlapping perspectives.

- **Requirements of Actor type**: Governing and Management type actors. Collaborating (Team and Individual) type actors.
- **Requirements of a type of procedure**: (a) Capturing, (b) Enabling and (c) Governing BIM Processes and Information-Flows.

Requirements are explored simultaneously in view of both (a) actor type and (b) the types of activities most relevant to a given actor. For example, the following section introduces a subset of the process-capture requirements most applicable to governing / management actors. Also, these requirements are focused upon 'what' must change of the common procedures / patterns of enabling and governing BIM information-flows. They also overlap with technological considerations due to the intertwined process and data-driven nature of proposals.

5.2.1 Inter and Intra Organisational Planning Requirements

This section outlines requirement for how information-planning and thereby initial process capture, should occur within and between organisations from onset of an organisation's appointment, and thereafter extend throughout the lifetime of arrangements. Accordingly, these requirements aim towards change of following factors.

- Ensuring detailed and agile definition of 'what' information responsibilities must be accomplished internally and 'how' they can be enacted in a security-minded manner.
- The effective and agile communication of internally defined information needs and responsibilities amongst external partners.

In other words, the proposed changes emphasise team and task level requirements, and how these factors span out across organisations. This is as opposed to requirements with emphasis on the organisational entity as a whole. Furthermore, these proposals aim to ensure definition of secure processes and transactions by ensuring that the correct actors (organisational and internal) are assigned.

Overall, requirements depicted within the following **Figure 5.1** are split between the inter-organisational and intra-organisational requirements, whilst displaying overlaps between the two. Finally, it should be noted these requirements assume an appointer has appointed an appointee in a security-minded manner cognisant of their project-role competencies. The tag-system for these requirement sub-domains comprise the following: (a) Inter organisational obligation capture (IO) and (b) Intra organisational process capture (IP). These tags are based upon the sub-type of process-capture explored within this section.

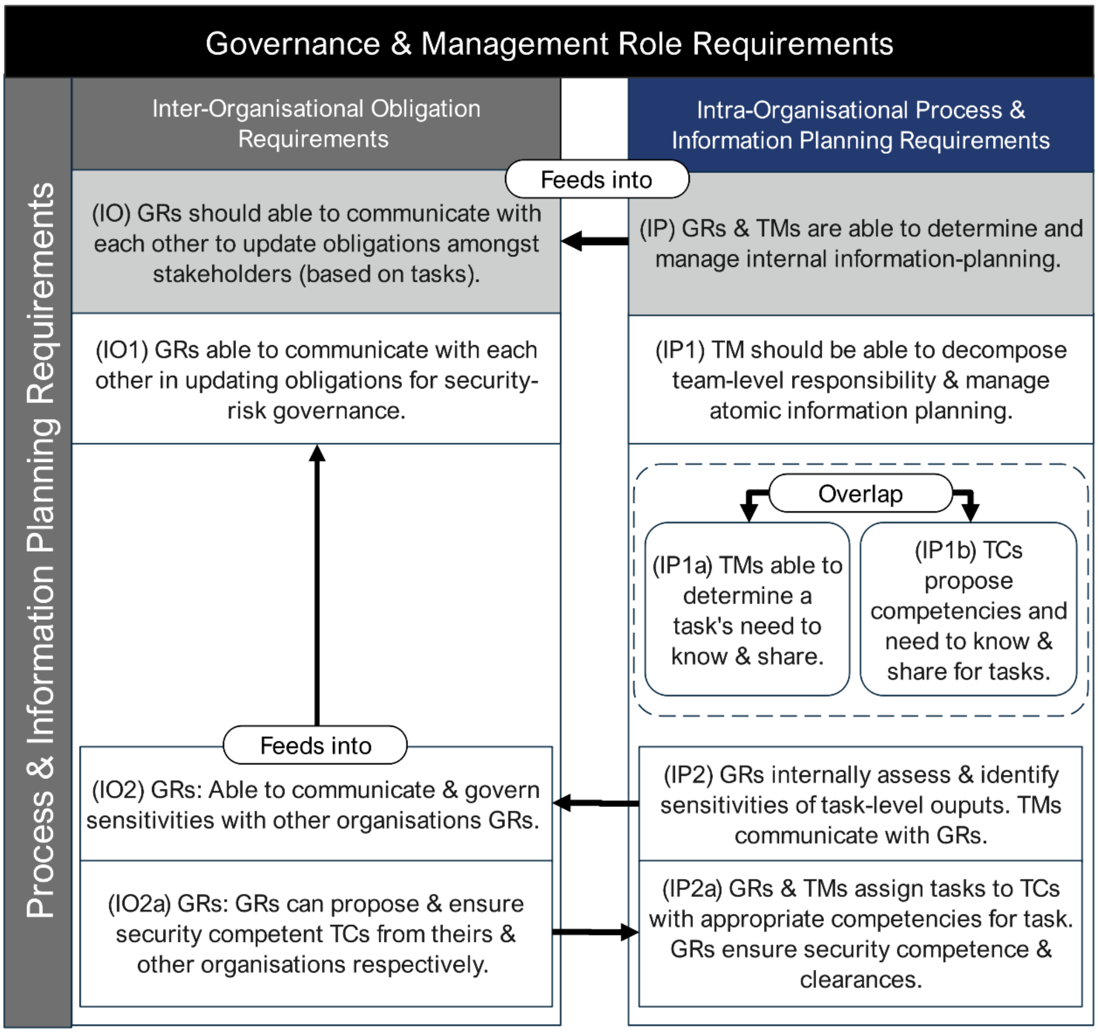

Governance & Management Role Requirements
Process & Information Planning Requirements
Inter-Organisational Obligation Requirements
Intra-Organisational Process & Information Planning Requirements
Feeds into
(IO) GRs should able to communicate with each other to update obligations amongst stakeholders (based on tasks).
(IP) GRs & TMs are able to determine and manage internal information-planning.
(IO1) GRs able to communicate with each other in updating obligations for security-risk governance.
(IP1) TM should be able to decompose team-level responsibility & manage atomic information planning.
Overlap
(IP1a) TMs able to determine a task's need to know & share.
(IP1b) TCs propose competencies and need to know & share for tasks.
Feeds into
(IO2) GRs: Able to communicate & govern sensitivities with other organisations GRs.
(IP2) GRs internally assess & identify sensitivities of task-level ouputs. TMs communicate with GRs.
(IO2a) GRs: GRs can propose & ensure security competent TCs from theirs & other organisations respectively.
(IP2a) GRs & TMs assign tasks to TCs with appropriate competencies for task. GRs ensure security competence & clearances.

Figure 5.1: Inter and Intra Organisational Obligation Capture / Information-Planning

Firstly, the directionality of overlaps between requirement sub-domains depicted in **Figure 5.1** represents how internally determined factors should feed into arrangements between organisations. This has been abstracted but could either be appointers or other partners. A further purpose of **Figure 5.1** is to convey proposals in ensuring appropriate clearances are present in accessing and handling of sensitivities. Such requirements, whilst general, are crucial. They reflect the need for any given collaborator to ensure effective governance. This includes ensuring that professionals possess the correct competencies. This is for both design and security competencies, where clearances should be *determined* by the security competence of a given professional. This approach is thereby also applicable and necessary for projects without sensitivity-tiers and clearance structures. It is further noted that certain activities occur first from the perspective of the project life cycle. For example, the definition of security-risk governance procedures is partly intra-organisational based in nature. **Figure 5.1** depicts that the determination of internal knowledge *should* feed into on-going inter-organisational security-risk governance and assurances of clearances, where both should occur throughout the lifecycle of any given appointee.

Finally, the overlap within **Figure 5.1** also depicts that definition of task-level responsibilities would need to *feed into* contractual obligations amongst stakeholders (partners / appointers). This specific perspective was however captured via expert feedback in **Section 6.3.6**. It is not part of the frameworks explored concepts in this chapter, but in line with the design-science method to capture a key theme to be considered for implementation of the type of approach posed. The following **Table 5.1 (following page)** provides additional context to the overlap of IO and IP areas, starting with the inter-organisational factors.

Inter-Organisational Obligations Capture:

Table 5.1: Inter-Organisational Obligations Requirements

Require-ment Codes	Inter Organisational Obligations Requirements	Requirement Details or Associated Requirements
IO	GRs should able to communicate with other organisations GRs to update obligations amongst stakeholders based upon on-going capture of task-level information-planning (IP1).	- A technology such as distributed ledgers may be required to underpin a contractual methodology of evolving *contracts* based on ID task responsibilities.
IO1	GRs able to communicate with each other in updating obligations for security-risk and thereby process and information-governance.	- *Feeds in* from IO2 which details on-going security-risk governance amongst stakeholders GRs.
IO2	GRs can communicate and govern sensitivities surrounding their and other stakeholders' information.	- Feeds in from IP2. Partners may *utilise* information non owned information. - i.e. they are not responsible for security-risk, but still necessary for stakeholders to communicate as part of a wider security governance approach.

IO2a	GRs can *propose* and *ensure* security competent TCs from *theirs and other* organisations respectively.	• TCs utilise sensitivities of other organisations; it is necessary for GRs (from both *owning* and *utilising* organisations) to ensure that security competent TCs access and manage.

The following **Table 5.2** depicts the second part of **Figure 5.1** as intra-organisational requirements for process and information-planning capture.

Intra-Organisational Process and Information Planning Capture:

Table 5.2: Intra-Organisational Process and Information Planning Capture Requirements

Code	Intra Organisational Requirements	Details or Associated Requirements
IP	GRs and TMs should be able to determine and manage internal task responsibilities (outputs) and information-needs (inputs).	
IP1	TMs should be able to decompose their team-level information-responsibility into task-level responsibilities which they should then be able to manage.	Concerns task-level information planning which leads to: • Identifying task IDs (Section 5.2.2.2). • Communicating organisational responsibilities (based on tasks) (IO1).
IP 1a	TMs should be able to communicate with their TCs in managing tasks. This includes determining factors of the task's scope and thereby information needs and responsibilities (need to know and share).	

IP1b	TCs can however propose their competencies for a task, details for the task responsibility and its outputs.	
IP2	Task-process capture feeds into internal security-risk governance and correspondingly identification of sensitivities associated with a task's information-outputs.	An organisational appointee may be responsible for governing sensitivities of partners. • If so, internal determination of sensitivities feeds into IO2. • This includes intellectual property owned by a given organisation but must be appropriately governed in sharing with collaborators.
IP2a	GR / TMs should assign tasks to TCs correspondent to a TCs competencies.	• Requires that a task's intended inputs and outputs have been identified (plus sensitivity). • TCs should be able to communicate their competencies (both disciplinary and security-oriented) and information-needs with their TM / GR.

5.2.2 Atomic Interconnectivity Requirements

This section introduces a sub-domain of information-planning for atomic task level inter-connectivity focused upon individual professional actors (TCs). It is an extension of internal process and information-planning within **Section 5.2.1** in ensuring an effective answer to the question of 'who' is required to support 'who else' for their task-work (internal and external), and what needs to be both shared and received between such actors. **Figure 5.2** depicts requirements for TCs (managed by TMs) in identifying IDs. The tag for these requirements is task-level inter-connectivity (IC).

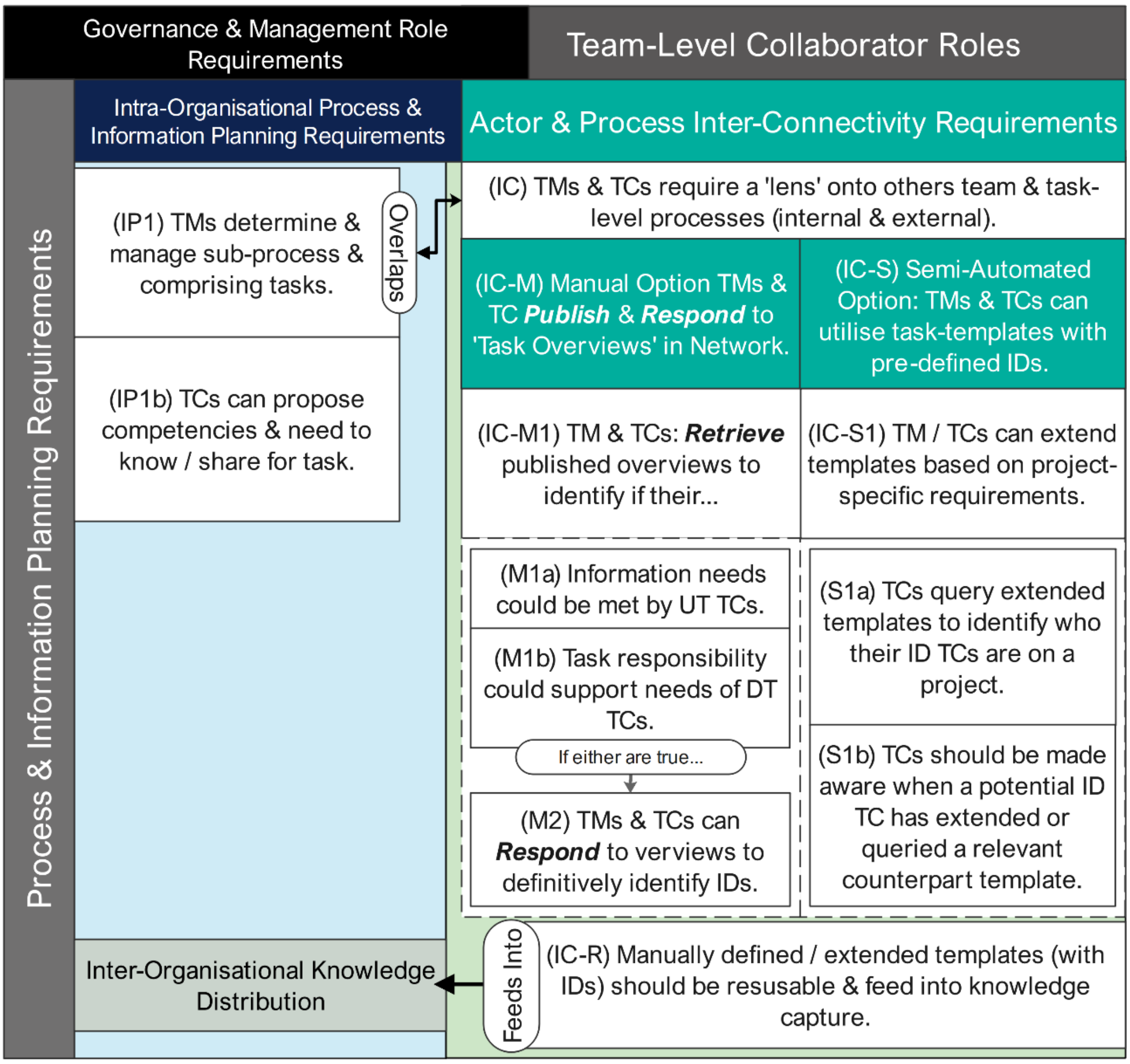

Governance & Management Role Requirements
Team-Level Collaborator Roles
Process & Information Planning Requirements
Intra-Organisational Process & Information Planning Requirements
Actor & Process Inter-Connectivity Requirements
(IP1) TMs determine & manage sub-process & comprising tasks.
Overlaps
(IP1b) TCs can propose competencies & need to know / share for task.
(IC) TMs & TCs require a 'lens' onto others team & task-level processes (internal & external).
(IC-M) Manual Option TMs & TC Publish & Respond to 'Task Overviews' in Network.
(IC-S) Semi-Automated Option: TMs & TCs can utilise task-templates with pre-defined IDs.
(IC-M1) TM & TCs: Retrieve published overviews to identify if their...
(IC-S1) TM / TCs can extend templates based on project-specific requirements.
(M1a) Information needs could be met by UT TCs.
(M1b) Task responsibility could support needs of DT TCs.
If either are true...
(M2) TMs & TCs can Respond to verviews to definitively identify IDs.
(S1a) TCs query extended templates to identify who their ID TCs are on a project.
(S1b) TCs should be made aware when a potential ID TC has extended or queried a relevant counterpart template.
Inter-Organisational Knowledge Distribution
Feeds Into
(IC-R) Manually defined / extended templates (with IDs) should be resusable & feed into knowledge capture.

Figure 5.2: Actor and Process Interconnectivity Requirements

Figure 5.2 also depicts the overlap between: (a) inter-connectivity and (b) intra-organisational process and information planning domains. The former domain extends the latter via the need to determine atomic overlaps of real-life counterpart professionals both intra and inter-organisationally. This as part of information-planning, should capture the bidirectional information-needs and information-responsibilities between professionals. These factors also feed outwards as part of inter-organisational capture. These requirements therefore address issues of dysconnectivity via needs of synchronicity and discoverability, so the process-structure is in place prior to enablement and governance of atomic sharing.

The following **Tables 5.3 and 5.4** break up the requirements depicted in **Figure 5.2** into two parts as a manual and semi-automated option.

Table 5.3: Team and Task Level Interconnectivity Requirements (1)

Code	Team and Task Level: Actor and Process Interconnectivity Requirements (Manual)	Details / Associated Requirements
IC	TCs require a 'lens' on-to others task-work. This entails *discovering* who can support who else. I.e. capturing IDs between actors and their tasks where any given TC will possess many IDs.	• Initial providing and receiving professionals are designated upstream (UT) and downstream (DT) respectively. • Thereafter any two TCs are ID if they possess mutual overlaps in their work – i.e. counterparts, acting in a requesting or sharing capacity to each other.
IC-M	Manual Option: TMs and TCs can publish 'overviews' of their tasks to the public network. They should also *respond* to other TCs published overviews. (The public network is a pool of published task responsibilities / needs. GRs / TMs would manage publication.)	
IC-M1	TMs and TCs in retrieving other teams' overviews should be able to identify: • **M1a:** If their information-needs (input) can be met by prospective UT TCs.	

	- **M1b:** If their information-responsibility (output) can support needs of prospective DT TCs.
IC-M2	TMs and TCs in *responding* to published overviews should be able to initiate dialogue with other TCs to definitively establish task IDs.

Table 5.4: Semi-Automated Interconnectivity Requirements

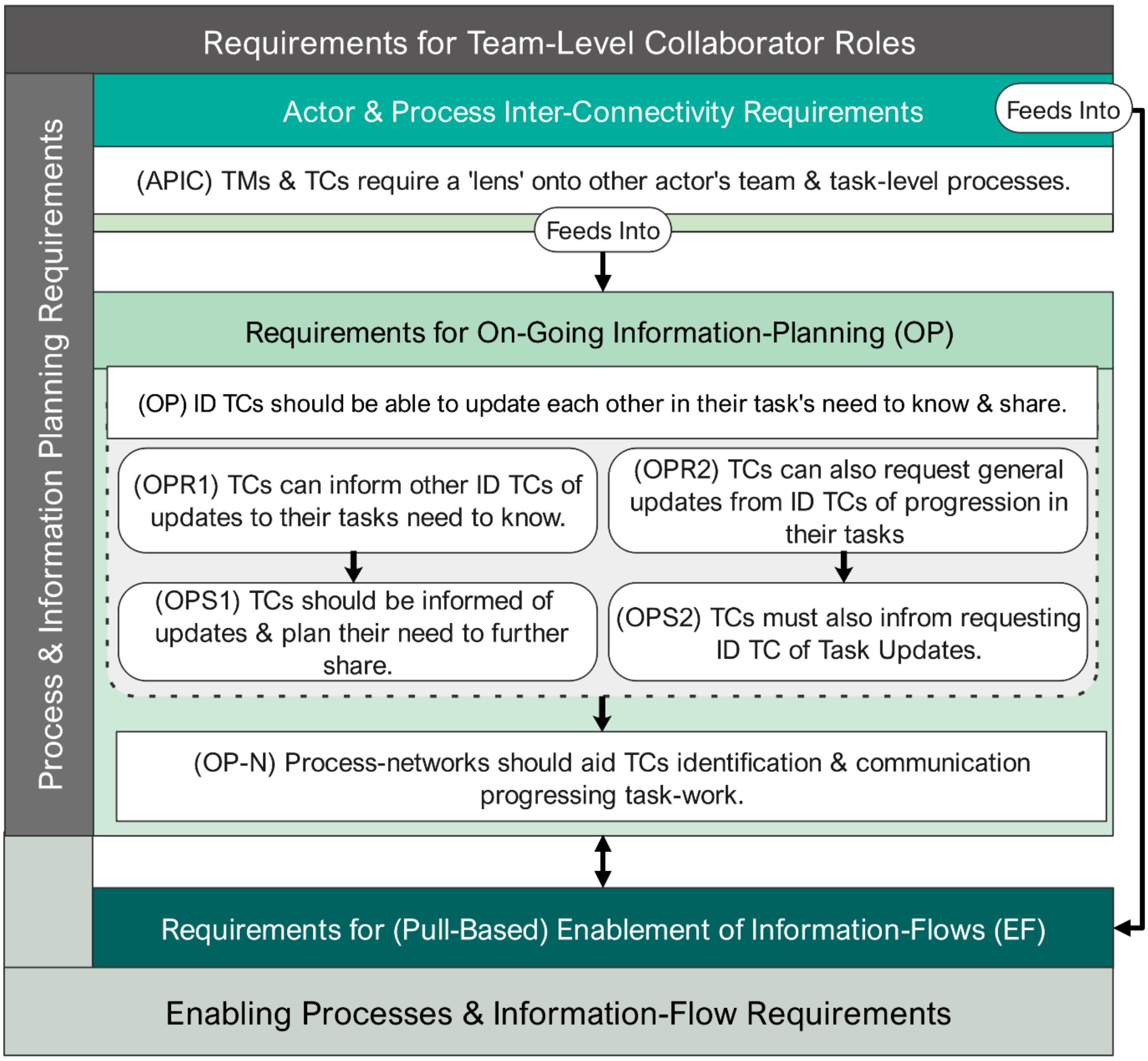
Code	Interconnectivity Requirements (Semi-Automated)	Details / Associated Requirements
IC-S	**Semi-Automated Option**: TMs and TCs can utilise task-templates with pre-defined IDs between different types of tasks.	**Task-templates**: Predefined types of tasks with pre-defined inputs and outputs. Instantiating a template with project-specific requirements extends it for project use.
IC-S1a	TMs and TCs can extend templates and thereafter query predefined IDs to identify counterpart (upstream) collaborating TCs.	• Upstream TCs should have instantiated counterpart templates. • This should make them aware of the tasks of other professionals (of relevance to them) without need for manual dialogue.

IC-S1b	TCs should be made aware of when other professionals have extended or queried a relevant counterpart template.	• Professionals are able to decide whether to *actualise* a predefined ID and release information in response to query. • May require modifying aspects of their task to fulfil requests (overseen by a GR / TM). Necessary when an upstream task implicates sensitivity.
IC-R	Manually defined / extended templates should feed into inter-organisational requirement setting. • As templates are extendable, reusability for future project processes should be gained. • This may also feed outwards that templated knowledge captured on a project be appropriately distributed via inter-organisational agreements.	

The final requirement of this domain as **'IC-R'** is relevant for both manual / semi-automated approaches. A final underlying motive for these requirements is that complexities of overlapping intra and inter-organisational atomic interlinkages would require an effective technological response. This is as the number of atomic inter-connections on real projects, comprising many different types of disciplinary activities, evolving over time must be able to be effectively captured, identified, and represented to in turn derive governance benefits from multiple perspectives. A principle is also noted in that actors who provide value to the process are able to connect, and plan and direct knowledge of what is and is not required.

5.2.3 Communication and Enablement of Information Flow Requirements

Figure 5.3 introduces two requirement domains which are: (a) on-going information-planning as well as (b) enabling pull-based information-flows. The former planning domain is a further extension of information-planning requirements. The following **Figure 5.3** depicts the requirements for this section.



Requirements for Team-Level Collaborator Roles
Process & Information Planning Requirements
Actor & Process Inter-Connectivity Requirements
Feeds Into
(APIC) TMs & TCs require a 'lens' onto other actor's team & task-level processes.
Feeds Into
Requirements for On-Going Information-Planning (OP)
(OP) ID TCs should be able to update each other in their task's need to know & share.
(OPR1) TCs can inform other ID TCs of updates to their tasks need to know.
(OPR2) TCs can also request general updates from ID TCs of progression in their tasks
(OPS1) TCs should be informed of updates & plan their need to further share.
(OPS2) TCs must also infrom requesting ID TC of Task Updates.
(OP-N) Process-networks should aid TCs identification & communication progressing task-work.
Requirements for (Pull-Based) Enablement of Information-Flows (EF)
Enabling Processes & Information-Flow Requirements

Figure 5.3: On-Going Planning and Exchange Requirements

In expanding upon **Figure 5.3**, the interconnectivity requirements (**Section 5.2.2**) also feed into exchange requirements to represent the first transaction between collaborating TCs. The sub-domain of on-going information-planning also overlaps the exchange domain where progressive information-planning provides up-to-date knowledge for progressive enablement of exchanges. This is reflective of progressive iterations and thus information-flows between professionals required to progress disciplinary work. Correspondingly, communication of needs and responsibilities between ID TC is also required via methods posed.

The following **Table 5.5** is associated with the requirements from the perspective of the former sub-domain. This assumes initial IDs have been identified for a given task.

Ongoing Information Planning Requirements:

Table 5.5: Ongoing Information Planning Requirements

Code	Ongoing Information-Flow Planning	Details / Associated Requirements
OP	ID TCs should be able to update each other in their task's need to know and share.	On-going information-planning between ID TCs in communicating task updates (prior to progressive transactions).
OP R1 and S1	• **R1**: TCs in a requesting capacity can inform other ID TCs of updates to their tasks needs (automated via updating their own responsibility). • **S1**: TCs in a sharing capacity should be informed of these updates and respond appropriately in providing optimal data to progressive queries.	
OP R2 and S2	• **R2**: TCs can also request general updates from ID TCs of task progression. • **S2**: TCs Must also inform requesting ID TC of general task updates.	

OP-N	TCs should be able to leverage the network to identify and communicate evolving task (needs and responsibilities).	Pertains to leveraging a network in enabling TCs to visualise and interact with ID TCs in progressing knowledge of who needs to know and share what.

In respect of the detailed requirements noted in **Table 5.5** It should be noted that requirements (**AP R1 and S2**) are interlinked as are **(AP R2 and S2)**. They are interlinked from the perspective of actors in a requesting capacity as the triggering actor for pull-based information-planning, and thereby a response from a counterpart TC in a sharing / providing capacity. Of course, both requesting and sharing capacities for any given TC would fluidly overlap.

Furthermore, the context of requirement '**AP-N**' is that task updates should be propagated to TCs who thereby identify what additional information would support progressive task-iterations of their counterparts (known or otherwise). This could entail updating what they intend to share. The other perspective is ability to know what information to request and from who. It is presumed a networks inter-connectedness would provide the foundation for achieving these needs. The following section and **Figure 5.4** however expand upon the enablement aspect of requirements that are noted at a high-level in **Figure 5.3**.

Enablement of Information Flows Requirements: The following **Figure 5.4** depicts the second part of this section as the enablement of information-flow requirements.

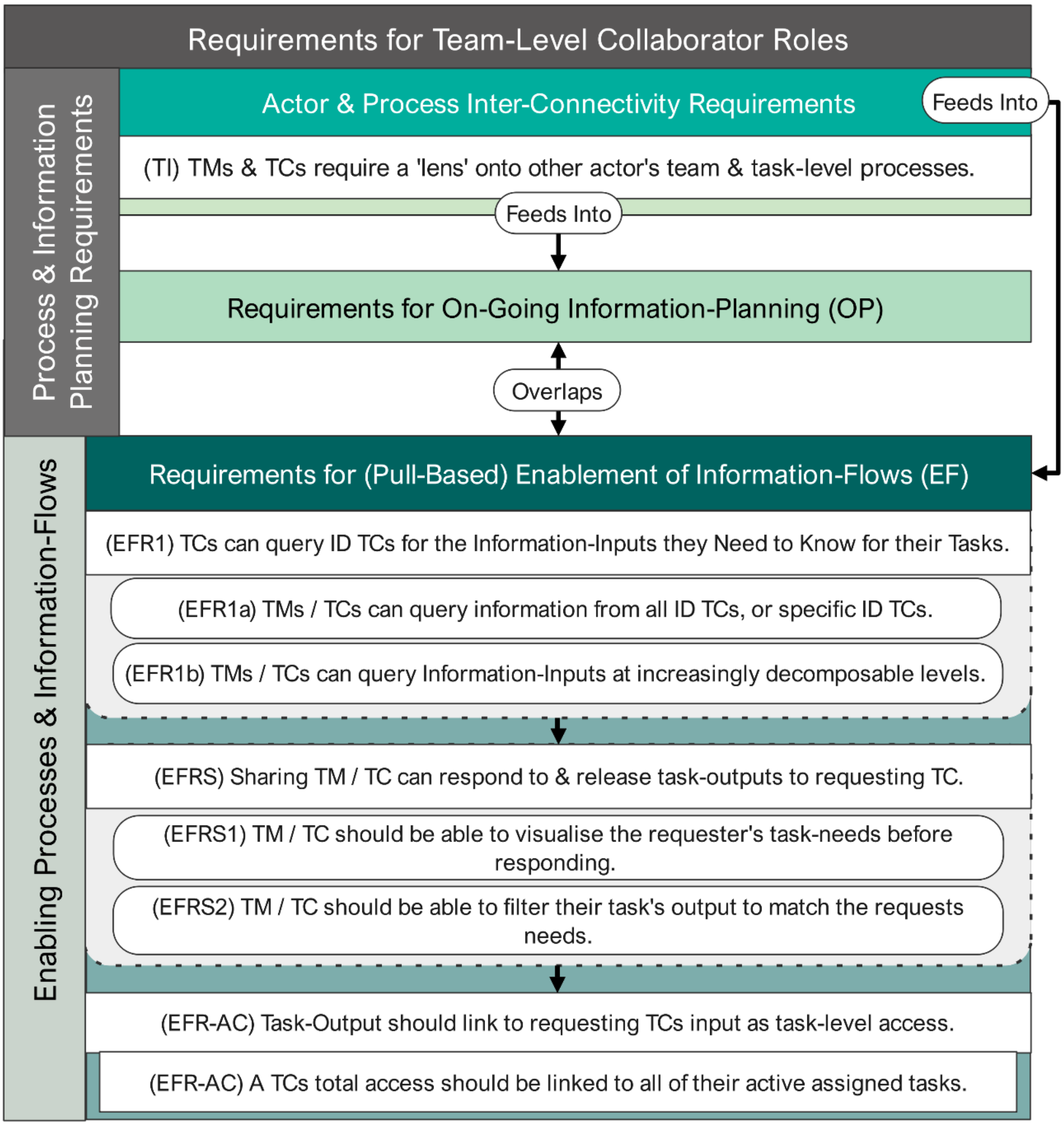

Requirements for Team-Level Collaborator Roles
Process & Information Planning Requirements
Actor & Process Inter-Connectivity Requirements
Feeds Into
(TI) TMs & TCs require a 'lens' onto other actor's team & task-level processes.
Feeds Into
Requirements for On-Going Information-Planning (OP)
Overlaps
Enabling Processes & Information-Flows
Requirements for (Pull-Based) Enablement of Information-Flows (EF)
(EFR1) TCs can query ID TCs for the Information-Inputs they Need to Know for their Tasks.
(EFR1a) TMs / TCs can query information from all ID TCs, or specific ID TCs.
(EFR1b) TMs / TCs can query Information-Inputs at increasingly decomposable levels.
(EFRS) Sharing TM / TC can respond to & release task-outputs to requesting TC.
(EFRS1) TM / TC should be able to visualise the requester's task-needs before responding.
(EFRS2) TM / TC should be able to filter their task's output to match the requests needs.
(EFR-AC) Task-Output should link to requesting TCs input as task-level access.
(EFR-AC) A TCs total access should be linked to all of their active assigned tasks.

Figure 5.4: Enablement of Exchanges Requirements

Having noted the overlap between the domains previously, the following table details requirements for actualisation of information-planning procedures between TCs. In other words, these requirements detail the pull-based enablement of transactions, and thereby TCs access to information. As seen, there is a fluid overlap between on-going information-planning and pull-based enablement.

Table 5.6: Enabling Information-Flows Requirements

Code	Enablement of Information-Flows	Details / Associated Requirements
EFR1	TMs / TCs in a requesting capacity can query (pull) the information required from ID TCs.	• Queries are based upon the requesters information-needs. • Requests are pending until governed, as such the sharer can choose what and what not to share.
EFR1a	TMs / TCs can query information-inputs (access) at increasingly decomposable levels.	
EFR1b	TMs / TCs in a requesting capacity can pull information from all ID TCs, or specific ID TCs. I.e. TCs should be able to direct queries against one or many established IDs.	
EFRS	TM / TCs in sharing capacity should be able to respond to queries and release task-level outputs to requesting actors.	Interfaces with information-flow governance requirement. I.e. information governance occurs in response to queries and involves potential to filter outputs.
EFRS1	TMs / TCs should be able to visualise requester task's needs before responding to requests.	

EFRS2	TMs / TCs should be able to filter task's outputs to match the requesters needs.	
EFR-AC	Released task outputs should link to requesting TCs input and by extension their access-rights.	A TC's total access should be based upon all active tasks assigned to them.

5.2.4 Process and Information Flow Governance Requirements

This section expands upon the final sub-domains for GRs who are required to govern the enablement of the manner of information-flows as explored in **Section 5.2.3.** It should be noted that GRs hold precedence over TMs who act in a localised governance-capacity over their own teams. GRs govern the connections internally and externally as a whole. The requirement domains are depicted within **Figure 5.5** and is then expanded upon.

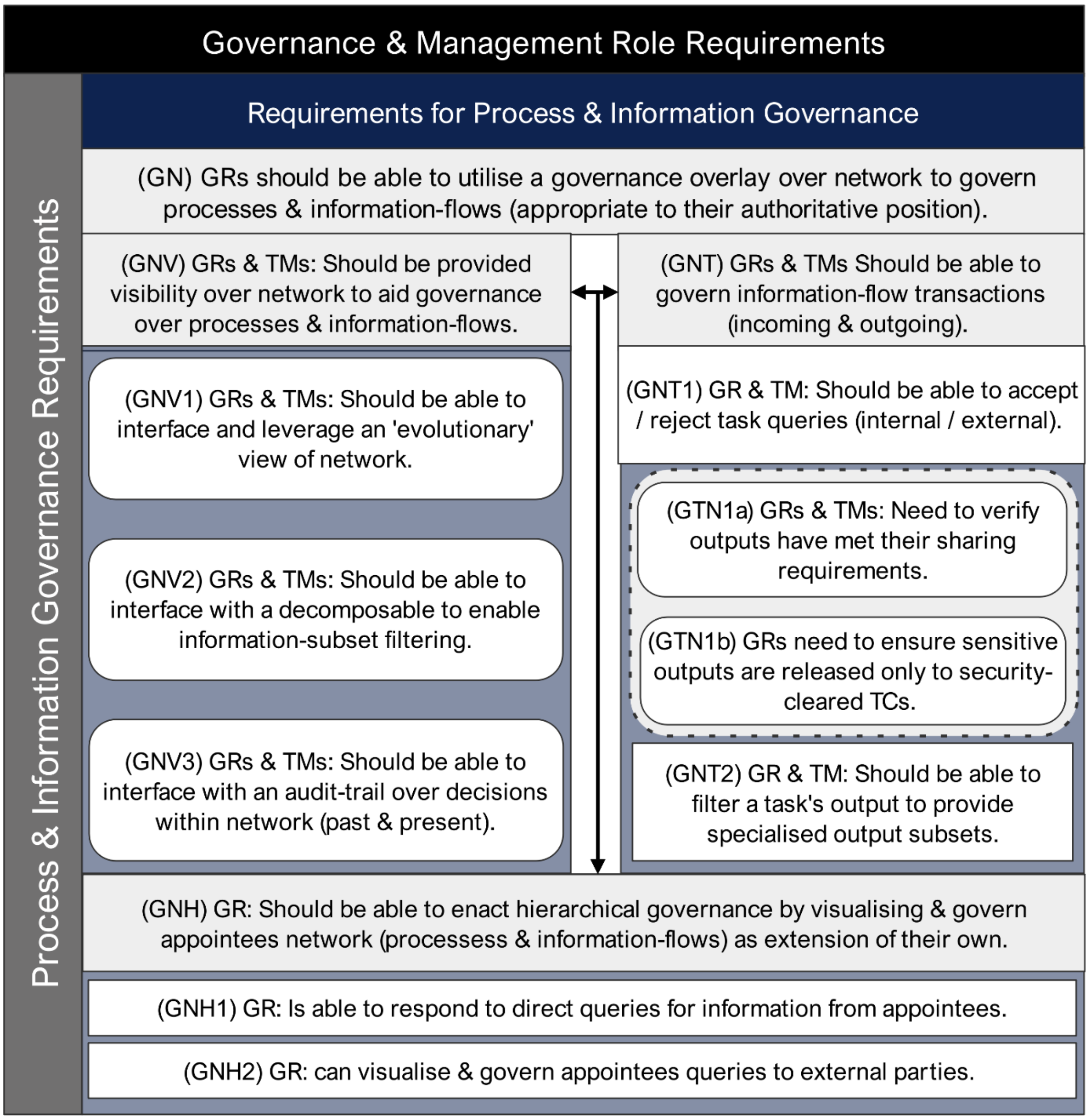

Governance & Management Role Requirements
Process & Information Governance Requirements
Requirements for Process & Information Governance
(GN) GRs should be able to utilise a governance overlay over network to govern processes & information-flows (appropriate to their authoritative position).
(GNV) GRs & TMs: Should be provided visibility over network to aid governance over processes & information-flows.
(GNT) GRs & TMs Should be able to govern information-flow transactions (incoming & outgoing).
(GNV1) GRs & TMs: Should be able to interface and leverage an 'evolutionary' view of network.
(GNT1) GR & TM: Should be able to accept / reject task queries (internal / external).
(GTN1a) GRs & TMs: Need to verify outputs have met their sharing requirements.
(GNV2) GRs & TMs: Should be able to interface with a decomposable to enable information-subset filtering.
(GTN1b) GRs need to ensure sensitive outputs are released only to security-cleared TCs.
(GNV3) GRs & TMs: Should be able to interface with an audit-trail over decisions within network (past & present).
(GNT2) GR & TM: Should be able to filter a task's output to provide specialised output subsets.
(GNH) GR: Should be able to enact hierarchical governance by visualising & govern appointees network (processess & information-flows) as extension of their own.
(GNH1) GR: Is able to respond to direct queries for information from appointees.
(GNH2) GR: can visualise & govern appointees queries to external parties.

Figure 5.5: Process and Information Flow Governance Requirements

The core requirement **(GN)** details GRs and TMs should be able to govern information-flows as the portions of the process network they have been given decision-rights over. This is with a view of both their internal TCs requesting information internally and externally and responding to task level queries. It also includes hierarchal governance of appointees. As noted by requirement **GNT1** in **Figure 5.5**, governance over actors' processes and information entails a motive for both information security and suitability as a further by-product of persistent synchronicity between professionals.

Accordingly, the framework posits GRs should be provided the necessary background knowledge to underpin decisions. In supporting understanding, systems could present different views of a network to visualise how internal flows overlap with those of external entities, and their TCs. This thereby provides GRs an 'overlay' over networked information-flows as a governance network from the perspective of GRs. An implementing system may also interrogate the network to provide GRs relevant inferences to support their understanding and thereby decision-making over transactions they are assigned to govern. The framework provides overarching considerations of the potential for such an approach. The following **Table 5.7** provides additional context to the requirements.

Table 5.7: Process and Information (Flow) Governance Requirements

Codes	Process and Information Governance Requirements	Details / Associated Requirements
GN	GRs should be able to utilise a governance overlay over network to govern processes and information-flows (appropriate to authoritative position).	
GNT	GRs and TMs should be able to govern information-flow transactions (incoming and outgoing).	Responses can be semi-automated / decided by the queried TC if no security implications.
GNT1	GR and TM should be able to accept / reject instances of task query (internal / external).	This is relative to authoritative position and should be informed based upon on-going governance.
GNT1a	GRs and TMs should be able to verify exchanges have met their IS requirements.	This overlaps with task template concept in extending from (in modifying) initial task-requirements.
GNT1b	GRs and TMs should be able to ensure that sensitive outputs are released only to security cleared TCs. (This requires initial dialogue with other organisations GRs.)	• On-going governance of task-iterations should be achievable. • This could be enabled by evolving networked visibility / functions of processes and associated information-flows.

GNT2	GRs and TM should be able to filter a task's cumulative outputs to provide an output-subset specific to the querying TCs information-needs.	Enabler for ensuring suitability and security of exchanges via following capabilities. • Task-decomposability of BIM objects elements referenced against a project's spatial-map. • A decomposed view of a task's cumulative outputs should enable filtering in defining subsets.
GNV	GRs and TMs: should be provided visibility over network to aid governance over processes and information-flows.	
GNV 1	GRs and TMs should be able to interface and leverage an 'evolutionary' view of network. I.e. governance over the process-network over time.	
GNV 2	GRs and TMs should be able to interface with a decomposable to both govern enable information-subset filtering. I.e. interfaces to enable the ability to effectively filter, create and manage information-subsets to specific actors. This requirement is also relevant to TCs.	
GNV3	GRs and TMs should be able to interface with an audit-trail over decisions within network (past and present).	

GNH	GR should be able to enact hierarchical governance by visualising and governing appointees’ network (processes and information-flows) as extension of their own.	
GNH1	GR should be able to respond to direct queries for information from appointees.	
GNH2	GR should be able to visualise and govern appointees’ queries to external parties.	Via the frameworks posed methods, appointees possess the potential to query from across direct chains of appointment. The contractual mechanisms to underpin this feature are however out of scope.

5.3 Exploration of Governance Framework Concepts

5.3.1 Introduction

This section will delineate the framework concepts. The requirements proposed within the previous section are explored via a series of figures within sub-sections. The following details the structure for exploration of the framework's concepts which will start from more general and work towards more detailed concepts.

- **Section 1 (5.3.2)** – Exploration of Core Task Construct: This section explores key features of a task construct to underpin actors in capturing, enabling or governing information-flows, these factors will be expanded upon throughout sections.
- **Section 2 (5.3.3)** – Exploration of Basic Conceptual Methods: This section focuses upon on an overarching overview of how actors would (based upon the basic constructs delineation) be able to plan, enable and govern. This section therefore provides high-level to actor's patterns that may be considered for implementation.
- **Section 3 (5.3.4)** – Exploration of [Further] Governance Constructs: This section explores further the concepts to enable decomposed filtering of subsets and task-templates. These concepts are necessary for effective governance.
- **Section 4 (5.3.5)** – Exploration of Governance Network Concept: This section explores high-level proposed ideas that a governance-network could aim to fulfil.
- **Section 5 (5.3.6)** – Summary of the framework as a whole. This includes an overarching representation of the requirements explored within **Section 5.2** and high-level considerations of requirements for a schema that could underpin the methods explored (concepts and requirements as a whole).

5.3.2 Exploration of Task Construct

This section explores the concept of a 'Task' as the core data entity to underpin planning, enablement, and governance of actor's atomic information-flows. The task construct must first be defined prior to exploring further conceptual methods in **Section 5.3.3**. The key proposal is that task-based responsibilities and associated exchanges should explicitly be captured, enabled, and governed via data-driven approaches. This comprises the following benefits.

- Atomic information planning and exchange is consistently structured, and comprehensively and constantly visible by appropriate parties.
- Atomic information-needs and thereby access can be met by another task's information-responsibility and thereby outputs.
- Atomic information-planning is interdependent. A given unit of work in meeting collaborating TCs information-needs can also receive information in response.
- Atomic information-planning is updated as needs and responsibilities progress. This is simultaneously from the perspective of a given professional (TC) and of their collaborating TCs.
- Atomic exchanges occur in response to pull queries, and *only* in meeting the requesting TCs information-needs (no more, no less).
- If information requested is sensitive the overriding principle is the 'need to know' of any given professional and their security-clearance.
- Verification of the output also occurs before response in explicit view of the requesters need; validation of suitability and security exchanges should thereby occur by default.
- Tasks possess a direct link to actual project-data generated and thereby shared to other TCs to form their access. Planning, exchange, and access thus become a fluid procedure.

These aforementioned strengths are proposed to enhance governance for security and suitability of information-flows. More broadly, the aforementioned benefits ensure a tighter link between BIM process information-requirements and the data that is actually generated. The following definitions characterise the first two constructs required for task-level exchanges.

- **Task-Sets**: A task-set is essentially a sub-process managed by team-managers (TMs) as their cumulative team-level responsibility. A task-set is also seen as a localised team-level aspect of the process and collaborator network.
- **BIM Task**: A BIM task is an atomic unit of work that is assigned by a TM and undertaken by an individual team collaborator (TC) to produce a desired result (i.e. to meet the information-responsibility of the task.) The tasks of focus pertain to the generation of BIM design-information.
- **Sub-Tasks**: Decomposed responsibilities in respect to operations that must be carried out on individual / groupings of BIM object elements which form a cumulative task responsibility.
- **Information Flow Directionality**: Atomic information-flows occur between tasks. Downstream tasks are dependent upon inputs from preceding upstream tasks before undertaking their initial task iteration. BIM process-flow can thereafter be interdependent where professionals are able to request, inform and receive in view of their counterpart TCs.

The following **Figure 5.6** also provides a diagrammatic representation of these concepts.

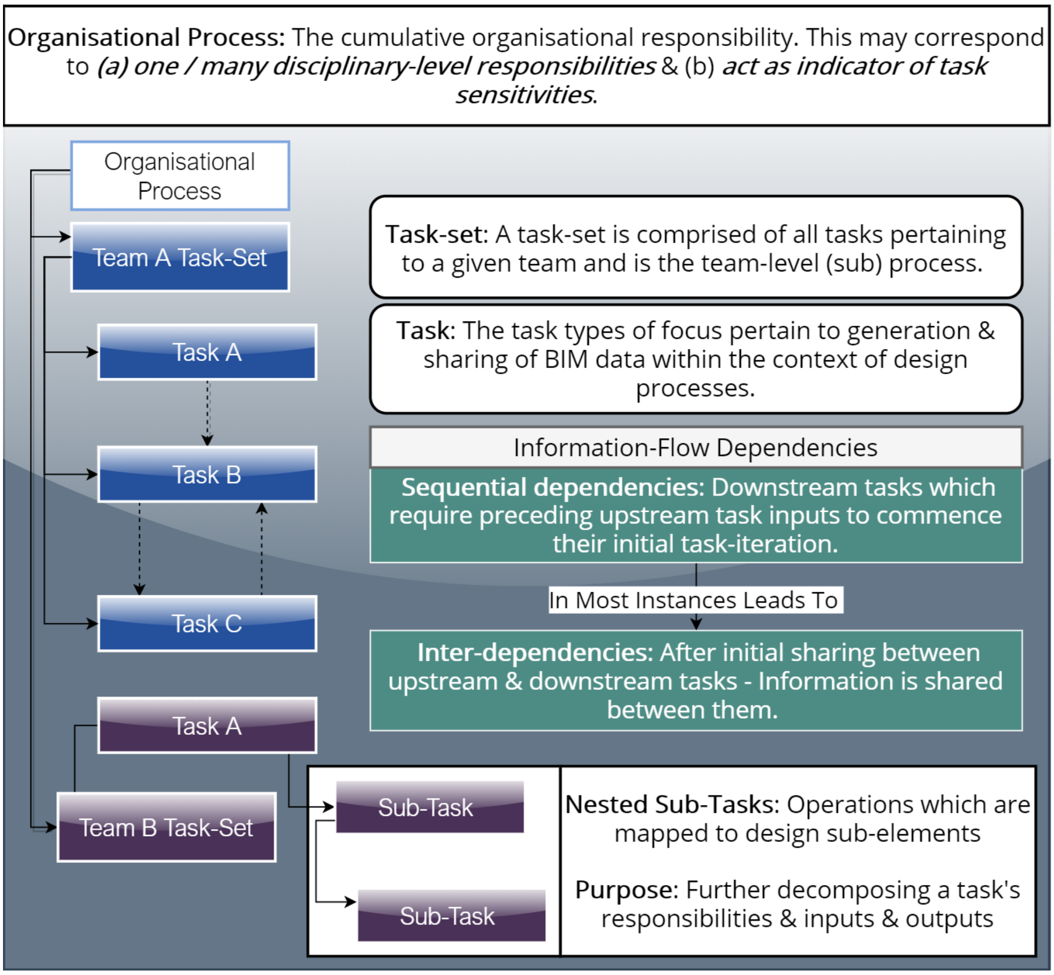

Organisational Process: The cumulative organisational responsibility. This may correspond to (a) one / many disciplinary-level responsibilities & (b) act as indicator of task sensitivities.
Organisational Process
Team A Task-Set
Task A
Task B
Task C
Task A
Team B Task-Set
Sub-Task
Sub-Task
Task-set: A task-set is comprised of all tasks pertaining to a given team and is the team-level (sub) process.
Task: The task types of focus pertain to generation & sharing of BIM data within the context of design processes.
Information-Flow Dependencies
Sequential dependencies: Downstream tasks which require preceding upstream task inputs to commence their initial task-iteration.
In Most Instances Leads To
Inter-dependencies: After initial sharing between upstream & downstream tasks - Information is shared between them.
Nested Sub-Tasks: Operations which are mapped to design sub-elements
Purpose: Further decomposing a task's responsibilities & inputs & outputs

Figure 5.6: Task Constructs (1)

It is depicted in **Figure 5.6** that 'Task' constructs act as a container, for an atomic information-responsibility to be met in view of other ID tasks atomic information-needs (in achieving their own information-responsibility). Accordingly, there is an explicit link between the assigned information-responsibilities of professionals and the information that is *actually* generated, exchanged, and thereby accessed. This is achieved via associating the core task construct with adjoining need to share components, which thereby feed into the need to know (information-needs) of receiving tasks. This approach enables principles of: (a) a directed stream of connectivity between tasks sharing and receiving information and (b) the ability to govern atomic exchanges and validate their suitability and security.

In line with the aforementioned information planning and enablement principles for information-flows, tasks possess the adjoining constructs depicted in the following **Figure 5.7**.

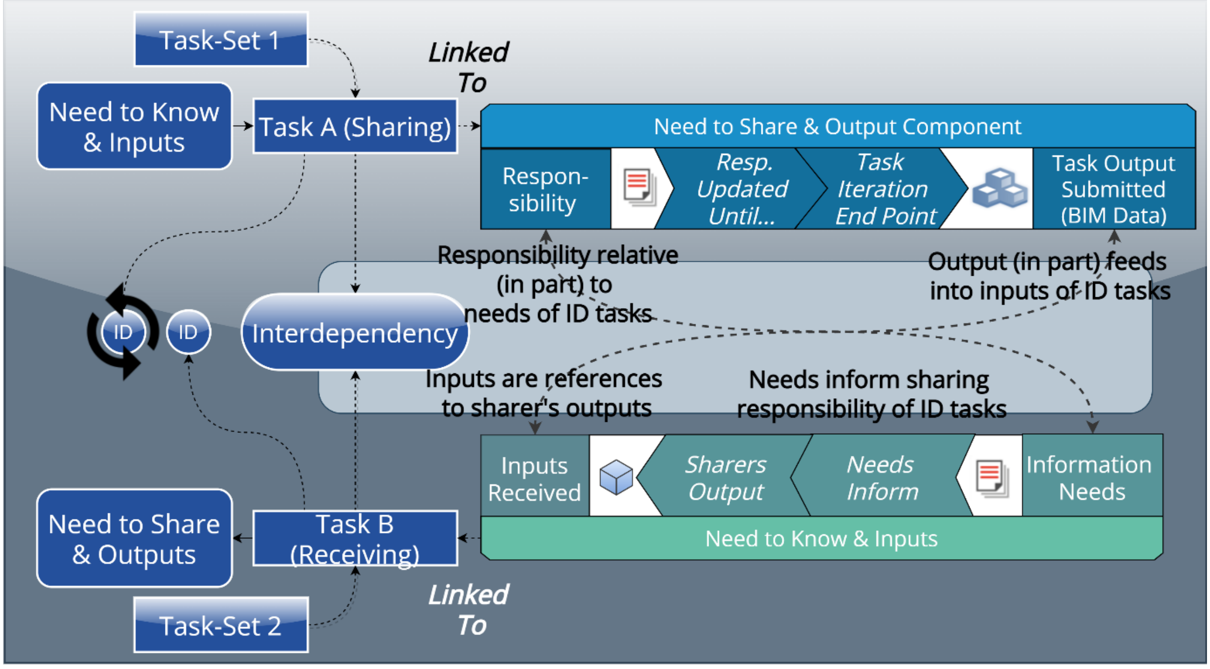


Figure 5.7: Task Constructs (2)

Within **Figure 5.7**, the task is depicted as the central construct. Its adjoining concepts are: (a) the need to share and output component; (b) the need to know and input component and (c) interdependencies with other tasks. These components are able to represent the planning and enablement perspectives of generating, sharing and receiving / accessing of information between collaborating TCs. The following points adds context to each component.

Need to Know and Input Component: The need to know being a task's information-needs in enabling a TC to most effectively undertake their task-responsibility whilst not providing irrelevant information or factors sensitive or may imply as such unless the actor possesses the 'need to know' and is competent and cleared.

- The input in turn is based against a task's need to know and determines the cumulative information-set any given task can access. A task's need to know component may possess different states throughout the project-lifecycle (expanded upon in summary).

- Need to Know components are linked to the Need to Share components of multiple other tasks as well as resources such as design-planning guidance. This context of bi-directionality feeds into the next factor.

Need to Share and Output Component: These components pertain to a task's information responsibilities. The generation aspects pertain to a task's *cumulative* responsibility to generate outputs. This cumulative responsibility is based on what needs to be shared to satisfy information-needs of *multiple* inter-dependent professionals, and their tasks. A given task's need to share / information-output can therefore be subset to provide the *specific* input required in response to the needs of *specific* collaborating TCs.

Task Interdependency Component (ID): A given task ID component characterises connectivity between two tasks in setting requirements over, and actualising exchanges. A task ID is therefore a high-level conceptual link between: (a) the needs and thereafter inputs of a given task with (b) the responsibilities and thereafter outputs of another interdependent task. The following points provide further context.

1. The responsibilities of the upstream task are relative in-part to the needs of downstream tasks. Correspondingly, a task's needs inform multiple other interdependent tasks and their responsibilities.
2. The 'in-part' and 'multiple' relationships respect how a given task possesses interdependencies with multiple other tasks.
    a. As part of any task ID, an initial downstream receiving task requires inputs from an upstream sharing task.
    b. After the initial flow of information between an upstream and downstream task, an ID characterises that both tasks should be able to share and receive information

between each other as part of progressive task-iterations (depicted by the loop around an ID component in **Figure 5.7**).

c. I.e. their needs and responsibilities are relative to, and persistently in view of each other. This persistency extends to multiple other IDs any given task may be linked to.

IDs between tasks and by extension, their assigned TCs can be captured either manually (**Section 5.3.3.1**) or via task-templates which capture predefined IDs between generic task-types (**Section 5.3.5**).

Summary: This section has introduced core concepts of the framework, explored from the perspective of constructs necessary to encapsulate and provide a container for atomic exchanges and governance thereof. The need to know and share perspectives represent the planning perspective whilst input and output perspective pertain to realisation of an exchange after information is submitted against a task in line with the plan perspective. The following provides detail over how tasks can also go through multiple revisions.

- Initial Iteration: Information-needs are represented as simple requirements linked to a task-type to provide context to the sharing party of what information to share. It is posed within **Section 5.3.5** that tasks extended via templates can simply query based upon pre-defined types of relevant information.

- Ongoing Iterations: This state is reached after initial receipt of information initial task-iteration. A task's requirements can be refined and may pose constraints on other ID tasks.

  - Moreover, this state enables on-going information-planning and transaction iterations between ID tasks. From the perspective of a TC, sub-tasks may be attached to their cumulative responsibility to be communicated with established TCs (**Sections 5.3.4**).

- Task Closeout: No further iterations are required as the responsibility associated with the task is finalised. Accordingly, input-access associated with a task and TC is closed down. The final closed out task however represents all iterations, and atomic interactions with other tasks throughout its lifetime.

The following **Section 5.3.3** will expand upon the essential 'construct' to represent the concepts to be considered sin enabling the governance-framework.

5.3.3 Exploration of Conceptual Methods

This section relates the task construct to conceptual methods explored in meeting the information planning, enablement, and governance requirements of the framework. This is at an overarching level, and some of these concepts will be revisited after introducing the task-decomposability concept as a means to structure exchange at whichever level of atomicity is needed.

It is also noted the core framework focuses are at the level of professionals and their tasks. Teams as a whole are considered within this section to provide a high-level view of transactions between organisations at various levels of stakeholder granularity. Such 'team' factors are valuable in consideration of aggregated modes of collaboration and managed information-delivery which are still further decomposed than the organisational-level. Team inter-connections are also necessary to consider as a starting point in task-level discoverability as explored in the next section as part of process and information-planning concepts.

5.3.3.1 Process and Information Planning Capture

This concept is in response to limited visibility of collaborators task-level work and thus recognition of relevancy in servicing their own needs / providing to others. This section thereby details actors' interactions in initial process ID capture, which also occurs throughout the project-lifecycle when new: (a) actors are appointed and (b) new task responsibilities and needs are defined.

Novel approaches are required to enable dialogue to form internal and external IDs between teams and their tasks. A system underpinning these discoverability and atomic dialogue characteristics (directly between professionals) would enable TMs / TCs to capture detailed overlaps between other teams and their professional's tasks. Once these IDs have been identified, they can thereafter be updated and maintained throughout task-iterations until a given unit of work has been closed out. The following figure a provides a depiction at the higher level between TM actors in capturing the overlaps, and thereby knowledge of where information must be managed in delivery.

Figure 5.8 depicts how actors define team-level sub-processes, and form IDs between them. TMs in figure a are depicted in an intra-team responsibility perspective. This overlaps the depicted outwards-facing perspective in a potential upstream and downstream capacity (i.e. identifying IDs with other actors).

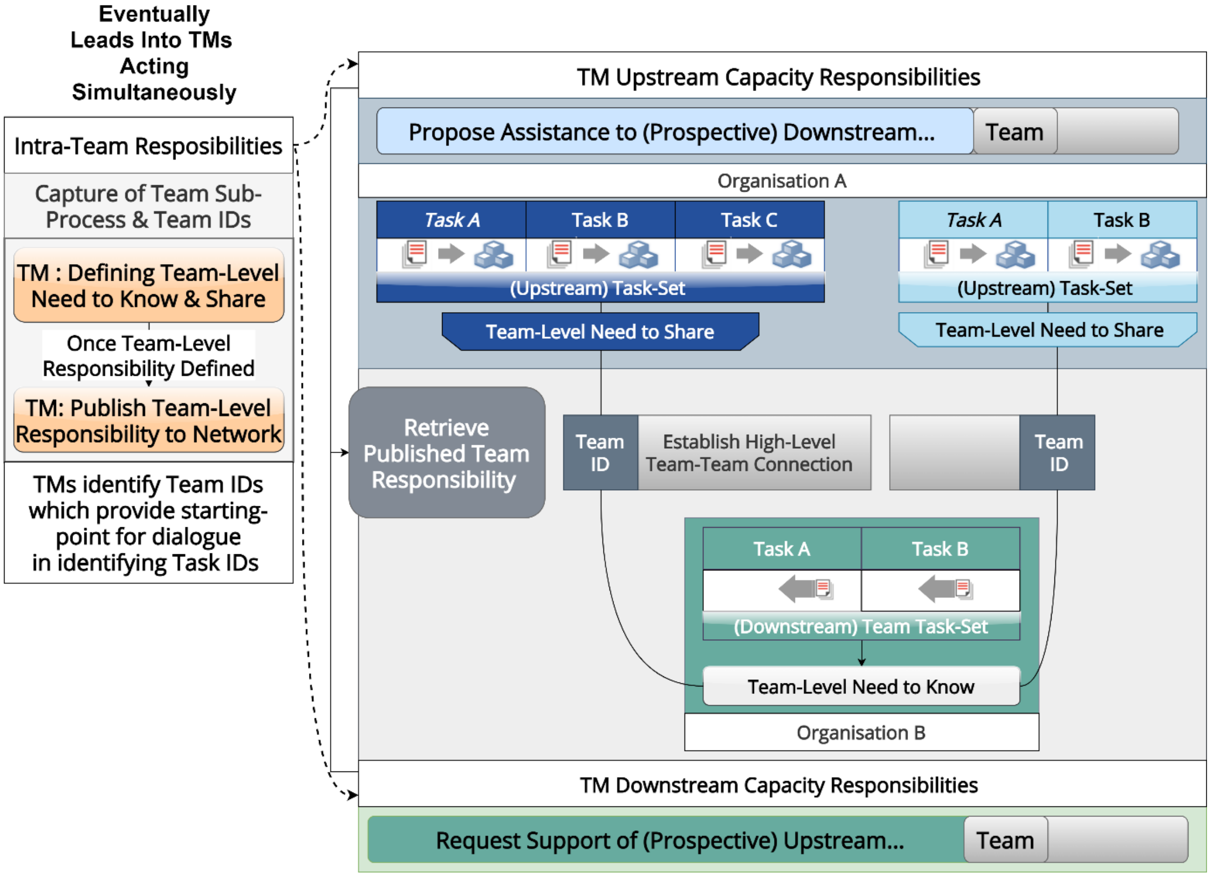

Eventually Leads Into TMs Acting Simultaneously
Intra-Team Resposibilities
Capture of Team Sub-Process & Team IDs
TM : Defining Team-Level Need to Know & Share
Once Team-Level Responsibility Defined
TM: Publish Team-Level Responsibility to Network
TMs identify Team IDs which provide starting-point for dialogue in identifying Task IDs
TM Upstream Capacity Responsibilities
Propose Assistance to (Prospective) Downstream...
Team
Organisation A
Task A
Task B
Task C
(Upstream) Task-Set
Team-Level Need to Share
Task A
Task B
(Upstream) Task-Set
Team-Level Need to Share
Retrieve Published Team Responsibility
Team ID
Establish High-Level Team-Team Connection
Team ID
Task A
Task B
(Downstream) Team Task-Set
Team-Level Need to Know
Organisation B
TM Downstream Capacity Responsibilities
Request Support of (Prospective) Upstream...
Team

Figure 5.8: Team Interconnectivity Capture

The following subtitle provides further context to pattern depicted in **Figure 5.8.**

Team-Level ID Capture: The definition of IDs between teams and their sub-processes requires dialogue between TMs. TMs would publish detail of their team-level responsibility to the process network for the purpose of identifying team IDs in providing and receiving information at team-level.

- Prospective Downstream TMs would then retrieve published team-level responsibilities and request the support from prospective upstream teams and their TMs.
- Prospective Upstream TMs would retrieve published team-level responsibilities and propose support for prospective downstream teams and their TMs.

The GRs of each organisation would govern external interaction and formalise these team-level IDs as part of the process network. TMs thereafter act simultaneously in an up and downstream capacity in view of other TMs published team-level responsibilities. These TMs would also be responsible for ensuring a managed response of information in response to organisational or client-led questions for progression points. TMs may also be delegated the responsibility by GRs to formalise task-level IDs.

In other words, further information inter-connectivity requirements at the level of TCs themselves. This is depicted in the following **Figure 5.9**. This adds more detail to **Figure 5.8** from the perspective of individual level actors within teams.

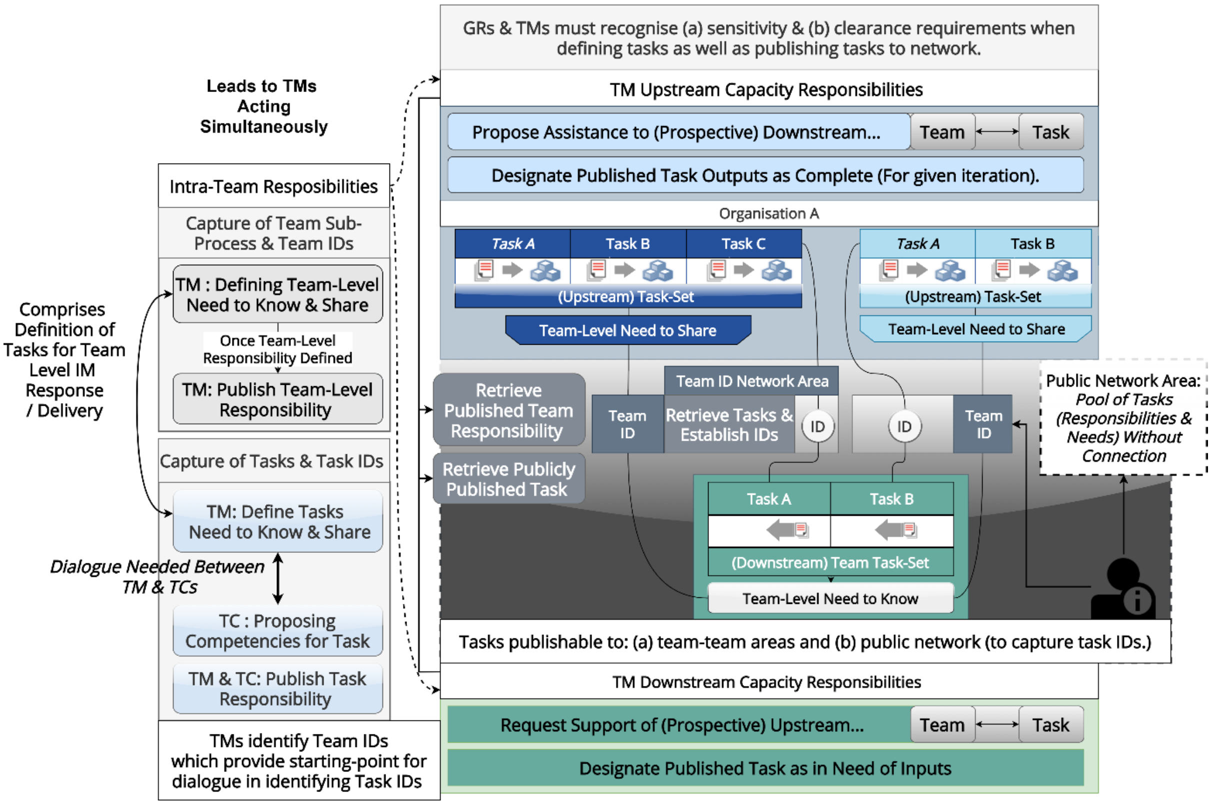

GRs & TMs must recognise (a) sensitivity & (b) clearance requirements when defining tasks as well as publishing tasks to network.
Leads to TMs Acting Simultaneously
TM Upstream Capacity Responsibilities
Propose Assistance to (Prospective) Downstream...
Team
Task
Designate Published Task Outputs as Complete (For given iteration).
Organisation A
Intra-Team Resposibilities
Capture of Team Sub-Process & Team IDs
TM : Defining Team-Level Need to Know & Share
Once Team-Level Responsibility Defined
TM: Publish Team-Level Responsibility
Comprises Definition of Tasks for Team Level IM Response / Delivery
Task A
Task B
Task C
(Upstream) Task-Set
Team-Level Need to Share
Task A
Task B
(Upstream) Task-Set
Team-Level Need to Share
Team ID Network Area
Retrieve Published Team Responsibility
Team ID
Retrieve Tasks & Establish IDs
ID
ID
Team ID
Public Network Area: Pool of Tasks (Responsibilities & Needs) Without Connection
Capture of Tasks & Task IDs
Retrieve Publicly Published Task
TM: Define Tasks Need to Know & Share
Task A
Task B
(Downstream) Team Task-Set
Team-Level Need to Know
Dialogue Needed Between TM & TCs
TC : Proposing Competencies for Task
TM & TC: Publish Task Responsibility
Tasks publishable to: (a) team-team areas and (b) public network (to capture task IDs.)
TM Downstream Capacity Responsibilities
Request Support of (Prospective) Upstream...
Team
Task
TMs identify Team IDs which provide starting-point for dialogue in identifying Task IDs
Designate Published Task as in Need of Inputs

Figure 5.9: Task Interconnectivity Capture

Firstly, in expanding upon **Figure 5.9**, it should be noted there is a cross-over between capturing team and task-level IDs. The aforementioned '*Team-level ID Capture Stage*' and following stages also assume background appointment information has been provided to enable the initial allocation of sub-processes and tasks by internal TMs in a security-minded manner.

Task-Level ID Capture: Established team-level IDs provide a starting point for TCs to capture IDs between other teams' tasks. Tasks can also however be publicly published to the network. The only detail to be communicated of task responsibilities would be so that other parties can discover relevant mutual overlaps in work. The following points characterise the detail depicted in **Figure 5.9.**

- A TM / TC (downstream capacity) would publish their tasks in need of inputs. They also retrieve other published tasks to determine (a) their relevance in providing inputs and (b) what outputs of their own (when generated) would be of relevance to provide back upstream.

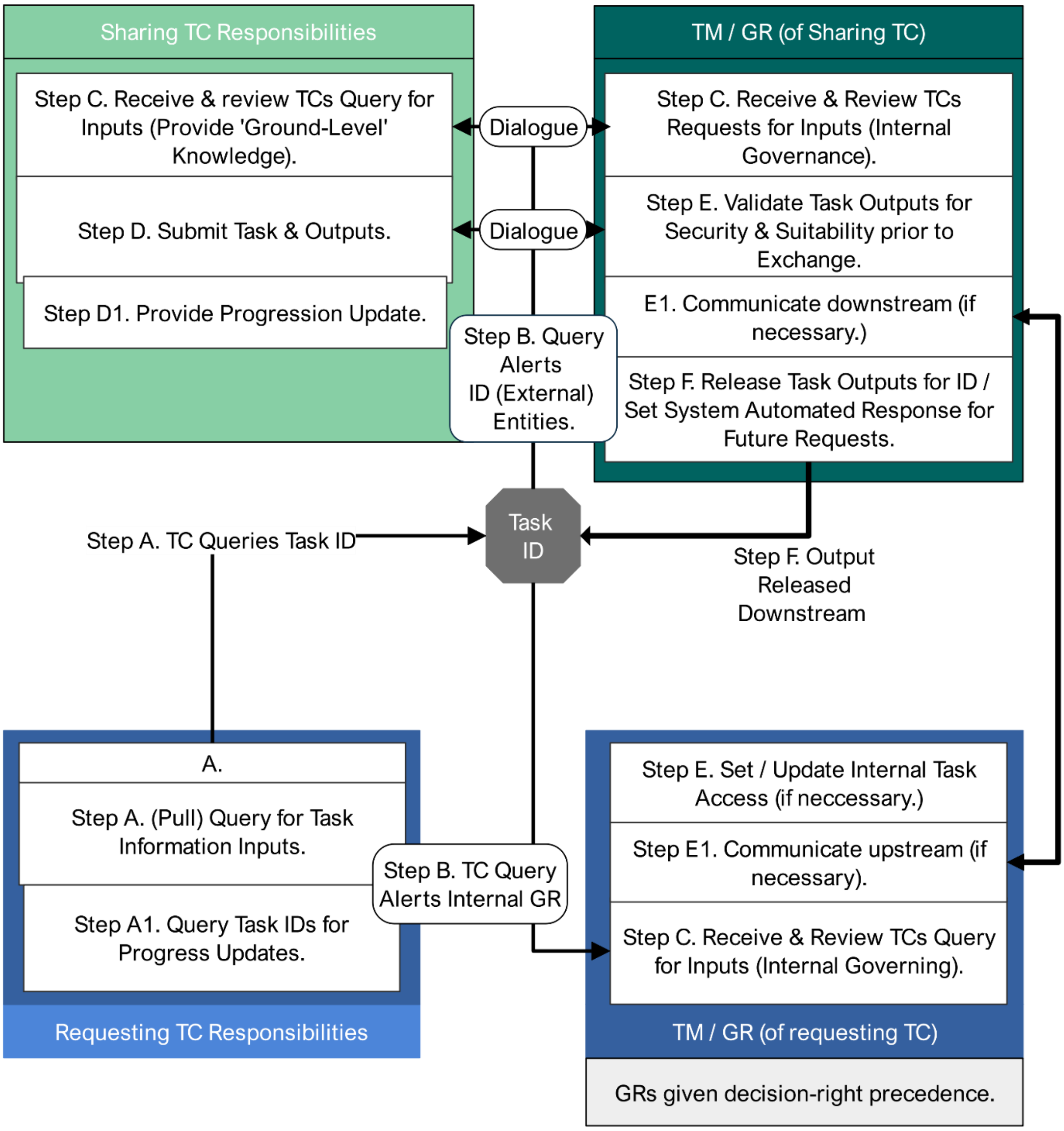
- A TM / TC acting in an upstream capacity publishes *tasks as ready to output* (if complete). They also retrieve *other published tasks* to identify what tasks of DTs (a) require outputs from their tasks and (b) is / will be of relevance to themselves in providing inputs.

Tasks published to network: Such scenario, without prior capture team-level IDs, can also feely occur by TCs via oversight from TMs to identify which other tasks can provide or require support. E.g. if a downstream task's needs cannot be fully met by an established team (and its tasks), support would be required from another team and their TCs tasks. If the responsible TM responds to this published task, this will form an ID at the team and task level.

Summary: It should be noted there would be a level of cross-over between capture of team and task IDs. The capture of team IDs is the starting point for collaborators to decompose the issue of 'who needs to know what' in capturing task IDs. However, identified team IDs may be unable to provide information for all downstream tasks. As such, publishing tasks to the network broadens the net of response and discoverability. Finally, it should be noted this depicted sequence between potential team collaborators does not account for the leverage of task templates. These factors discussed within **Section 5.3.5** are important to facilitate pre-defined capture of IDs as opposed to entirely manual formation of tasks and IDs.

5.3.3.2 Ongoing Planning, Enablement and Governance of Information-Flows

This section expands **Section 5.3.3.1,** whereby after an ID has been identified, a downstream task must query upstream inputs to commence their responsibilities. It is noted after the initial query process that release to queries could be semi-automated. **Figure 5.10** provides a depiction of the generic sequence that follows in a downstream task querying upstream inputs.



Sharing TC Responsibilities
Step C. Receive & review TCs Query for Inputs (Provide 'Ground-Level' Knowledge).
Step D. Submit Task & Outputs.
Step D1. Provide Progression Update.
TM / GR (of Sharing TC)
Step C. Receive & Review TCs Requests for Inputs (Internal Governance).
Step E. Validate Task Outputs for Security & Suitability prior to Exchange.
E1. Communicate downstream (if necessary.)
Step F. Release Task Outputs for ID / Set System Automated Response for Future Requests.
Dialogue
Dialogue
Step B. Query Alerts ID (External) Entities.
Task ID
Step A. TC Queries Task ID
Step F. Output Released Downstream
A.
Step A. (Pull) Query for Task Information Inputs.
Step A1. Query Task IDs for Progress Updates.
Requesting TC Responsibilities
Step B. TC Query Alerts Internal GR
Step E. Set / Update Internal Task Access (if neccessary.)
Step E1. Communicate upstream (if necessary).
Step C. Receive & Review TCs Query for Inputs (Internal Governing).
TM / GR (of requesting TC)
GRs given decision-right precedence.

Figure 5.10: General Transaction Interaction

Within **Figure 5.10**, responsibilities are grouped against the capacity in which an actor acts e.g. a TM / GR acts in governing capacity over internal TCs. It also noted the sequence of interactions between actor's responsibilities which are numbered within **Figure 5.10**, as 'Steps A through F'. These steps have been combined for following stages and scenarios.

TC Requests Information: A TC requests information for their task. Alternatively, they may query for an update to the status of an upstream task. Both actions **(Step A1** and **A2)** occur via TCs querying the ID that links their task to corresponding provider/s of information.

Dialogue between upstream GR / TM and internal TC: After a request is made, both the external TC and TM / GR are informed of the request **(Step B)**. They are both able to reference the need of the requesting actors and should communicate to determine response **(Step C)**. Communication also occurs in ensuring an output has been submitted **(Step D)** and in validating outputs are suitable and secure (in view of requesting TCs needs).

Dialogue between upstream and downstream TMs: After a request is made, the internal TM / GR is notified. Their dialogue between upstream GRs / TMs is noted in **Step E1**. This may be necessary for additional governance of security-risk prior to release.

Outcome Scenario - Release of Information: The depicted scenario in **Figure 5.10** is where the upstream GR / TM allows release of information after validating the task's suitability and security. This requires the following conditions to be met.

- A task-output has been submitted by the upstream TC and the cumulative task-output is able to meet the information-needs of the downstream task.
- The total information-output is filtered by the upstream TM / GR to not exceed downstream needs and not present risk / privacy concerns. Filtering of a task's cumulative output-container to create a distinct output subset is noted from **Sections 5.3.4** through **5.3.4.4**.

- Before an output has been released, the TM (upstream and downstream) may communicate to refine the TCs task-level access and by extension their work responsibility.

Finally, the aforementioned stages are from the perspective of a downstream TC requesting inputs from their upstream counterparts. The generic query sequence is equally applicable for upstream TCs querying information (once generated) from their downstream counterparts. I.e., during subsequent task and information-flow iterations. Finally, the latter scenario of being unable to meet a query for inputs also occurs within progressive information-flow iterations.

Outcome Scenario - Unable to release information: Alternatively, the requested information cannot be released due to: (a) the TC not submitting an output or (b) the submitted outputs not meeting the project requirements to release information. The responsible TC may also (c) be unable to respond until receiving information from their own providers who may also require information, and so on in the form of a cascading chain of requests that must be resolved. This is briefly noted within **Section 5.3.6.3** as a feature networks may in turn help resolve.

Summary: Some further factors are noted of aforementioned stages and scenarios. Firstly, TMs are a localised governance capacity over their own teams and transactions. However, GR holds precedence in governing information-flows. More detailed governance factors are expanded upon in **Section 5.3.3.4**. It should also be noted that ongoing information-planning was noted implicitly in this section as it follows a similar general route.

5.3.3.3 Enabling Team Level Information-Flows

A motivation for team-level information-flows is that TMs should possess ability to request and share to other teams for scheduled IM activities such as delivery and coordination of outputs. It is perceived latency of project coordination points would be lessened via implementation of the framework's methods, and potentially increased efficiency between stakeholders. In consideration of these factors, this section details the general information-sharing patterns between teams in view of comprising task IDs. This section portrays the same constructs detailed **in Section 5.3.2** underpin team-to-team level information-flows with small deviations. The following **Figure 5.11** depicts aggregated modes of collaboration, still in view of further levels of atomicity, and intra / inter-organisational visibility as motivators.

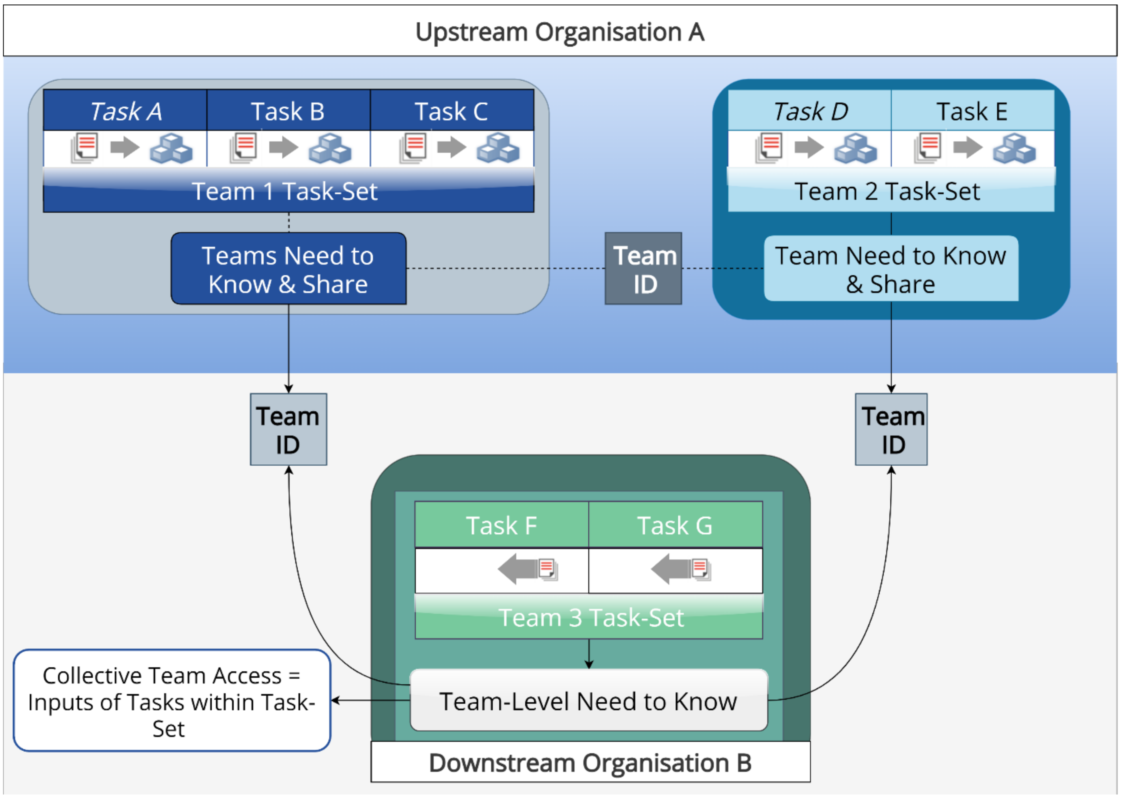


Figure 5.11: Team-to-Team Pattern (1)

In expanding upon the aforementioned **Figure 5.11** the same constructs detailed in **Section 5.3.2** underpin team-to-team level collaboration with the following patterns.

1. Distinct yet overlapping disciplinary responsibilities are assigned at the organisational level. These are decomposed to team-level task-sets which are comprised of individual TCs tasks.
    a. Each task-sets component (need to know etc) is a cumulative representation of its comprising tasks informational-needs.
2. Collaborating teams are interconnected via team IDs. This represents a team *need to know* is met (in-part) by another team's *need to share*.
    a. Depicted in **Figure 5.11** is that all teams share a team ID at the high-level.
3. This figure also depicts team-level queries provides the total access of a team.
    a. This is based upon all established task IDs in a task-set.
    b. If a TC were to further establish an ID as noted in **Section 5.3.3.1,** the access governed by TMs at a team-level would be extended accordingly.

To clarify, the in-part constraint of **Point 2** is because individual tasks (within a task-set) *do not* overlap with *all* tasks of another team. In other words, task IDs between teams are *only* established where relevant to ensure sharing specificity. **Figure 5.12** depicts Tasks IDs in view of this 'in-part' constraint between teams.

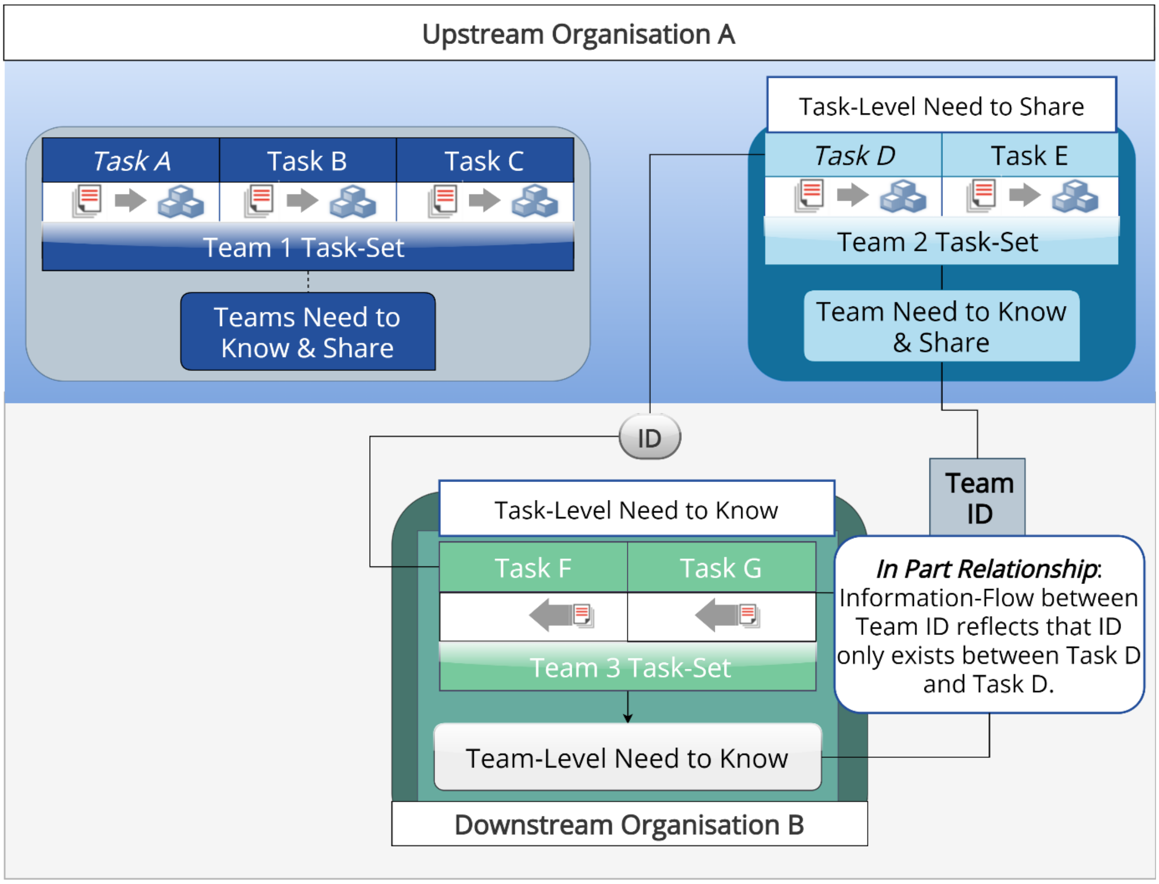


Figure 5.12: Team-to-Team Pattern (2)

In **Figure 5.12**, Team 2 only feeds into Team 1. In other words, the Team ID and the flow of information between Team 1 and 2 is based only on one task ID between the teams. This is between Task G and Task D and is representative of the specificity amongst teams, in view of professionals.

Based on motives of specificity, the cumulative output of given tasks may also be split between multiple ID tasks. I.e. to be able to represent scenarios where the receiving TC only requires a subset from a given task's output, as input for their task's responsibility. Filtering and subsets are further expanded upon in **Section 5.3.4**. **Figure 5.13** however depicts the same end motive in enabling specific sharing, but from the aggregated perspective of teams.

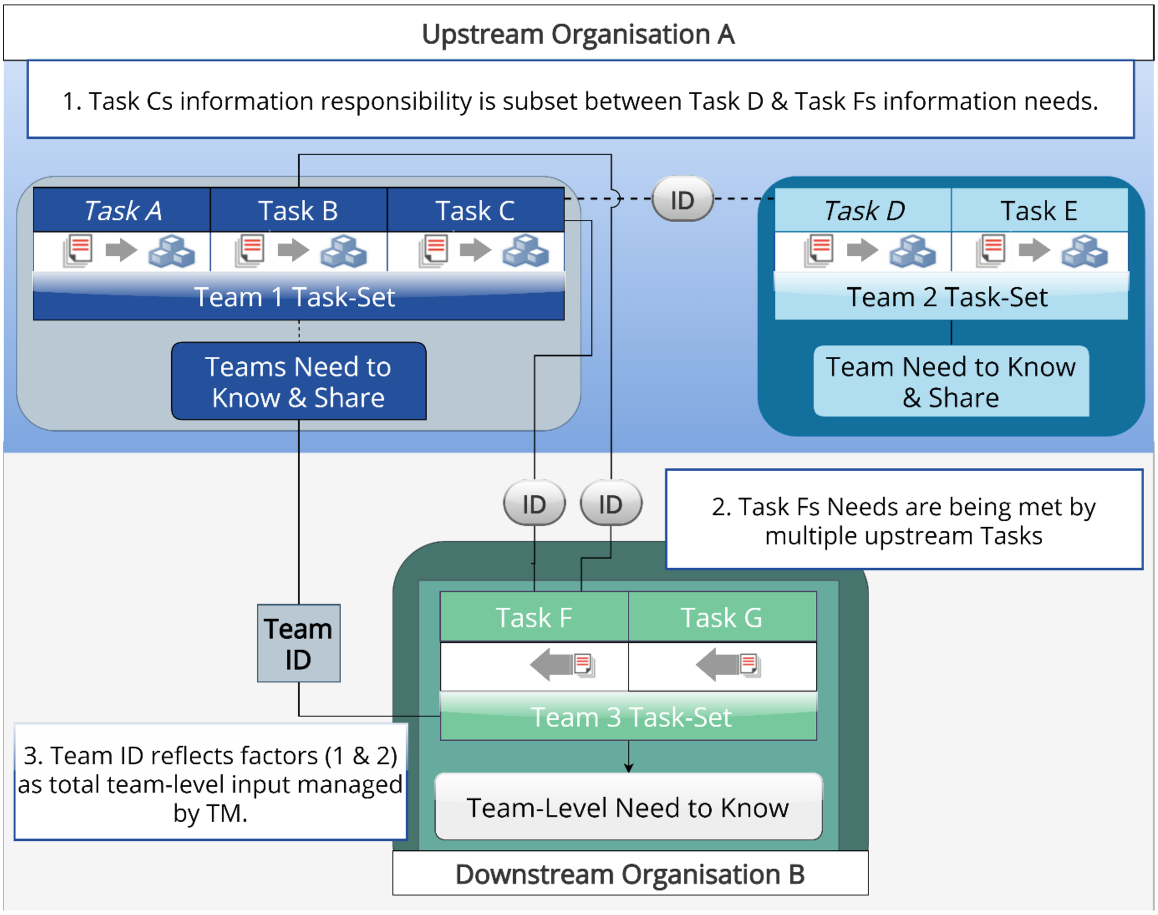

Upstream Organisation A
1. Task Cs information responsibility is subset between Task D & Task Fs information needs.
Task A
Task B
Task C
Team 1 Task-Set
Teams Need to Know & Share
ID
Task D
Task E
Team 2 Task-Set
Team Need to Know & Share
ID
ID
2. Task Fs Needs are being met by multiple upstream Tasks
Team ID
Task F
Task G
Team 3 Task-Set
3. Team ID reflects factors (1 & 2) as total team-level input managed by TM.
Team-Level Need to Know
Downstream Organisation B

Figure 5.13: Team-to-Team Pattern (3)

Depicted in **Figure 5.13** are the following scenarios which characterise patterns over what IDs should mean in terms of flow of information and thereby access. This is characterised in the following descriptors.

Cumulative Output Split:

- Task C of Team 1 is interdependent with Task D of Team 2.
- Task C of Team 1 is also interdependent with Task F of Team 3.
- As such, Task C (may) provide a specific subset of its cumulative output to Task D and another specific subset to Task F.

Cumulative Input Split:

- Task Fs information-needs are met by multiple upstream tasks (Task B and Task C).
- As such, the information-flow between Team 2 and Team 3 respects this constraint.

- Also, if either Task B or C filters a subset of their cumulative output to Task F:
    - Task Fs cumulative input reflects only what has been filtered and released to them. This is reflected also at the team-level.

Summary: The constructs explored within this section are an additional perspective from the aggregated team-level. Moreover, the focus is to characterise information-sharing specificity patterns based upon the IDs that have been generated via information-planning procedures. Similar such perspectives are detailed within **Section 5.3.4.4** as exploration of filtering of exchanges. The following section will expand upon the concepts explored here from a broader governance perspective.

5.3.3.4 Governing Team and Task Level Information-Flows

This section will explore governing information-flows, either at the team / task-level. It thus expands upon **Section 5.3.3.2**. The core motivator is that GRs possess the ability to ensure governance over information-flows (of those they are governing within a network). The following **Figure 5.14** depicts different types of actors possess different elements of responsibility when acting in an initiating capacity when querying information from other bodies.

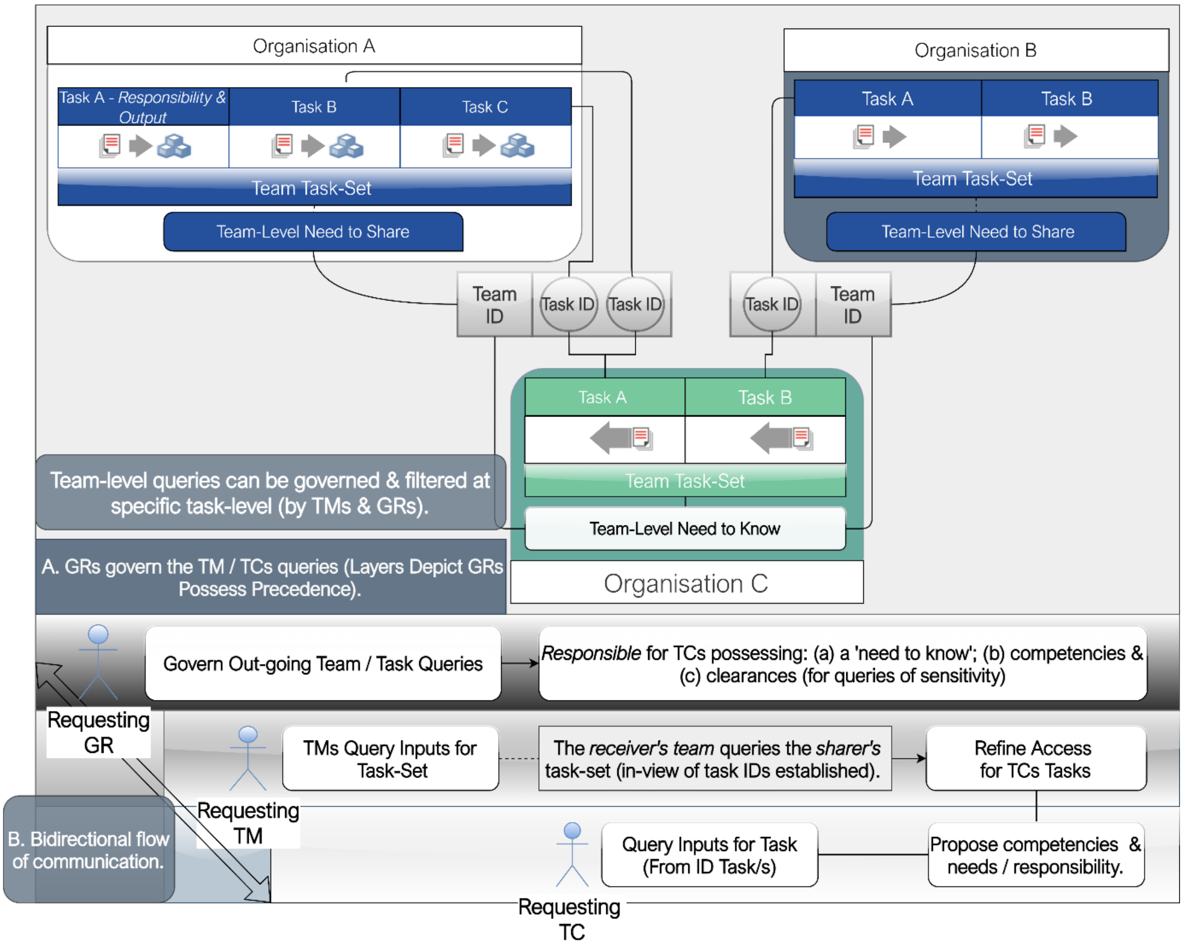

Organisation A
Task A - Responsibility & Output
Task B
Task C
Team Task-Set
Team-Level Need to Share
Organisation B
Task A
Task B
Team Task-Set
Team-Level Need to Share
Team ID
Task ID
Task ID
Task ID
Team ID
Task A
Task B
Team Task-Set
Team-Level Need to Know
Organisation C
Team-level queries can be governed & filtered at specific task-level (by TMs & GRs).
A. GRs govern the TM / TCs queries (Layers Depict GRs Possess Precedence).
Requesting GR
Govern Out-going Team / Task Queries
Responsible for TCs possessing: (a) a 'need to know'; (b) competencies & (c) clearances (for queries of sensitivity)
Requesting TM
TMs Query Inputs for Task-Set
The receiver's team queries the sharer's task-set (in-view of task IDs established).
Refine Access for TCs Tasks
B. Bidirectional flow of communication.
Requesting TC
Query Inputs for Task (From ID Task/s)
Propose competencies & needs / responsibility.

Figure 5.14: Governance Pattern (Requester)

The aforementioned **Figure 5.14** is expanded upon in the following descriptor.

Requester Perspective: **Figure 5.14** depicts generic responsibilities accordant to actor-types. It also depicts these actors possess different degrees of influence over enabling and governing of information-flows. GRs at the upper-most level can achieve all factors. However, the flow of dialogue for TCs can reach both TMs and GRs in ensuring the professional actors are not only able to communicate with other professionals (internal / external), but also possess a degree of influence over decision-making internally in view of localised knowledge.

- Firstly, it is noted TCs can query for inputs and coordinate with their TMs in view of progressing their task, of responsibilities / outputs, and accordingly, their needs. TCs can also coordinate directly (internal / external) whilst being governed.
- Secondly, GRs and TMs can query team IDs to pull inputs in view of all tasks. This may be for motives of managed information coordination / delivery between stakeholders at points in the project-schedule.
- GRs and TMs can also initiate their queries in view of particular tasks they manage. Accordingly, both TMs and GRS can refine internal access to internal TCs as necessary.
    - Via principles posed however, work-units and needs are linked, as are access-rights. Refining access is thereby reflective of minor modifications in a TCs work-responsibility via coordination between TCs themselves, and their TMs.
- GRs are responsible for governing the broader picture of all transactions (incoming / outgoing) and governing clearances.

The following **Figure 5.15** however provides the perspective of the organisations, and their actors that must provide a response, where the requester and sharer's GR, TM and TC is notified of queries (team / task level).

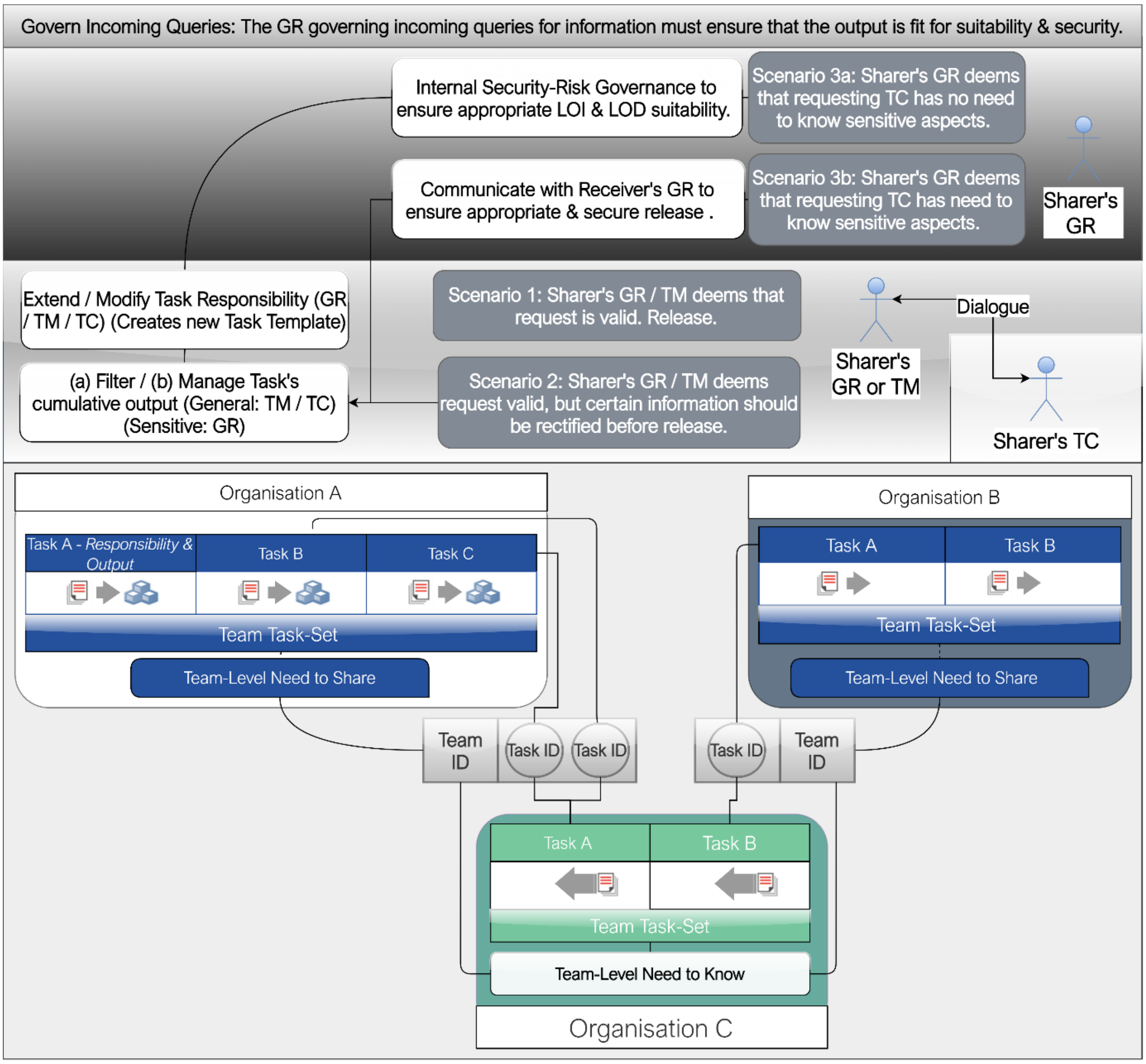

Govern Incoming Queries: The GR governing incoming queries for information must ensure that the output is fit for suitability & security.
Internal Security-Risk Governance to ensure appropriate LOI & LOD suitability.
Scenario 3a: Sharer's GR deems that requesting TC has no need to know sensitive aspects.
Communicate with Receiver's GR to ensure appropriate & secure release .
Scenario 3b: Sharer's GR deems that requesting TC has need to know sensitive aspects.
Sharer's GR
Extend / Modify Task Responsibility (GR / TM / TC) (Creates new Task Template)
(a) Filter / (b) Manage Task's cumulative output (General: TM / TC) (Sensitive: GR)
Scenario 1: Sharer's GR / TM deems that request is valid. Release.
Scenario 2: Sharer's GR / TM deems request valid, but certain information should be rectified before release.
Sharer's GR or TM
Dialogue
Sharer's TC
Organisation A
Task A - Responsibility & Output
Task B
Task C
Team Task-Set
Team-Level Need to Share
Organisation B
Task A
Task B
Team Task-Set
Team-Level Need to Share
Team ID
Task ID
Task ID
Task ID
Team ID
Task A
Task B
Team Task-Set
Team-Level Need to Know
Organisation C

Figure 5.15: Governance Pattern (Responder / Sharer)

Responder and Sharer Perspective: As depicted in **Figure 5.15**, a number of overarching scenarios can occur in response to queries at task / team level. **Scenarios 1** and 2 are where a request is received, and decisions is made to either release (**Scenario 1**) or a release caveated by further management or filtering outputs (**Scenario 2**). These scenarios can be enacted either by the upstream TM / GR. In either case, actors should also be able to semi-automate future iterations of the task to ensure fluid agility of response.

GRs may also delegate responsibilities to TMs to act as a localised governance capacity. A TM to ensure their outputs are effectively managed (team / task). Accordingly, **Scenarios 1** and **2** relate to general patterns in governing responses from a suitability perspective, which relates to creation of new templates. Templates are detailed within **Sections 5.3.5** but briefly noted here from a suitability and IM perspective. This is where TM directs their TCs to modify their work-outputs, thereby creating a new iteration of their task. This is whereby a particular iteration of a TCs cumulative task-responsibility, and its outputs may be tailored to specific collaborators.

Scenario 3a and **3b** however pertain to a request via a TC implicating sensitivity. The requester is unaware of this factor, and the responding GR must make decisions based upon general security-risk governance procedures, wherein organisations and their GRs must have understood the types of asset-information that may present vulnerabilities.

The internal TCs of requesting organisation depicted in the previous **Figure 5.14** are unaware of actual the project-context and potential sensitivities of information. The pattern here is to coordinate with the downstream GR in *ensuring* information is released *only* to those TCs with correct clearance (**Scenario 3a**). On the other hand, the GR deems the downstream request requires certain information in order to continue, but not the sensitive aspect. In which case filtering would occur. Finally, the downstream GR is also required to ensure clearance.

Section 5.3.3 Summary: This section has explored a high-level perspective of actors' interactions in capturing, enabling and governing information-flows. These interaction concepts are in response to functional requirements of the framework (of what should occur) and provides some detail of general patterns to be considered in future implementation of the frameworks methods as a whole.

Further detailed exploration of methods of governing exchange can be detailed after further exploration of concepts such as sub-task decomposability, spatial-mapping and task-templates. The following sections expand upon technicalities of such concepts. This starts by expanding the nature of transactions detailed throughout this section, which implicitly assumed sub-tasks could be captured as noted initially in **Section 5.3.2**. This would be to plan and thereby enable exchange of bespoke subsets of information between professionals.

5.3.4 Exploration of Decomposability Concepts

This section expands upon the summary of **Section 5.3.3** whereby it was posed that task-decomposability must be explored to detail how fully atomic sharing could be achieved. The series of concepts to be explored therefore comprise the frameworks proposals for decomposed task exchanges at the level of BIM data subsets. This will introduce concepts procedurally.

5.3.4.1 BIM Spatial Decomposition

The format and structure of BIM data shared amongst collaborators is IFC in many cases within industry (ISO - International Organization for Standardization, 2018b). Whilst the purpose of IFC and associated initiatives pertain to evolving challenges of interoperability (Berlo, 2019), the concepts that comprise the IFC schema are of pertinence as it provides context to spatially oriented and object-level BIM data explored as part of this framework. These concepts are displayed within **Figure 5.16**.

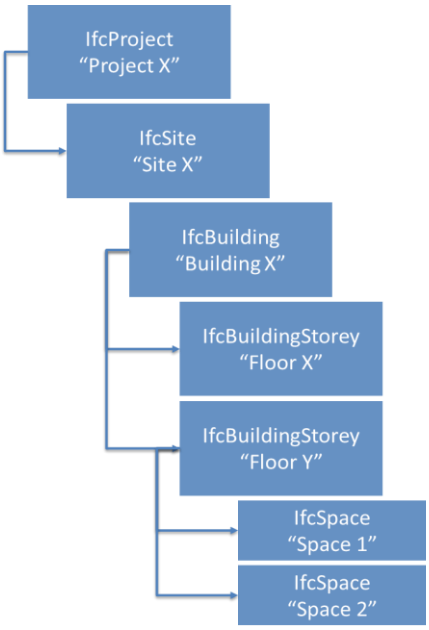
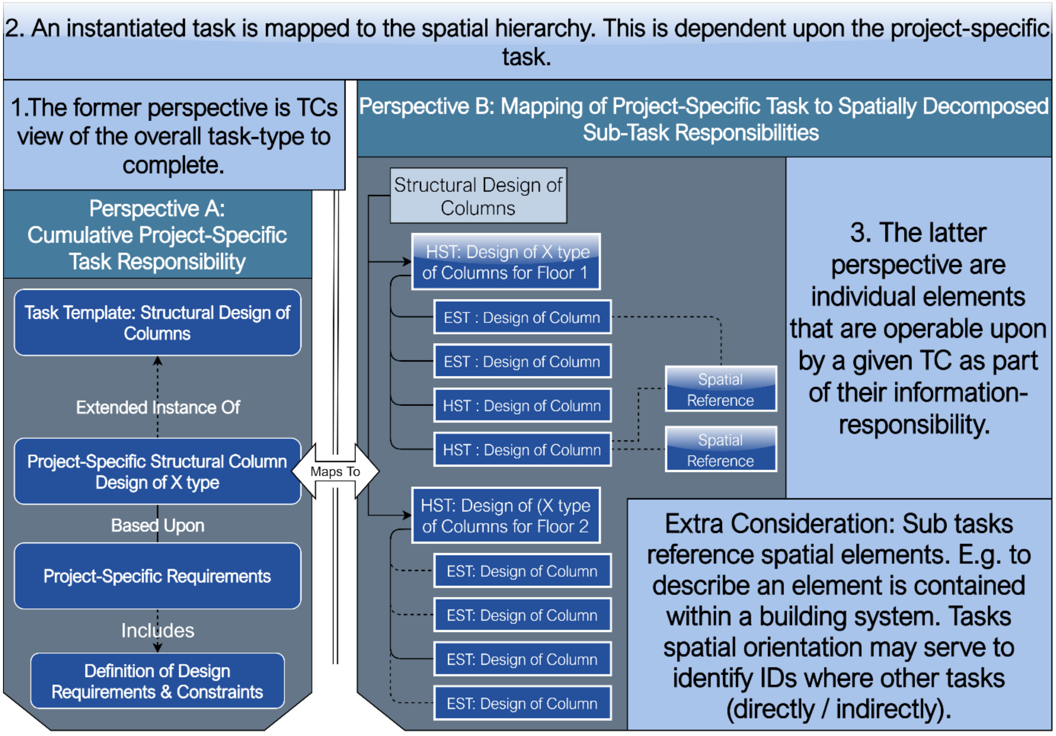


Figure 5.16: IFC Spatial Breakdown Structure

Spatially oriented concepts enable a standardised approach in structuring built-asset data. In the depicted hierarchy, the spatial-structural elements are progressively decomposed and other building elements are contained within this spatial hierarchy (e.g. a space is contained within a floor.) The following section expands on these concepts in the context of the framework.

5.3.4.2 Spatial Decomposition of Tasks

It should be noted the IFC schema enables an approach to structure BIM data. This is as opposed to structured atomic work-processes that are inter-linked with project-specific BIM data. I.e. an approach to allow real-life TCs to extend pre-defined processes, based upon their requirements for generating project-specific information to share with other TCs. The framework repurposes IFC concepts in providing TCs a means to achieve this which entails structuring and decomposing their task in whichever way is relevant depending upon their project-specific responsibility. An abstract overview of this concept is displayed within **Figure 5.17** which delineates two overlapping perspectives of task-based processes.



2. An instantiated task is mapped to the spatial hierarchy. This is dependent upon the project-specific task.
1.The former perspective is TCs view of the overall task-type to complete.
Perspective A: Cumulative Project-Specific Task Responsibility
Task Template: Structural Design of Columns
Extended Instance Of
Project-Specific Structural Column Design of X type
Based Upon
Project-Specific Requirements
Includes
Definition of Design Requirements & Constraints
Maps To
Perspective B: Mapping of Project-Specific Task to Spatially Decomposed Sub-Task Responsibilities
Structural Design of Columns
HST: Design of X type of Columns for Floor 1
EST : Design of Column
EST : Design of Column
HST : Design of Column
HST : Design of Column
Spatial Reference
Spatial Reference
HST: Design of (X type of Columns for Floor 2
EST: Design of Column
EST: Design of Column
EST: Design of Column
EST: Design of Column
3. The latter perspective are individual elements that are operable upon by a given TC as part of their information-responsibility.
Extra Consideration: Sub tasks reference spatial elements. E.g. to describe an element is contained within a building system. Tasks spatial orientation may serve to identify IDs where other tasks (directly / indirectly).

Figure 5.17: Overlapping Cumulative and Decomposed Perspectives

A core aspect depicted in **Figure 5.17** is the cumulative task responsibility **(Perspective A)**. This depicts that TCs possess an overarching task responsibility to complete. I.e. a *type* of disciplinary task which is assigned in line with a professionals given competencies. The notion of a task-type overlaps the task-template to be discussed within **Section 5.3.5**. It is discussed here briefly due to their relevance to the mapping of the cumulative responsibility to sub-tasks **(Perspective B)**.

This as depicted in **Figure 5.17** is where any task *extended* from a template is representative of the TCs project-specific requirements, which are comprised of further atomic sub-task operations to be undertaken with respect to specific BIM data objects. Sub-tasks themselves are decomposed and mapped against the project's spatial map which includes the spatial hierarchy noted in **Section 5.3.4.1** and other project-specific spatial groups based on concepts such as IFCsystem which are also pertinent for structuring TCs cumulative information-responsibilities against specific elements of work.

In other words, the cumulative responsibility is mapped against whichever individual / groupings of BIM elements (comprised within the spatial map) are part of a TCs task responsibility. This mapping itself is also thereby based upon requirements and constraints associated with a task's information-responsibility; this should be planned and coordinated between TMs and TCs. It is also driven by project-level requirements / constraints.

The methodology based around sub-tasks, and sub-tasks themselves prescribes consideration in planning atomic responsibilities and filtering outputs in response to queries, with specificity over individual elements and attributes. For this to occur however, sub-tasks must also be linked to their own output components.

Accordingly, the following factors expand upon the 'Sub-Task Perspective B'. Sub-tasks would be generated for all object-elements pertaining to the task's project-specific requirements. Two overarching types are depicted.

- **Hierarchal Tasks**: These are common spatial containers for the project, which reference a given level of the asset's hierarchy, to act as a container for all nested elements residing within a given level. They are 'parents' to all nested child sub-tasks to be noted in **Section 5.3.4.4**. Hierarchal spatial containers can also contain other spatial sub-tasks.
- **Element sub-tasks**: These are generated and structured in line with the spatial-container with which their referenced elements reside. For example, the hierarchal sub-task '*Design of X Type of Columns for Floor 1*' nests several element sub-tasks which reference the individual design-elements. Element sub-tasks may also be contained within other spatial-grouping concepts such as IFCsystem.

Summary: This section has further expanded upon how the framework poses a TCs given cumulative task can be further decomposed. The following section expands upon the manner in which sub-tasks are proposed to possess sub-outputs; this in turn finalises the groundwork for filtering of a task's outputs in generating subsets. It should also be noted that the aforementioned considerations in essence would enable data-driven information-planning of IDMs but should be enacted by the professionals themselves with effective usability. The mapping may also occur automatically upon submission of BIM data against a type of task.

5.3.4.3 Sub-Tasks and Mapping to Sub-Outputs

This section expands upon the mapping of sub-task in view of sub-task level outputs. Firstly, it should be noted that from a data schema perspective, tasks should be able to recursively nest other tasks as sub-tasks. This by extension means nesting of their need to share and output components. This recursive nesting approach allows them to be procedurally attached as TCs iteratively identify them as part of their cumulative responsibility. The following **Figure 5.18** depicts this notion.

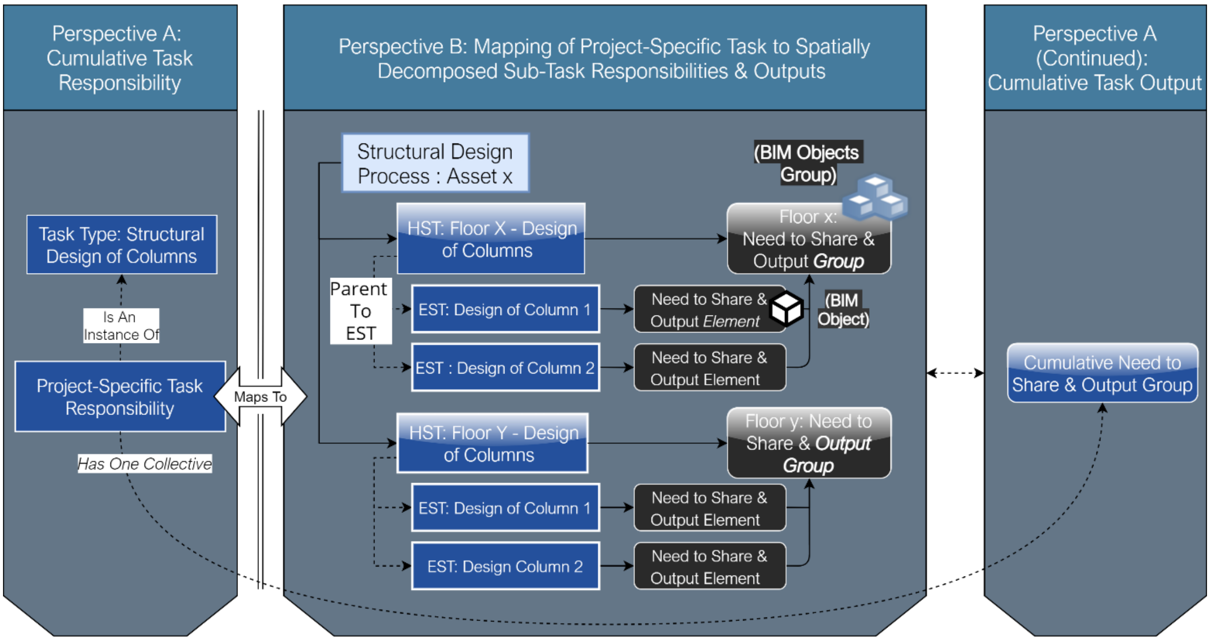

Perspective A: Cumulative Task Responsibility
Task Type: Structural Design of Columns
Is An Instance Of
Project-Specific Task Responsibility
Has One Collective
Maps To
Perspective B: Mapping of Project-Specific Task to Spatially Decomposed Sub-Task Responsibilities & Outputs
Structural Design Process : Asset x
(BIM Objects Group)
HST: Floor X - Design of Columns
Floor x: Need to Share & Output Group
Parent To EST
EST: Design of Column 1
Need to Share & Output Element
(BIM Object)
EST : Design of Column 2
Need to Share & Output Element
HST: Floor Y - Design of Columns
Floor y: Need to Share & Output Group
EST: Design of Column 1
Need to Share & Output Element
EST: Design Column 2
Need to Share & Output Element
Perspective A (Continued): Cumulative Task Output
Cumulative Need to Share & Output Group

Figure 5.18: Decomposed Responsibilities and Outputs

As a general example, **Figure 5.18** depicts the grouped outputs of hierarchal sub-tasks comprise individual output elements. For example, the hierarchal sub-task 'Design of Columns: Floor 1' acts as a container of the need to share and outputs of all nested element tasks and their 'Nested Information Responsibilities'. I.e. Sub-tasks possess decomposed 'need to share components'. These are linked to either further nested groupings of BIM data outputs, or individual-elements e.g. design of specific columns at the bottommost level of a given TCs cumulative responsibility.

The cumulative task-responsibility is in turn based upon all sub-tasks (defined as part of the TCs responsibility). A task's cumulative information-output group collates all outputs generated in respect to sub-tasks defined as part of the sub-task perspective. The output-groups subsets are in turn comprised of specific sub-task level outputs (based upon the information-needs of its ID tasks).

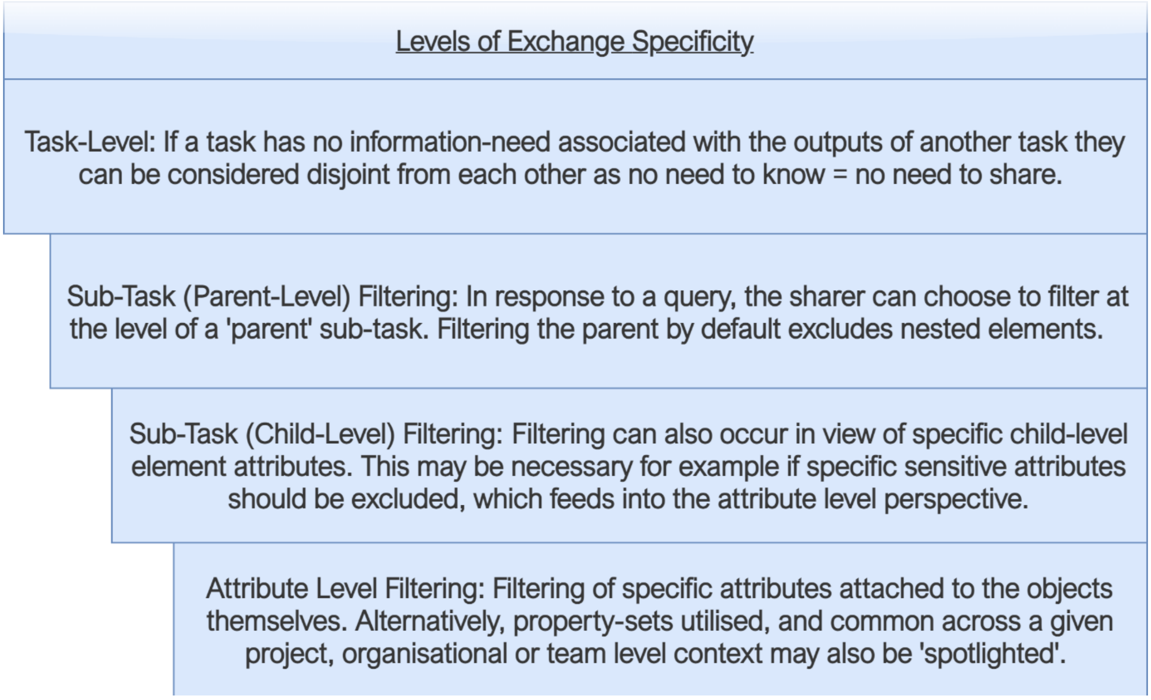
These perspectives are essentially mirrored representations of each other. The cumulative responsibility is based on the sub-task perspective. I.e. sub-tasks possess individual need to share and output components and can be (a) outputted from individually in response to specific sub-task level queries, but also (b) form the cumulative responsibility.

Interlinking with the information-planning benefits noted in **Section 5.3.4.2** of structured and explicit representation of a TCs responsibility, these two interlinked perspectives also represent the potential for actors to switch between the cumulative perspective to a further atomic level in responding to pull-requests.

Summary: Concepts noted in this section which follow from **Section 5.3.4.2** would also be underpinned by interfaces and functionality in: (a) filtering their output to form a precise sub-set (in response to a query) or (b) initiating a sub-task level query themselves. In the latter sense, a sub-task can also be linked to a nested 'need to know' component. The following sections expand upon the consideration of these concepts in exchanging subsets in line with sub-tasks.

5.3.4.4 Facilitating Exchange of Filtered Subsets

This section expands on enabling sharing actors to filter a task's cumulative outputs in response to a query from another task. Firstly, a task's cumulative output group is subset when exchanging information. Each subset is aligned to the information-needs of a receiving task.



Levels of Exchange Specificity

Task-Level: If a task has no information-need associated with the outputs of another task they can be considered disjoint from each other as no need to know = no need to share.

Sub-Task (Parent-Level) Filtering: In response to a query, the sharer can choose to filter at the level of a 'parent' sub-task. Filtering the parent by default excludes nested elements.

Sub-Task (Child-Level) Filtering: Filtering can also occur in view of specific child-level element attributes. This may be necessary for example if specific sensitive attributes should be excluded, which feeds into the attribute level perspective.

Attribute Level Filtering: Filtering of specific attributes attached to the objects themselves. Alternatively, property-sets utilised, and common across a given project, organisational or team level context may also be 'spotlighted'.

Figure 5.19: Levels of Exchange Specificity

Figure 5.19 depicts that a combination of increasingly specific levels can be employed in exchanging any given task's outputs. Filtering in creating a subset comprises the means of actors being able to specify at the cumulative task-level, the level of a parent sub-task, element and attribute level.

The following **Figure 5.20** correspondingly depicts an example where the sharing task's (mapped to sub-tasks) employs the aforementioned filtering levels to split the cumulative output into two subsets. This is in response to the receiver's cumulative task query.

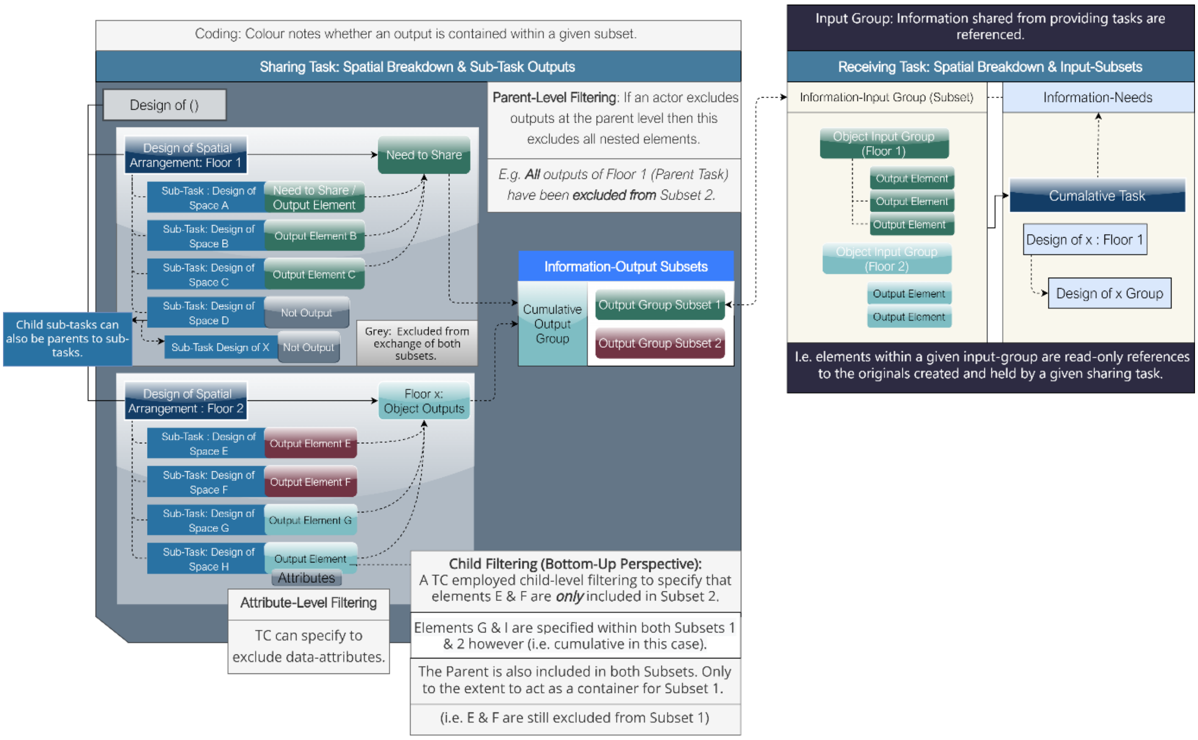

Coding: Colour notes whether an output is contained within a given subset.
Sharing Task: Spatial Breakdown & Sub-Task Outputs
Design of ()
Design of Spatial Arrangement: Floor 1
Need to Share
Sub-Task : Design of Space A
Need to Share / Output Element
Sub-Task: Design of Space B
Output Element B
Sub-Task: Design of Space C
Output Element C
Sub-Task: Design of Space D
Not Output
Sub-Task Design of X
Not Output
Child sub-tasks can also be parents to sub-tasks.
Grey: Excluded from exchange of both subsets.
Parent-Level Filtering: If an actor excludes outputs at the parent level then this excludes all nested elements.
E.g. All outputs of Floor 1 (Parent Task) have been excluded from Subset 2.
Information-Output Subsets
Cumulative Output Group
Output Group Subset 1
Output Group Subset 2
Design of Spatial Arrangement : Floor 2
Floor x: Object Outputs
Sub-Task : Design of Space E
Output Element E
Sub-Task: Design of Space F
Output Element F
Sub-Task: Design of Space G
Output Element G
Sub-Task: Design of Space H
Output Element
Attributes
Attribute-Level Filtering
TC can specify to exclude data-attributes.
Child Filtering (Bottom-Up Perspective):
A TC employed child-level filtering to specify that elements E & F are only included in Subset 2.
Elements G & I are specified within both Subsets 1 & 2 however (i.e. cumulative in this case).
The Parent is also included in both Subsets. Only to the extent to act as a container for Subset 1.
(i.e. E & F are still excluded from Subset 1)
Input Group: Information shared from providing tasks are referenced.
Receiving Task: Spatial Breakdown & Input-Subsets
Information-Input Group (Subset)
Information-Needs
Object Input Group (Floor 1)
Output Element
Output Element
Output Element
Object Input Group (Floor 2)
Output Element
Output Element
Cumalative Task
Design of x : Floor 1
Design of x Group
I.e. elements within a given input-group are read-only references to the originals created and held by a given sharing task.

Figure 5.20: Subset Based Filtering

Figure 5.20 also depicts the cumulative task's output group is subset, to be linked to the input groups of one of the receiving tasks. The following points provide detail of filtering employed.

- **At the level of parent tasks (top-down perspective):** Parent tasks recursively nest other tasks as sub-tasks. As such, if the sharing TC excludes a 'parent task', this thereby excludes all nested elements (as part of a given subset).

Of a general abstract example, hierarchal tasks in figure b are parent all to nested element-level sub-tasks and output-elements. The example depicted is that the hierarchal task of Floor 1 is excluded from subset 2. As such, all elements that fall under this parent are excluded.

- **At the level of child sub-tasks (bottom-up perspective):** Filtering of the tasks cumulative output can also occur from a bottom-up perspective of the individual, or groupings of nested element sub-task outputs to be included as part of a given subset.

In other words, if a child sub-task is included as part of a subset, then the parent sub-task is also included (but only to the extent as a container, unless otherwise specified). Child (sub) tasks will also be parents to other sub-tasks or possess attribute-elements attached to the task in which case the top-down perspective is employed. This is noted of the following.

- **At the level of element attributes**: Filtering at the child-level also takes place at the level of individual element attributes held / referenced at the level of a given object. This may be necessary for example if specific sensitive attributes should be excluded.
    - GRs should be able to 'spotlight' project-specific properties across dynamically defined property-sets (extending beyond IFC schema and derived with respect to different project resources and activities). This is for the purposes of drawing attention to types of attribute data that requires elevated governance.

Moreover, all perspectives should be simultaneously utilised to effectively filter outputs. Also depicted in **Figure 5.20** is that output subsets form the cumulative input-group of receiving tasks. The context depicted is that the receiving tasks request inputs based upon their task's cumulative need to know. However, the receiving task will also possess need to know components at the level of their sub-tasks, in which case further atomic links can be made at an element and attribute-level as these connections are identified by collaborating TCs.

Summary: This section has expanded upon the need to filter a specific subset of a given TCs responsibility in view of other professionals needs. Accordingly, a TC could only filter elements their cumulative responsibility comprises, in response. If, however the TCs responsibility must be expanded to respond to a need, then this should also be captured via ongoing coordination in **Section 5.3.3.1**. The next section will detail responses and governance of sub-task queries.

5.3.4.5 Enabling and Governing Pull Based Querying of Subsets

Enabling Pull-Based Querying of Subsets: Having explored concepts that should achieve on-the-fly structuring of the actor's information-responsibilities and thereby exchanges. This section explores: (a) sub-task level queries and (b) GRs in governing incoming / outgoing queries and associated transactions. **Figure 5.21** depicts a TC should be able to request and pull the information required at the level of their specific sub-tasks.

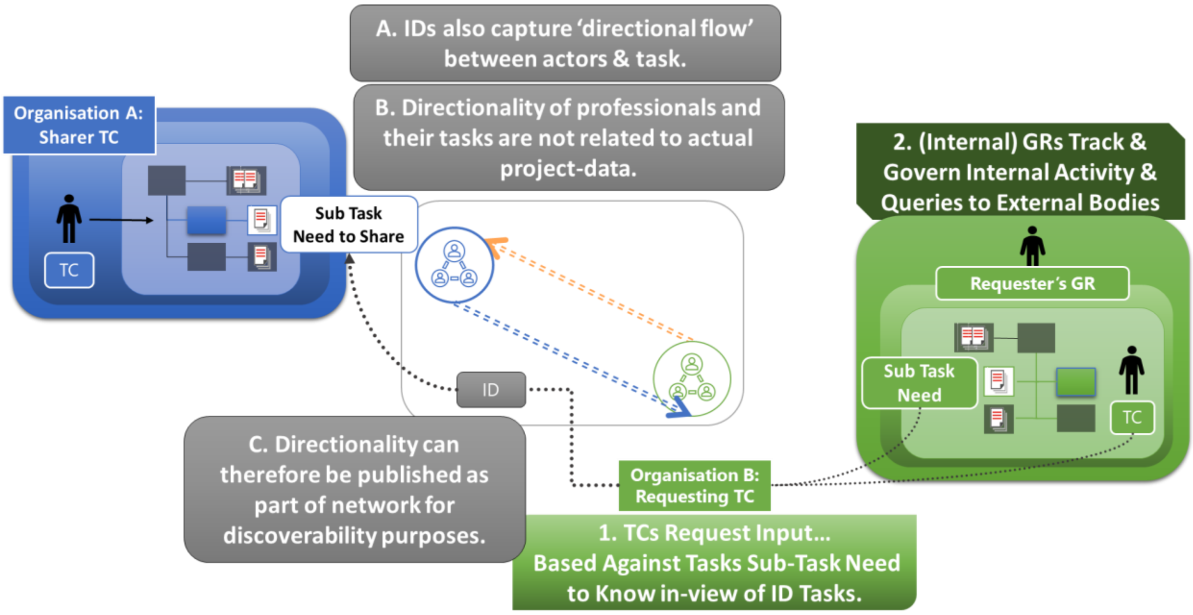

A. IDs also capture 'directional flow' between actors & task.
B. Directionality of professionals and their tasks are not related to actual project-data.
Organisation A: Sharer TC
TC
Sub Task Need to Share
ID
2. (Internal) GRs Track & Govern Internal Activity & Queries to External Bodies
Requester's GR
Sub Task Need
TC
C. Directionality can therefore be published as part of network for discoverability purposes.
Organisation B: Requesting TC
1. TCs Request Input... Based Against Tasks Sub-Task Need to Know in-view of ID Tasks.

Figure 5.21: Querying of Subsets

Figure 5.21 depicts the requesting TC has queried their information-needs at the level of one of their sub-tasks. This query is directed at a sub-level ID of a counter-part interdependent task. In other words, the query is directed at specific or groupings of element-level inter-connections. A TC would be able to query the need to know components of their sub-tasks once these sub-tasks have been procedurally defined and updated against their cumulative task responsibility.

Also depicted in **Figure 5.21**, a sub-task's need to know component can also be linked to specific sub-tasks need to share components. This is also once these element-level inter-connections have also been defined. As such, the 'needs' of individual or groups of sub-tasks can be linked to the outputs of one or many counterpart sub-tasks. The capture of specific element and attribute level

IDs are the finest level of detail in reconciling actors needs and responsibilities. These would be procedurally attached and updated via progressive task-iterations.

Correspondingly, an implicit factor is the localised sub-structure of a cumulative task is published to other cumulative task IDs when these are established (either manually / semi-automated via templates). This is respective of on-going visibility TCs should possess of requests / updates directed by their counterpart collaborating TCs at this atomic level.

This should enable on-going visibility between interdependent TCs as part of progressive iterations of their tasks and understanding of overlaps. It is also noted in **Figure 5.21** that factors of 'directionality' between tasks can be separated from actual data. Publication of directionality thereby enables increased discoverability within a broader perspective. It is assumed the cumulative task ID could be published where GRs could govern this facet.

Finally, these finite-level factors are also however representative of parametric inter-connections between project-information. Benefits of such are noted as future considerations in **Section 7.2** as standard capabilities of future BIM processes and technologies.

Governing Pull-Based Querying of Subsets: Figure 5.22 details governance responses to queries at a sub-task level. The depiction within **Figure 5.22** is similar to the perspective displayed within **Section 5.3.3.2** and **5.3.3.4** but further characterises the level of atomicity GRs should possess in governing and pre-validating exchanges.

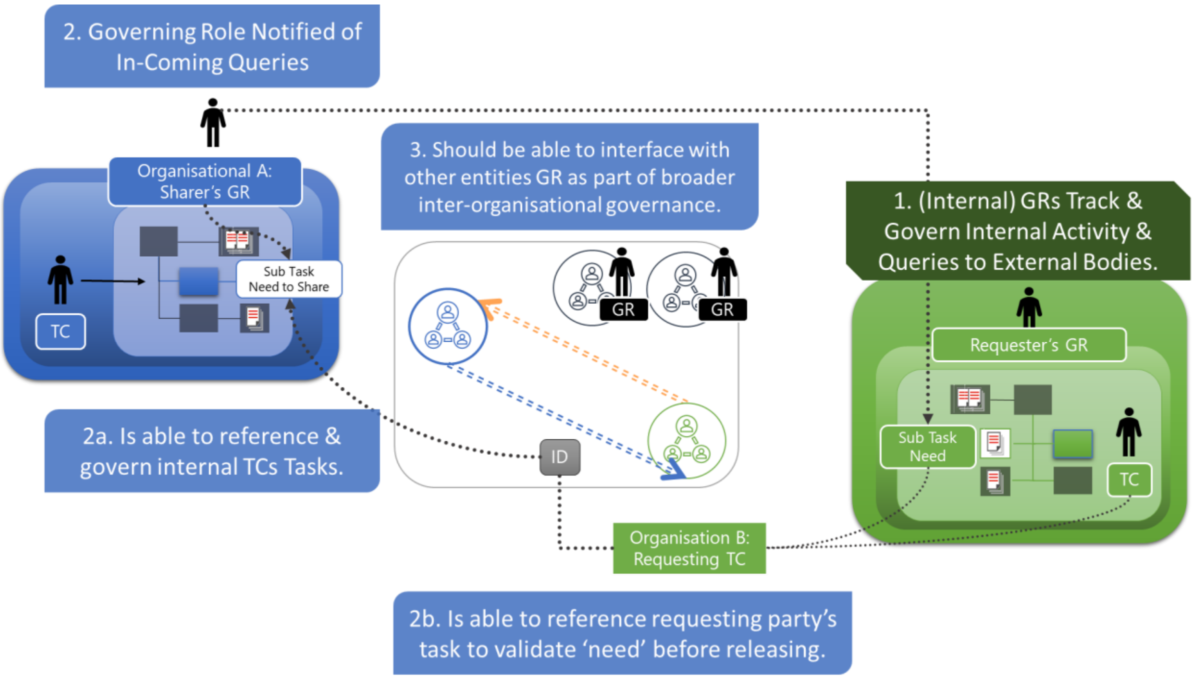

2. Governing Role Notified of In-Coming Queries
Organisational A: Sharer's GR
TC
Sub Task Need to Share
3. Should be able to interface with other entities GR as part of broader inter-organisational governance.
GR
GR
ID
1. (Internal) GRs Track & Govern Internal Activity & Queries to External Bodies.
Requester's GR
Sub Task Need
TC
2a. Is able to reference & govern internal TCs Tasks.
Organisation B: Requesting TC
2b. Is able to reference requesting party's task to validate 'need' before releasing.

Figure 5.22: Governing Sub-Task Querying

It is depicted in **Figure 5.22** that GRs should be able to reference the specific sub-task level queries of TCs. The further decomposition of work-units, and thereby information-flows provides GRs comprehensive visibility and context over what is being requested / shared, why and to which external TCs in this context. Validation of receiver's information-needs and governance of security-risk should also take place over task-based exchanges.

This should enhance security-risk governance prior to sharing utilising filtering mechanisms characterised in **Section 5.3.4.3** and **5.3.4.4** of governing sensitive exchanges. Finally, it is depicted both GRs are in sync, which is spanned out as part of broader inter-organisational governance approaches.

Summary: This section has expanded upon concepts in characterising the atomicity of governance that GRs should possess and also ability to enact specific information-sharing transactions between interdependent TCs with added benefits of agility and decrease in latency between transactions. The following section details templated approaches for semi-automated ID capture, querying and governance thereof.

5.3.5 Exploration of Task Template Concepts

This section expands upon task-templates from the perspective of generic transactions between tasks which can be *extended* with project-specific requirements. The core purpose of templates is to alleviate inefficiencies in manually capturing interdependencies between professionals and their tasks. These were noted during the proposition for manual discovery of actor's IDs in **Section 5.3.3.1**. Firstly, the underlying structure of templates is described within **Figure 5.23.**

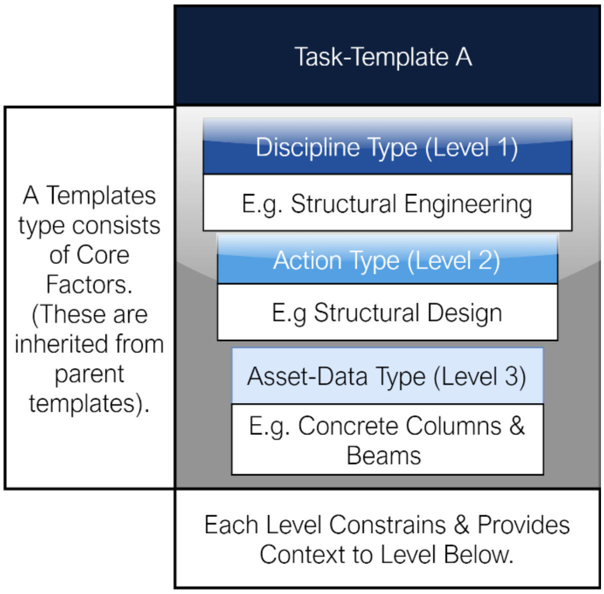

Task-Template A
A Templates type consists of Core Factors. (These are inherited from parent templates).
Discipline Type (Level 1)
E.g. Structural Engineering
Action Type (Level 2)
E.g Structural Design
Asset-Data Type (Level 3)
E.g. Concrete Columns & Beams
Each Level Constrains & Provides Context to Level Below.

Figure 5.23: Task Template Construct

In expanding upon **Figure 5.23**, further context is provided by the following points.

Discipline Type Context (Level 1): A task-type is based upon a given discipline. The specific discipline provides an upper-level context to differentiate the lower-level action-types and information-types. A discipline-type can itself be differentiated by sub-discipline types.

Action Operation Type Context (Level 2): A generic type of action. E.g. 'Analysis' is a common type of disciplinary action which is contextualised within a specific discipline e.g. structural static analysis. It is also provided further context by the type of method (software or otherwise) utilised to undertake the type of action.

Information type context (Level 3): An information-type is a type of BIM asset / element. The information-type is provided increasing context by the discipline-type and action-types.

The aforementioned components of a template detail that templates correspond to a 'type' of disciplinary task, where these key components are a starting structure for detailed expression of information responsibilities of actors. The components dictate increasing context and conditions over the types of design-information that are relevant to a given templates need to know and share. **Figure 5.24** depicts an abstract example.

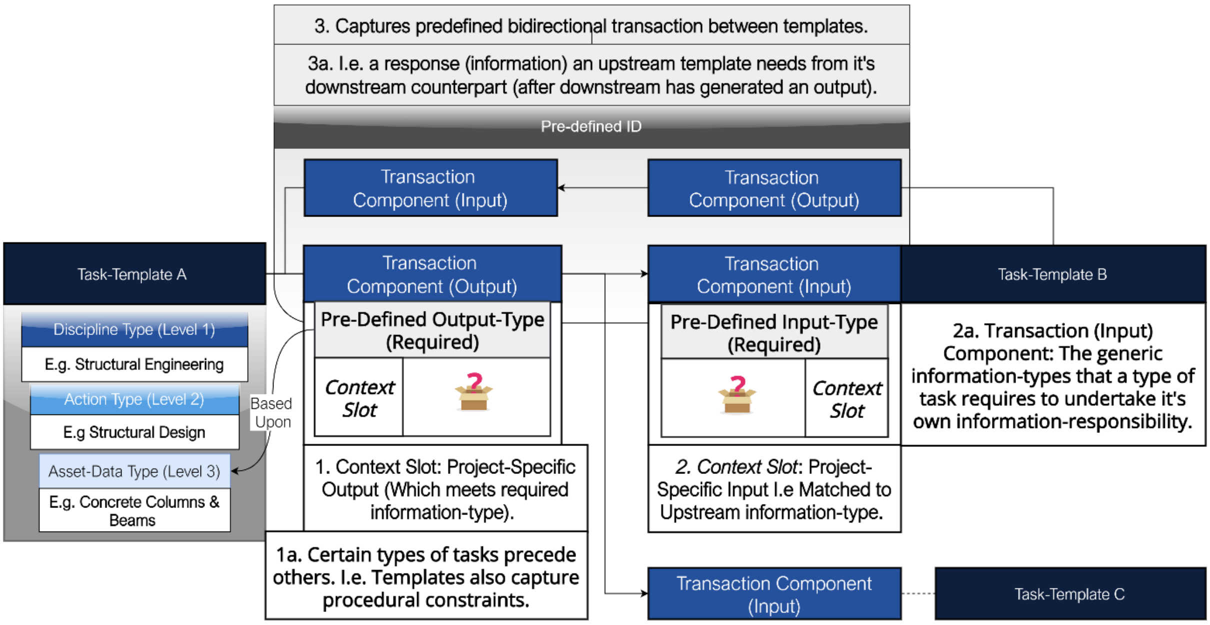

3. Captures predefined bidirectional transaction between templates.
3a. I.e. a response (information) an upstream template needs from it's downstream counterpart (after downstream has generated an output).
Pre-defined ID
Transaction Component (Input)
Transaction Component (Output)
Task-Template A
Transaction Component (Output)
Pre-Defined Output-Type (Required)
Context Slot
Transaction Component (Input)
Pre-Defined Input-Type (Required)
Context Slot
Task-Template B
2a. Transaction (Input) Component: The generic information-types that a type of task requires to undertake it's own information-responsibility.
Discipline Type (Level 1)
E.g. Structural Engineering
Action Type (Level 2)
E.g Structural Design
Asset-Data Type (Level 3)
E.g. Concrete Columns & Beams
Based Upon
1. Context Slot: Project-Specific Output (Which meets required information-type).
2. Context Slot: Project-Specific Input I.e Matched to Upstream information-type.
1a. Certain types of tasks precede others. I.e. Templates also capture procedural constraints.
Transaction Component (Input)
Task-Template C

Figure 5.24: Task Template Transaction

As depicted within **Figure 5.24**, a templates output and input component together form a transaction component i.e. the generic information-types required as outputs and inputs to another template. In addition, the pre-defined IDs also depicted by **Point 3** within **Figure 5.24** represents a high-level link between two templates to represent the ability to capture predefined bidirectional transactions. The following points provide context to **Figure 5.24** from the transaction component perspectives.

- **Transaction Output Component**: A template's output-component is based upon its information-type (given context by upper-level designations). TCs assigned to project-specific tasks **extended from a template** must submit information which meets the pre-defined output-component.
    - This is allocated an output 'contextual-slot' to inform, direct and require a project-specific BIM information-type is generated to fill the slot based on the type of task.
- **Transaction Input Component**: A templates transaction input-component as pre-defined information-needs is matched to the generic information-types to be provided by the upstream template's transaction output component.
    - A link is thereby present between output and input components. It is *expected* these information-type/s will be provided based upon its own task-type responsibility.
    - This approach also implicitly captures sequential dependencies between different task-types whereby upstream information is required to initiate downstream tasks.

A transaction's component input-slot thereby allows TCs instantiating tasks from templates to query against the information-type that is needed against the templates requirements. Template therefore acts as a process-centric data container that expect certain types of sub-tasks will be carried out by a TC, and that they will generate certain *types of* information which they will provide real-life context.

A templated approach also *expects* that certain types of information-output will exist within the spatial context of a real asset. This approach also pre-considers that another TC will be *reliant* upon certain types of information. As such, when, a real-life task is extended from a template, the real-life task possesses the pre-defined link between transaction components depicted in **Figure 5.24**. This may for example be a type of heating-system where the specialisation aspect will be project-specific and determined by real-life actors themselves.

The key factor however is that it is known a *type* of heating-system is required, and the contextual-slots of a transaction component enables the capture of the project-specific aspect. This in turn allows downstream dependent actors to query against the predefined ID. The requesting TC does not need to 'discover' via manual dialogue who else can support their information-needs. Rather, predefined links would already exist for a system to infer whether the output has been derived. This is further detailed within the next section.

The other core benefit of a templated approach is that TCs extending a template are given a 'starting-point' of what types of actions (software included) will be required, and what types of inputs / outputs will be required to / from who. This in turn enables and requires them to provide in-depth consideration of project-specific requirements; as this is an data-driven approach, these considerations are explicitly captured to be communicated with mutually relevant parties such that no ambiguity is present in the information-planning and enablement amongst professionals.

Summary: The implementation templates from a project implementation perspective are also intended to provide an approach whereby additional dialogue is not necessary in creating atomic IDs. This approach may decrease procedural inefficiencies in capturing IDs between actors who would leverage templates as a starting point in defining their task-based responsibilities. This is with a view of information-types required to and from other actors to fulfil their input and output slots. Project-specific requirements and constraints can thereafter be layered with this starting point in-mind.

In addition, templates may be composite, comprising sub-task templates in themselves. For example, the extension of a template to design a particular type of heating-system would by extension expect the generation and sharing of particular components. These would be representative of the types of IFC members that are required for the composite template.

Finally, it is noted templates are aligned to interoperability initiatives. This is however implicit as the focus of the research is to expand core ideas from the perspective of enabling secure pull-based exchanges within systems architecture. **Section 5.3.5.2** however provides some preliminary considerations of the overlap potential for providing a generalisable to further specific representations of stakeholder's processes at industry level, via template libraries.

5.3.5.1 Transactions via Templated Approaches

This section will detail pull-based transaction scenario based around a templated approach. Firstly, newly extended templates inherit from their parent templates transaction components. This includes extended tasks with pre-defined IDs with counterpart producing templates. This is such that they can query information-needs. **Figure 5.25** provides a depiction of at the first instance of wherein tasks have been extended from parent templates.

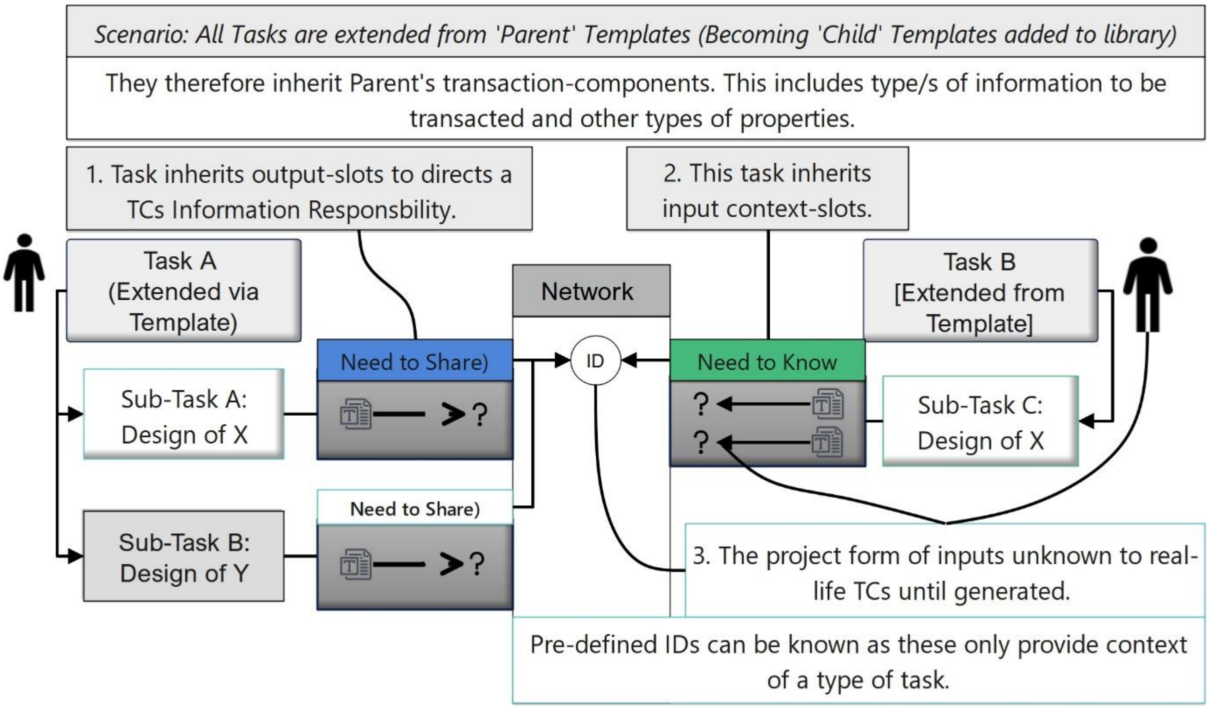
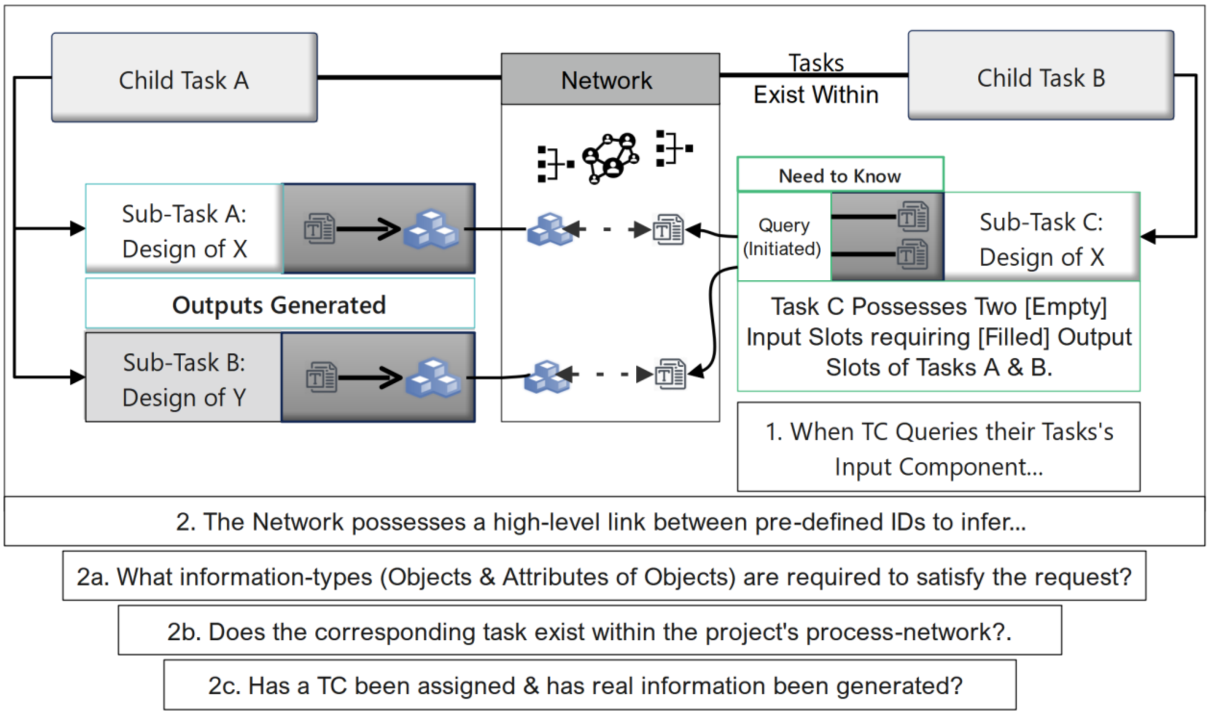

Scenario: All Tasks are extended from 'Parent' Templates (Becoming 'Child' Templates added to library)
They therefore inherit Parent's transaction-components. This includes type/s of information to be transacted and other types of properties.
1. Task inherits output-slots to directs a TCs Information Responsbility.
2. This task inherits input context-slots.
Task A (Extended via Template)
Network
Task B [Extended from Template]
Need to Share)
ID
Need to Know
Sub-Task A: Design of X
?
Sub-Task C: Design of X
Need to Share)
Sub-Task B: Design of Y
?
3. The project form of inputs unknown to real-life TCs until generated.
Pre-defined IDs can be known as these only provide context of a type of task.

Figure 5.25: Template Pre-Query

Firstly, **Figure 5.25** depicts a generalised scenario where all tasks were extended from 'parent' templates. This informs the need to know and share, but also places constraints on types of information required. The depicted tasks inherit the input / output slots based upon the template's transaction-components.

This is such that the extended tasks expect that project-specific information will be generated to fill them. Accordingly, Task C possesses predefined IDs to Tasks A and B, where the slots of their output-component align to Task Cs input components (information-type required to satisfy Task Cs need to know). The following route depicted by **Figure 5.26** occurs when TCs query information from a task extended from a template. This presumes a scenario where upstream information has been generated.



Task C Possesses Two [Empty] Input Slots requiring [Filled] Output Slots of Tasks A & B.

1. When TC Queries their Tasks's Input Component...

2. The Network possesses a high-level link between pre-defined IDs to infer...

2a. What information-types (Objects & Attributes of Objects) are required to satisfy the request?

2b. Does the corresponding task exist within the project's process-network?.

2c. Has a TC been assigned & has real information been generated?

Figure 5.26: Figure 5.26: Template Transaction Scenario 1

When the TC initiates a query, a system implementing a templated approach would cross-reference its own template library with the project's live process network to identify the counter-part templates with matching transaction-components. I.e., whether upstream tasks output-component matches the information-type needed of downstream task's input-component.

Figure 5.26 also depicts a network as the collection of all actors, tasks and IDs would infer if counter-part upstream tasks are live i.e. an upstream TC has been assigned to the matching task. If so, the system would return to a querying TC that a corresponding task exists. Similarly, the relevant counterpart TC is notified of relevancy. The pre-existing ID is thereby made known.

If both TCs decide to proceed, the ID would be actualised for on-going information-flows and information would be released. This would thereby link to the newly extended tasks input-components i.e. the information-types from the need to share required to satisfy the downstream tasks need to know.

The final scenario to note is depicted in **Figure 5.27** is where a network infers that a correspondent TC has been assigned to a task, but no output has yet to be generated. Via such scenarios, the requesting party would receive the response that no information exists of a given task-iteration, correspondingly, the counter-part TC would also be notified of a pending request. It would thereafter be the GR / TMs responsibility to thereafter ensure the response is met.

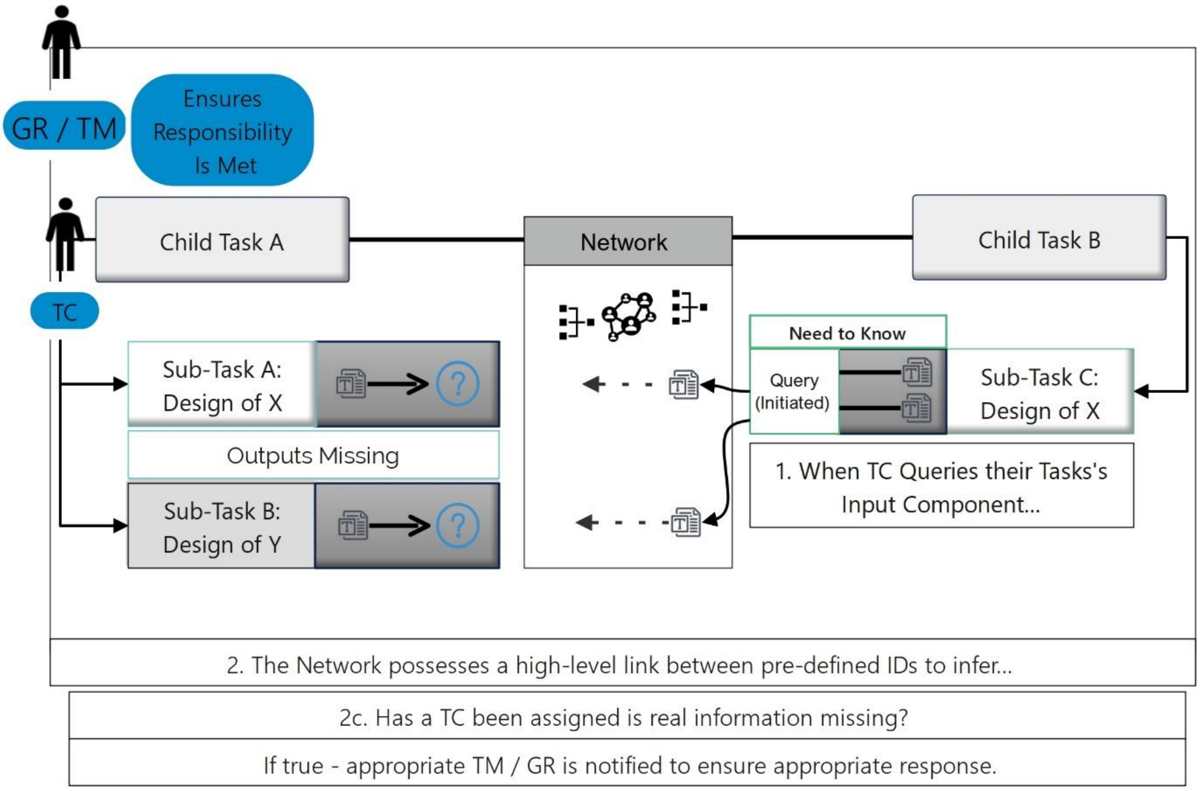

GR / TM
Ensures Responsibility Is Met
Child Task A
Network
Child Task B
TC
Need to Know
Sub-Task A: Design of X
Query (Initiated)
Sub-Task C: Design of X
Outputs Missing
1. When TC Queries their Tasks's Input Component...
Sub-Task B: Design of Y
2. The Network possesses a high-level link between pre-defined IDs to infer...
2c. Has a TC been assigned is real information missing?
If true - appropriate TM / GR is notified to ensure appropriate response.

Figure 5.27: Template Transaction Scenario 2

Summary: In summary, system implementation of a templated and networked approaches (as directionality between all task's, actors and relation to project-data) should infer and return to querying TCs whether a correspondent upstream task (based itself on a template) has been: (a) extended and assigned an actor and (b) whether upstream information has been provided project-specific context. If so, upstream task with an output-component would feeds into their task's input-component.

5.3.5.2 Extendibility of Task Templates

Templates must be extendable as project-specific work varies based upon (a) client-requirements and (b) project methods / constraints. This section therefore details the general concepts for template extension to accommodate for project-specific factors.

Firstly, an implementing system should find and inform downstream TCs of relevant project-specific information. This is if the information has been generated and instantiated into the spatial context of an asset. This should satisfy many scenarios for TCs in querying information against their general task-type, and information-types commonly required.

Conversely, a templated approach should assume and account for scenarios where this may not be the case given the actual project-specific context of any number of diverse, and specialised process requirements within BIM projects. The framework reconciles this need via patterns to meet scenario where the requesters project-specific information-needs are not fully aligned to the information-responsibilities for outputs of a counterpart task derived from a matching counterpart.

The latter scenario of misalignment between actors of their project specific responsibility and needs is depicted within the **Figure 5.28** where the upstream TCs task has generated [non-specific] outputs, with minimal change from the parent templates requirement.

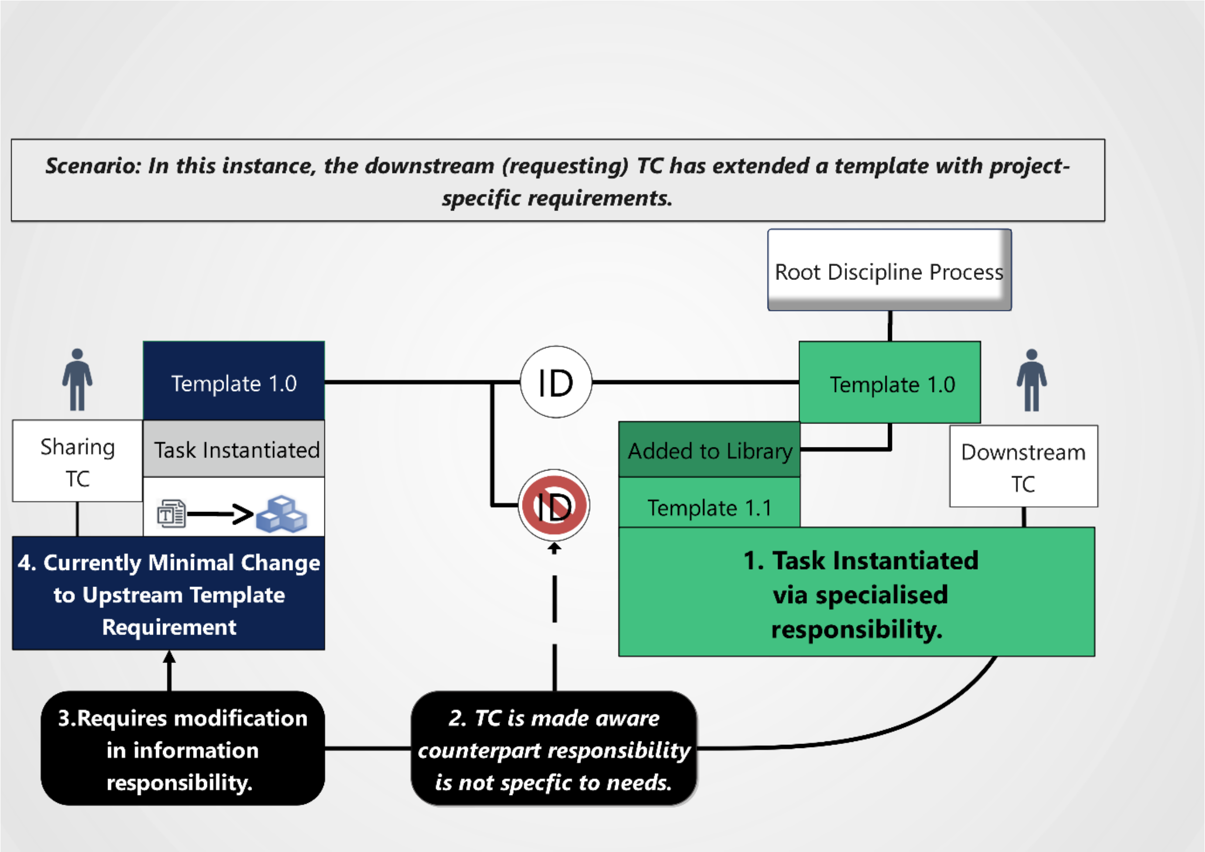

Scenario: In this instance, the downstream (requesting) TC has extended a template with project-specific requirements.
Root Discipline Process
Template 1.0
ID
Template 1.0
Sharing TC
Task Instantiated
Added to Library
Template 1.1
Downstream TC
4. Currently Minimal Change to Upstream Template Requirement
1. Task Instantiated via specialised responsibility.
3.Requires modification in information responsibility.
2. TC is made aware counterpart responsibility is not specfic to needs.

Figure 5.28: Template Extendibility (1)

The focus in **Figure 5.28** is thereby from the perspective of a downstream requesting TC having extended their task with a project-specific use-case. Having instantiated the task, the downstream TC is made aware of a real-life counterpart TC, but also that the upstream task's need to share requirements are not representative (in whole / in part) in meeting their needs for their project-specific responsibility.

Furthermore, by simply extending a template, the downstream party has provided notice of their requirements (attached to project-task]. Implementations should make both upstream TCs and their TMs / GRs aware their output is no longer specific to the downstream TCs information-needs. This factor is depicted within **Figure 5.29**.

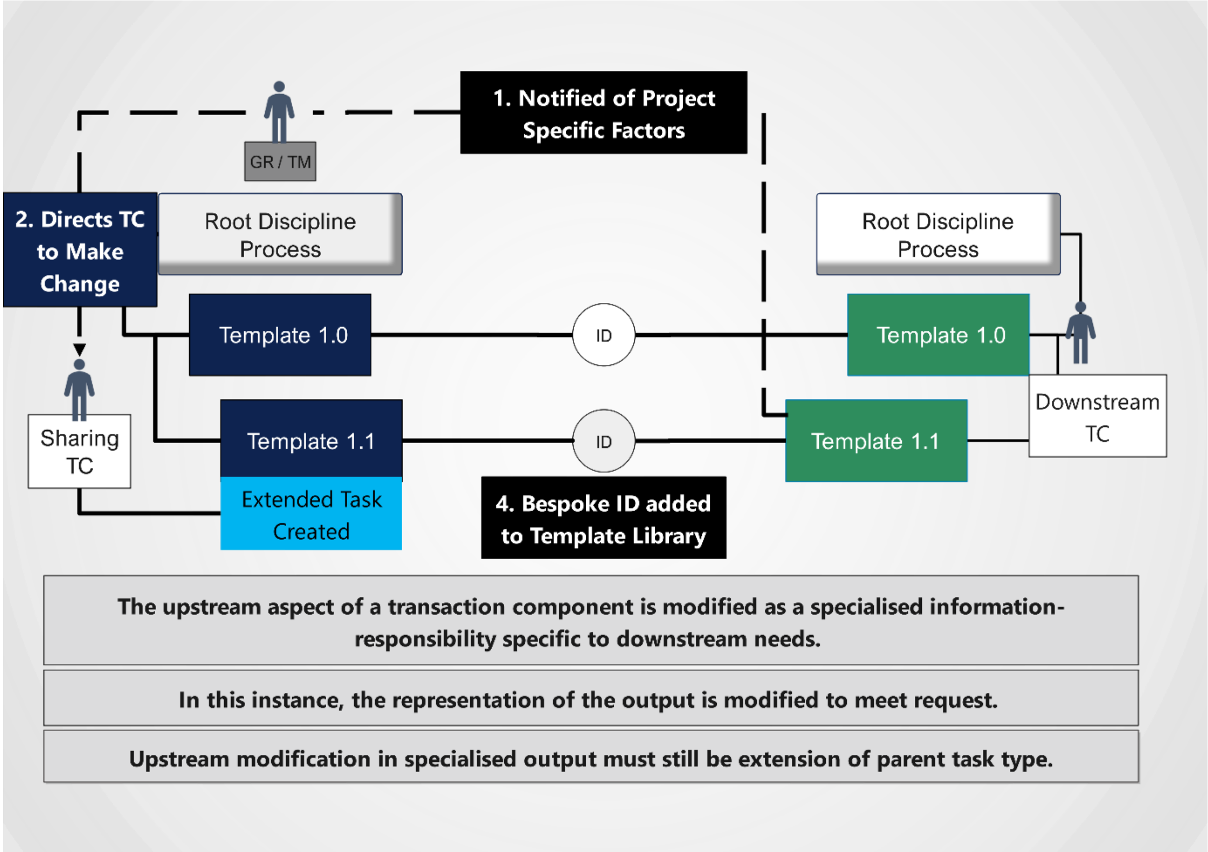

1. Notified of Project Specific Factors
GR / TM
2. Directs TC to Make Change
Root Discipline Process
Root Discipline Process
Template 1.0
ID
Template 1.0
Sharing TC
Template 1.1
ID
Template 1.1
Downstream TC
Extended Task Created
4. Bespoke ID added to Template Library
The upstream aspect of a transaction component is modified as a specialised information-responsibility specific to downstream needs.
In this instance, the representation of the output is modified to meet request.
Upstream modification in specialised output must still be extension of parent task type.

Figure 5.29: Template Extendibility (2)

Also depicted in **Figure 5.29**, the upstream GR / TM thereafter notifies the sharing TC their task-level output to be rectified. This would see the upstream task extends its task's information-responsibility, in view of a particular IDs information-needs. This in turn results in a modification in the upstream task-level process which is matched to the downstream template. The output is in turn rectified a modification of the information-planning perspective. This may for example simply be that the representation of the output changes by providing an altered visual representation of the output, which would thereby provide a new version of the template against the parent template.

Given the numerous IDs any given TC may possess, a system built upon this extendibility perspective should provide TCs with fluid interplay in providing for production of information in view of particular requirements of ID TCs. It should also utilise the inherent nature of task-iterations for change-management of different outputs as a responsibility for a TM.

Finally, **Figure 5.30** depicts that libraries can upon the derivation of a parent task-template, lead to further branching templates. These would still be in line with commonalities of structuring a task discussed within **Section 5.3.5** but would capture further specialised representations of task-level information responsibilities. Such responsibilities, and specific relevant ID information transactions would be captured as part of such extended transaction components.

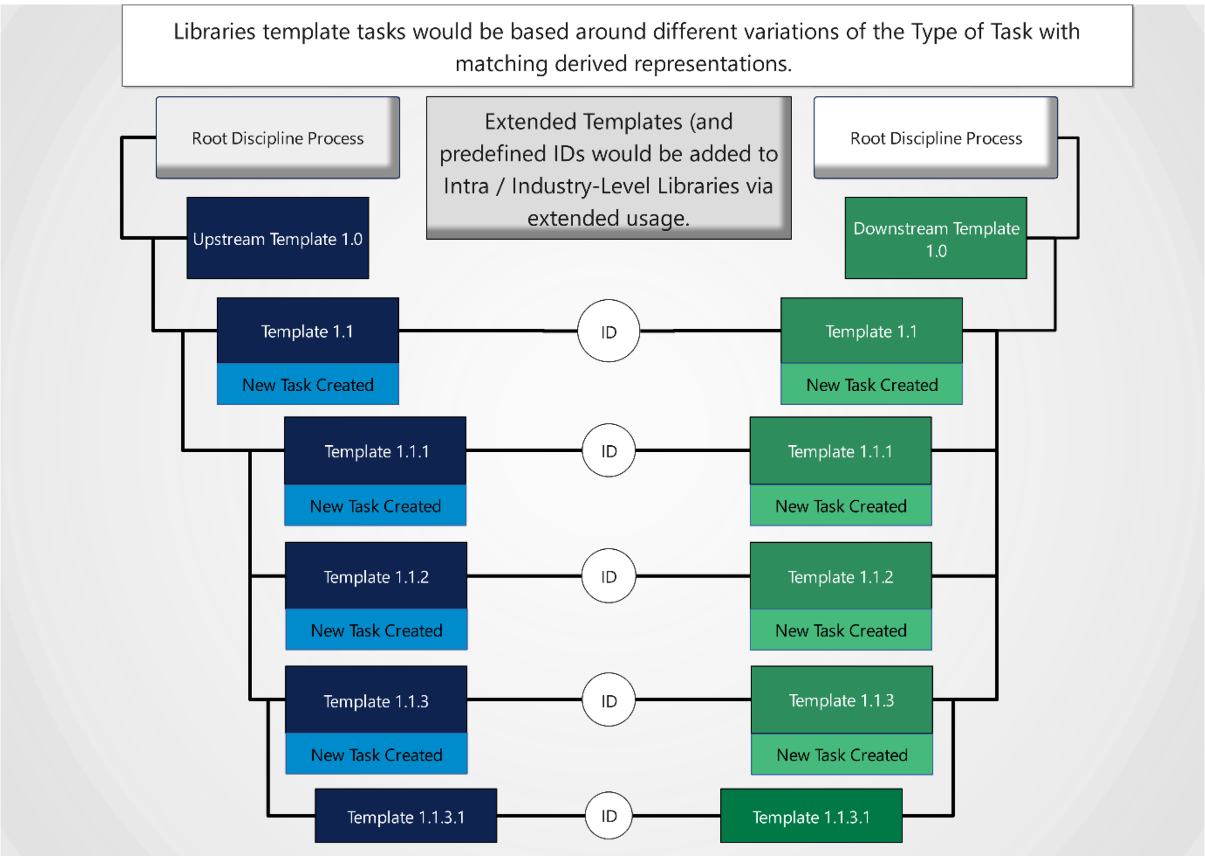


Figure 5.30: Template Extendibility (3)

Discussion: This section explores an envisaged extension process for templates. The main intention is efficient information-planning for pull-based exchange and governance approaches. It is also linked to a broader proposal of enabling a standardised, data-centric definition of atomic processes with commonalities, differences and constraints captured amongst different project-contexts. This represents a proposal in extending knowledge capture for AEC processes where libraries could be achievable via industry 'crowd-sourcing' initiatives. Individual partners could share anonymised templates representative of their specialisations, and other partners could utilise published templates, or entire libraries as a whole.

As such, project-process knowledge reuse is captured for internal purposes, which via a templated approach can be shared amongst industry-level partners for a crowd-sourced approach to process and information-planning capture. Adaptors could be both industry partners and software vendors to facilitate seamless data-centric capture of specialised process-knowledge for real projects. It is envisaged adaptors could capture libraries of more specific templates relevant for their internal work-processes.

These libraries could be interlinked and further refined via process knowledge captured via on-going interactions with stakeholders. This could allow stakeholders and their actors to choose their tasks information-planning (needs and responsibilities) via pre-defined template libraries. Feedback of the concept noted that this could be in view of particular types of tasks, or potentially types of projects and assets as a whole.

5.3.5.3 Governing Sensitivity via Templated Approaches

Sections 5.2.3.4 and **5.2.4.6** discussed patterns for GRs in governing atomic exchanges. This section details the request of information which has been deemed sensitive by internal GRs. It is assumed GRs would have appropriately assessed sensitivity of information in view of security-risk. This links to a general requirement for inter-organisational and hierarchal security-risk governance at project-onset and continuing thereafter. This section however expands upon the pattern of response to a query indicative of sensitivity via a templated approach.

A templated approach provides further benefit to alleviate current scenarios where sensitive aspects redacted from information-containers of lesser classification leaves gaps within lesser sensitivity models (**Section 4.5.2.5**). Firstly, the sharer's GR would be notified of requests and must appropriately govern responses. This is depicted within the following **Figure 5.31**.

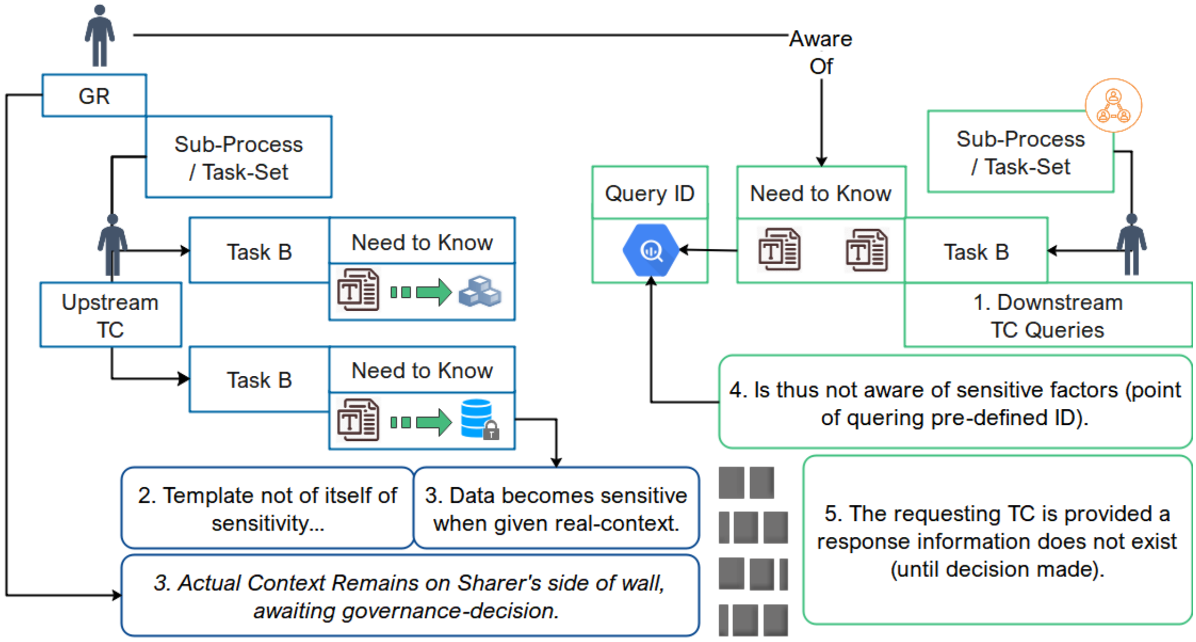

Aware Of
GR
Sub-Process / Task-Set
Task B
Need to Know
Upstream TC
Task B
Need to Know
2. Template not of itself of sensitivity...
3. Data becomes sensitive when given real-context.
3. Actual Context Remains on Sharer's side of wall, awaiting governance-decision.
Query ID
Need to Know
Sub-Process / Task-Set
Task B
1. Downstream TC Queries
4. Is thus not aware of sensitive factors (point of quering pre-defined ID).
5. The requesting TC is provided a response information does not exist (until decision made).

Figure 5.31: Templated Approach to Govern Sensitivity

As noted in **Point 5** of **Figure 5.31**, queries would not return a response until a decision has been set. Classified information can only be released if a TC meets the required clearances and additional governance in line with the need to know principle. Further to this, the boundaries that were noted as issues in **Section 4.5.3** act as a benefit via a pull-based governance approach. This is as the project-specific context of originated information, including factors that imply sensitivity remain with the originator who can choose what not to disclose. E.g. detailed functions and attributes of a lab room handling sensitive materials.

Via a templated approach, information is also only given context when instantiated into the project-specific context of the asset, and its spatial-context (i.e. where a given aspect of an asset resides in real-space). Until this point, planned information does not present sensitivities. This is also depicted within **Point 3** of **Figure 5.31**. As such, the implications of a task in planning or generating sensitive information is not disclosed to requesting TCs.

The benefits of a templated approach present the following governance response scenarios. This being based on GRs who possess a direct view of the requesting TCs need and clearances. This is depicted in **Figure 5.32** and expanded on via descriptors.

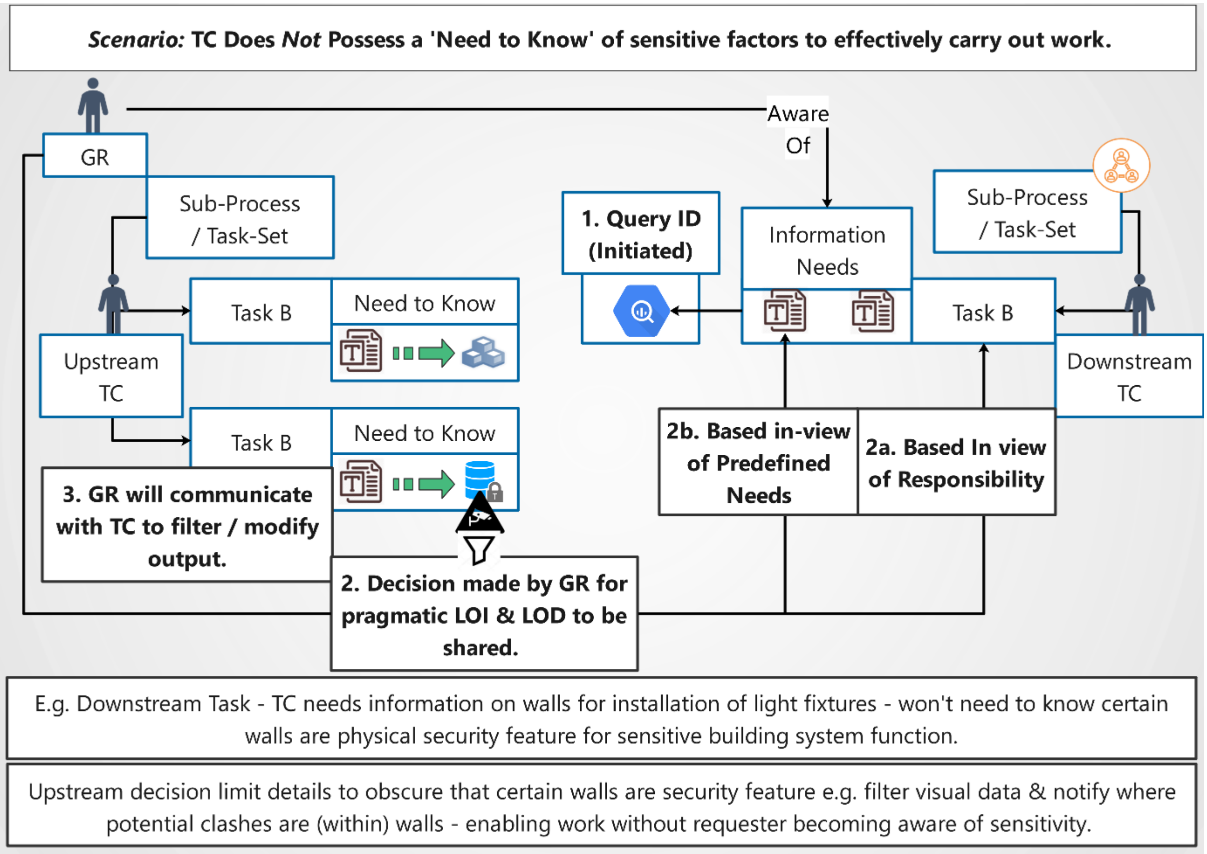

Scenario: TC Does *Not* Possess a 'Need to Know' of sensitive factors to effectively carry out work.
Aware Of
GR
Sub-Process / Task-Set
Task B
Need to Know
Upstream TC
Task B
Need to Know
3. GR will communicate with TC to filter / modify output.
2. Decision made by GR for pragmatic LOI & LOD to be shared.
1. Query ID (Initiated)
Information Needs
Sub-Process / Task-Set
Task B
Downstream TC
2b. Based in-view of Predefined Needs
2a. Based In view of Responsibility
E.g. Downstream Task - TC needs information on walls for installation of light fixtures - won't need to know certain walls are physical security feature for sensitive building system function.
Upstream decision limit details to obscure that certain walls are security feature e.g. filter visual data & notify where potential clashes are (within) walls - enabling work without requester becoming aware of sensitivity.

Figure 5.32: Templated Sensitivity Scenario (1)

Query Scenario (No need to release sensitive information): **Figure 5.32** represents the requesting TC has queried information. Based in direct view of the requesting tasks responsibilities, the GR may deem there is no need to share the sensitive aspect of a task's output. Accordingly, only the upstream information relevant to the requesting TC would be released. This requires the GR of the sharing organisation filters based upon the relevant LOI and LOD to the requesting TCs need to know. This in turn implicitly creates an extended template, where a derivation of a task occurs if some aspect of geometric or attribute-level aspects of an output must be modified in communicating the aspect of the design to other parties, based upon their needs to achieve their task.

- These considerations are aligned to pragmatic decisions and filtering of information, and is in consideration of methods to communicate the essential aspect of information needed for actors to undertake their tasks without (a) mass elevation of clearances or (b) obvious 'gaps' left in an actors access.

- A installations-centric example of a task was captured via research-analysis and noted in **Figure 5.32** where the individual simply requires information on the walls, but without explicit detail that walls (in any part of the assets spatial-map) serves as a physical security-feature, or the further vulnerable aspect of what it protects.

In this sense, templates also serve a purpose of identifying the ideal information to meet a given work-unit. In some instances, this may also the minimum, and is determined as necessary. This represents the need to know principle is applied as part of governance for either security-minded environments with definitive tiers of information or those without in the broader sector in still ensuring appropriate governance. Accordingly, the following **Figure 5.33** characterises the scenario where a GR has deemed a requester possesses a need to know of sensitive aspects.

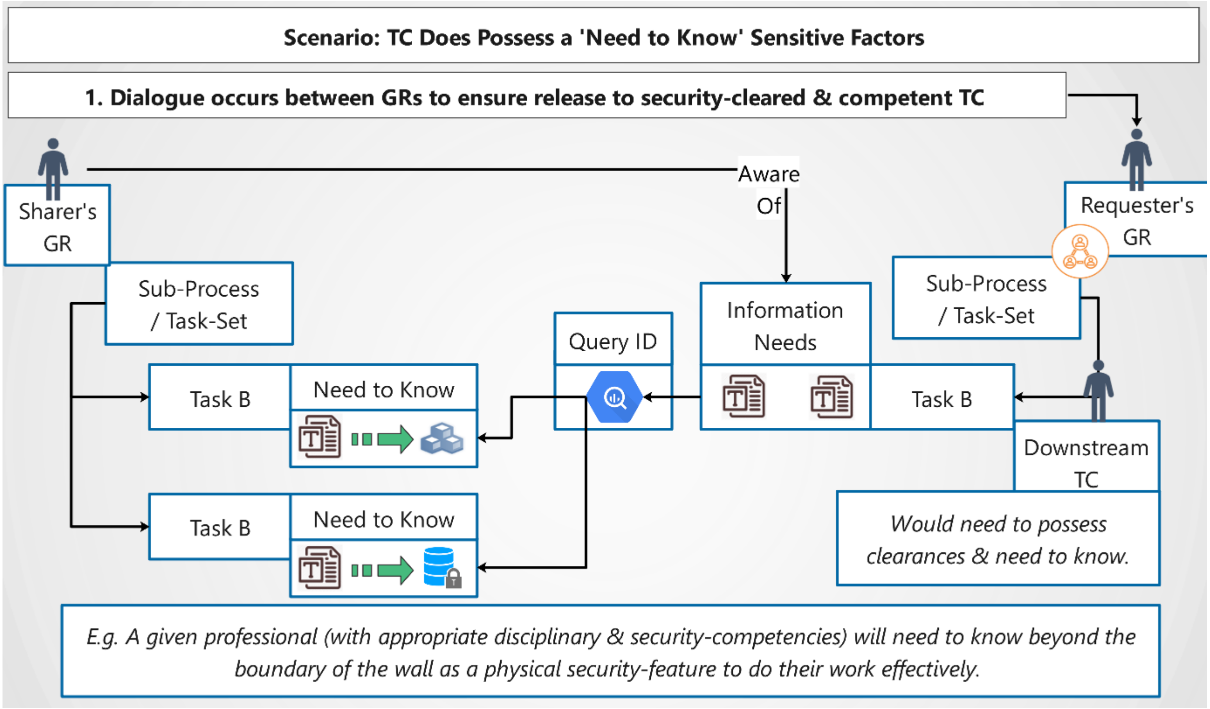

Scenario: TC Does Possess a 'Need to Know' Sensitive Factors
1. Dialogue occurs between GRs to ensure release to security-cleared & competent TC
Sharer's GR
Aware Of
Requester's GR
Sub-Process / Task-Set
Sub-Process / Task-Set
Query ID
Information Needs
Task B
Need to Know
Task B
Task B
Need to Know
Downstream TC
Would need to possess clearances & need to know.
E.g. A given professional (with appropriate disciplinary & security-competencies) will need to know beyond the boundary of the wall as a physical security-feature to do their work effectively.

Figure 5.33: Templated Sensitivity Scenario (2)

Need to release sensitive information: The GR deems the requesting TC possesses the need for information, thereby deciding *certain* sensitive aspects would be released. This is still on a *need to know basis* to an individual TC with the correct security-clearances which should be determined based upon competencies (disciplinary and security). The GR of the upstream organisation would communicate with the downstream GR to ensure these conditions have been met prior to release. Further iterations of outputs to a cleared TC could be semi-automated.

Rather a templated approach ensures that certain elements / attributes have been categorised against the transaction output-component and they will at some point exist within the network. This is as opposed to a manual approach wherein it must be manually determined that certain tasks outputs may become sensitive as some point. Accordingly, predictive features could also be utilised in flagging awareness for GRs over on-going iterations for streamlined, effectual governance. This is particularly pertinent in responding to queries where sensitivity concerns are present the sharing task due to increasing LOI and LOD, even if risk has been cleared in respect to a previous task-iteration (and its outputs).

5.3.5 Summary: Overall, this section has explored concepts of re-using project-knowledge in the form of templates, for collaborative and security purposes. The final section of the framework concepts to be explored is the network concept. In response to incoming queries over tasks GRs govern, it should be possible for GRs to possess views to visualise and validate whether actors under their governance has met their task responsibility prior to release to queries. This can likely be semi-automated to an extent, as a task's submitted outputs should only be accepted if it matches the information-types a given template directs.

5.3.6 Exploration of Network Concepts

5.3.6.1 Introduction to Networked Concepts

This section details the general process network concept arising from the culmination of gap-analysis (**Sections 4.5.3**). Issues being: (a) limited visibility and recognition of overlaps in the task-work of stakeholder's actors; (b) limited validation exchanges meet suitability / security needs and associated governance difficulties; (c) inability to govern the continuity of responsibilities, or simply capture overlaps in processes.

A network extrapolates the notion of bidirectionality in interconnecting all tasks within a project's process, which naturally forms a 'network' of tasks. Human actors would be embedded in a network as a digital representation of a professional assigned to a task. Human actors would also reference a *point* within the digital representation of hierarchal entities which would also be captured i.e. teams within organisations within appointment-chains. A network would capture relationships between entities themselves and professionals therein within and across teams, organisations, and appointment-chains.

This section details high-level considerations for a fully realised network could achieve from an information planning perspective leading to progressive exchanges, whereby TCs should be able to possess a live understanding of factors relevant to their optimal work. This section expands upon the general concept, having introduced other relevant concepts such as sub-tasks.

Firstly in response to overarching needs for reducing the 'disconnect' and latency between TCs and enabling them to reconcile their need to know and share, **Figure 5.34** depicts an abstract representation which depicts tasks (and their TCs) acting as nodes within the network in inter-connecting team-level actor's and their tasks, either internally or externally.

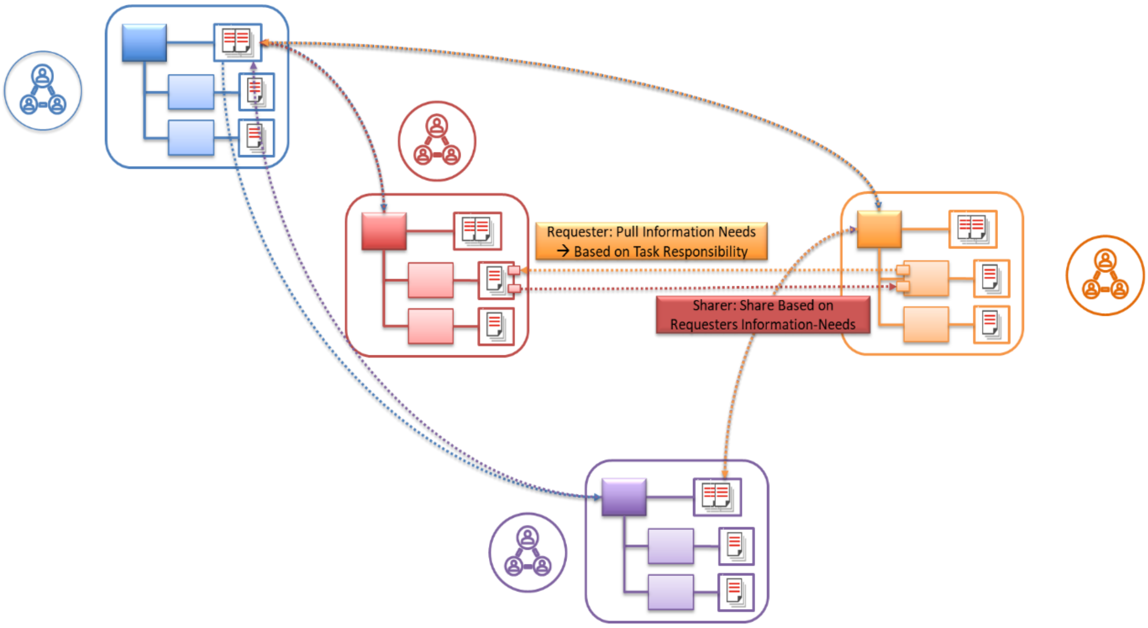

Requester: Pull Information Needs
→ Based on Task Responsibility
Sharer: Share Based on
Requesters Information-Needs

Figure 5.34: Network Concept (1)

In **Figure 5.34**, all tasks are inter-connected. An implementing platform and system-specific implementation of a network would enable real-time connectivity over information-flows. It is postulated that many atomic tasks, more-so than depicted would be occurring on any given project, at any point in time. Many would also be non-design-centric, but their inputs / outputs relatable back to specific spatial-facets of an asset as part of its spatial-map space. It is acknowledged the multitude of transactions taking place on any given project would far exceed the relative simplicity depicted.

As such, it is posed an interconnected architecture is necessary to capture the complexity over atomic processes within the core project-stages, but also capturing atomic progression over lifetime of an asset. With these factors in-mind, the figure aims to depict the following.

- How different organisations and their team's tasks have been decomposed, where all task IDs have been correspondingly mapped if mutual relevancy is present. The inclusion of the actors themselves as part of the network as nodes / points in the network.

- The flow of information amongst these tasks, where each network edge (i.e. directionality) represents a flow of inter-dependent exchange, which will reoccur over many task-iterations.
- A network would hold the associations between all actors' tasks, and association to real-data. As such, the network as seen as an atomic, interconnected and process-oriented data-structure is necessary for achieving atomic pull-based information-flows, and in embedding governance over them.

Summary: A network as a whole represents the project's process-map and all interconnections therein. In a sense, it can also be seen as a project-specific extension of a library of interconnected task-templates. A proof-of-concept implementation may utilise an appropriate real-world technology such as graph databases. This may be held on decentralised server instances. Future technologies could thus provide functionality for the data-centric capture, enablement and governance of the network. Further benefits may however be realised which are noted as future work. The following section will expand upon benefits for enablement from the perspective of TCs whilst **Sections 5.3.6.3** and **5.3.6.4** will expand from GRs perspective.

5.3.6.2 Network Benefits for Collaborating Team-Level Actors

A network would enable TCs to track how their responsibilities should evolve in view of inter-dependent professionals in the network. Accordingly, GRs / TMs can also govern this evolutionary perspective. This aligns to the following high-level scenarios of updated task-level responsibilities being automatically propagated to inter-dependent TCs.

- **Implications to Need to Know**: Notified TCs should recognise another TCs task-update implicates them. They thereafter either: (a) become aware they require the new update or (b) become aware the update requires the *notified* TC to in turn request further new information for themselves.

- **Implications to Need to Share**: Notified TCs should recognise a collaborators task-update implicates them and *how* in understanding whether they should in turn respond in further provision of information (to the professional who has notified them).
    - This may simply be in the provision of a further output-iteration. If the updated task responsibility however requires a specific response or modification from a given notified collaborator, then this should also be facilitated.

Furthermore, and alongside benefits of TCs ability in responding to established ID counterparts (in optimal progressive delivery and receipt of information), networks could provide knowledge of cascading dependencies between actors which are unknown from the perspective of implicated actors. In other words, TCs may be unaware how their task-work indirectly *affects* or is *affected* by other actors removed from themselves in the network and project process accordingly. This may for example be appointees within another appointment-chain, or tasks closed out and no longer live.

Moreover, cascading implications which are likened to a 'butterfly effect' do not appear capturable, and thereby governable. This appears due to limited atomic inter-connectivity of BIM methodologies, both from process and technology standpoints. Conversely, a network captures all inter-connections and could therefore aid in governing cascading needs and responsibilities of all actors, at all levels within a network. Networked information-architectures should be able to infer via their own interconnectedness, the cascading implications of a given TCs information needs and responsibilities upon indirect actors; this also includes queries or submission of outputs.

Networked inferences could enable mutually *unaware* actors in *recognising* the cascading progression in presently unknown, direct / indirect overlaps in TCs tasks. Correspondingly this should enable them to adapt to cascading implications to ultimately ensure the optimal receipt and provision of information. The benefits of interconnectedness may also go beyond optimal and secure delivery of information. In consideration of a network to govern the cascade-effect of BIM processes, the following potential benefits are posed.

Benefit Posed (1): From the perspective of the requester not being able to receive information (querying a task extended from template), a network would infer if a TC has been assigned to a corresponding upstream task. If they have, they would be required to deliver the information. An upstream task may be unable to do so, however. For example, if a task is incomplete at some part in the network.

If such a scenario occurs, then the actor initiating the request would normally be unaware of (a) how many actors are required to respond as part of a 'request-chain' and (b) ultimately, who is the final actor responsible in resolving the chain.

This unawareness is due to actors being multiple 'steps' removed from each other in respect to workflows and organisational-tiers. Queries via a network could however be propagated throughout itself to reach relevant actors in satisfying the chain. This is possible as a network captures IDs between directly established professionals and their tasks, their neighbours, and so on.

Benefit Posed (2): Understanding implications of how progression in an TCs *Need to Share* affects somebody else's *Need to Know.* In other words, if progression in a TCs responsibility occurs (updates) then it may indirectly implicate hidden TCs. As noted, these hidden IDs would be captured and known by a network, via its own interconnectedness. As such, the implications of actor's progressive responsibilities should be propagated to the relevant TCs.

The motive from the perspective of an actor in generating / sharing capacity is being able to *understand* where the overlaps may arise. This is to thereby ensure their work is being utilised by others where relevant, ultimately in progressing broader project information suitability. This is wherein the complexities of *how exactly* a given TCs responsibilities may implicate other professionals' requirements are difficult to judge, from the perspective of any sole professional or team. Based upon research-analysis, this knowledge is further constrained on projects of higher numbers of stakeholders / complexity of work.

An appropriate interface should thereby notify them of relevancy, which may thereby progress to the capture of new IDs, or simply awareness of the indirect reliance upon information and actors responsible. This may in turn feeds into project-process knowledge expansion (templates section).

Benefits Posed (3): Understanding implications of how progression in a TCs *Need to Know* affects somebody else's Need to Share. This is the mirroring perspective of Benefit 2. Similar to how a TCs information-needs update affects established ID counterparts, their needs could also be propagated out to the broader network. It should be able to capture where hidden overlaps in mutual relevancy of work exist. Again, as with Benefit 2, this would comprise capturing new

IDs if necessary, or simply awareness of indirect reliance (i.e. sequential dependencies) on information.

Benefit Posed (3): Another benefit that may be realised by a networked approach is wherein TCs are able to *direct* the work-responsibilities of other actors. This is as opposed to the perspective of *informing* ID TCs of information-needs. Whilst these perspectives overlap, they are distinct as the former *directive* motive pertains to emplacing and mediating design-constraints on the work of inter-connected actors. This is not particularly a perspective the framework at time of conceptualisation has focused upon. It is hoer noted that it would be possible and could be considered.

5.3.6.3 Networked Governance Perspective

Some factors of a governance overlay over a process-network (i.e. governance network) were previously implicitly explored of GRs being notified of queries to govern responses. The final factors are explored of the overlay as a GRs comprehensive and continuous view of all task-level queries under their purview. i.e. the portion of the network GRs are allocated decision-rights based in turn on their organisation's responsibility. This comprises the teams and tasks they are governing in visualising, tracking, and making decisions upon the internal / external directionalities of units of work, at increasingly decomposable perspectives. **Figure 5.35** characterises this by expanding the network abstraction in view of GRs.

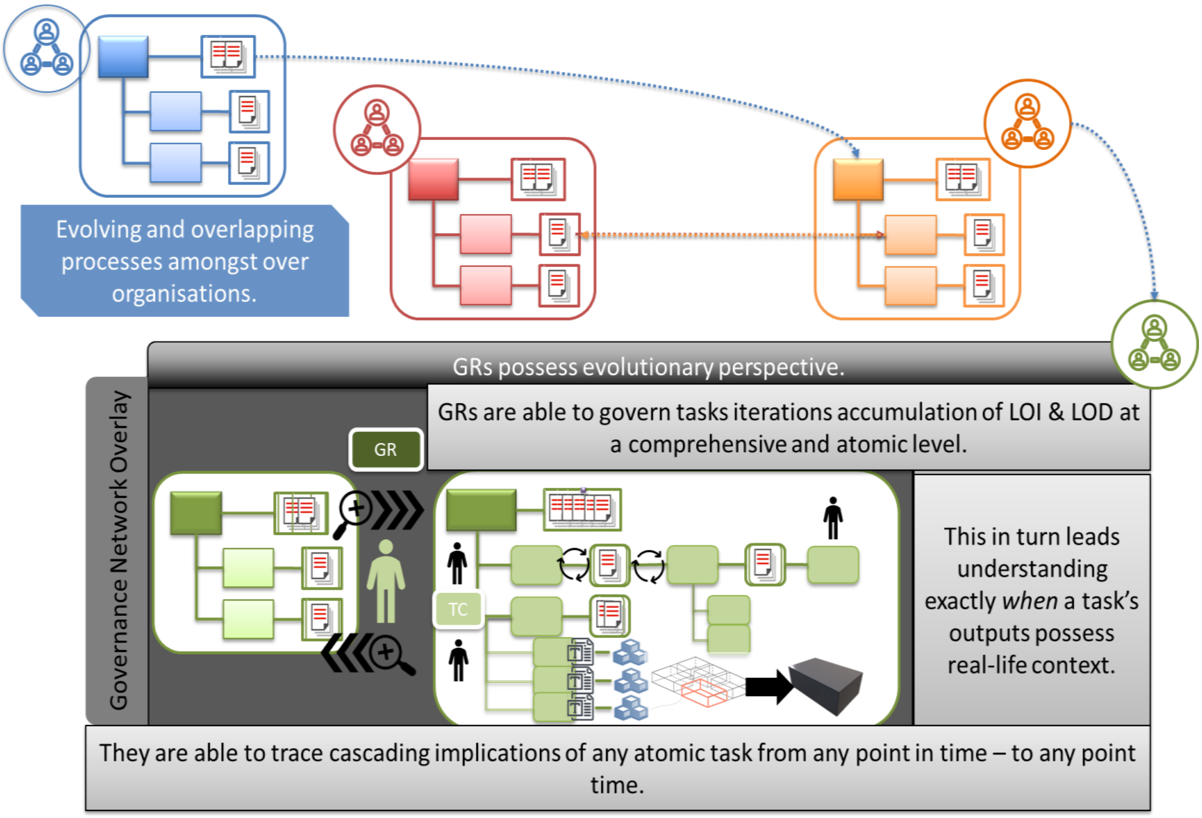

Evolving and overlapping processes amongst over organisations.
GRs possess evolutionary perspective.
GRs are able to govern tasks iterations accumulation of LOI & LOD at a comprehensive and atomic level.
Governance Network Overlay
GR
TC
This in turn leads understanding exactly *when* a task's outputs possess real-life context.
They are able to trace cascading implications of any atomic task from any point in time – to any point time.

Figure 5.35: Networked Governance Approach

Figure 5.35 depicts a perspective of specific flows of data from task to task, over time. I.e. the evolutionary perspective as the ability to capture and view progression in on-going task-iterations, and associated transactions. This includes how atomic tasks accumulate detail and assurance.

Whilst not depicted due to overly visual complexity, the perspective depicted intra-organisationally will also be occurring inter-organisationally. A network will thereby also be evolving at the inter-organisational in capturing the numerous overlaps, and progression thereof. A number of factors are expanded upon.

- Firstly, the internal perspective of the GRs overlay is depicted to note its units of work have expanded to accommodate further extended templates. I.e. GRs can trace implications of present change, but also 'rewind' through the network's progression.
- The expansion of the network has in turn created a directed internal flow between TCs. It is noted via the loop that this section of the network's internal flow will be interdependent to support further iterative progression.

Figure 3.35 also characterises the nature of task-iterations wherein previous tasks have reached a level of progression that outputs are considered to represent their real-life context.

- In tandem with the network providing comprehensive and evolving visibility, the GR is able to consider whether TCs progressive task-iteration information-responsibility (prior to updated output) would be sensitive.
- This would be as the outputs possess real-life context. Its intended function would have been allocated into the spatial context of an asset such that it is known both 'where' and 'what' vulnerabilities a given piece of information may present.

Accordingly, any queries previously directed of a given task and previous versions of outputs may not be implicative of concerns over exposure. However, as a specific task-iteration, and its related data may now implicate sensitivity, a GR must proactively ensure clearances competencies both internal and externally. This is if the clearances have not already been captured. Filtering or the extension of task's outputs may also be required to ensure recipients previously provided another version of an output can carry on without inferring sensitive aspects if they do not possess a need to know.

5.3.6.4 Hierarchal Networked Governance

The decomposability of AEC stakeholders and their project-work within a network is also hierarchal and the network also captures the hierarchal perspective of the appointee's contribution to network. This based upon their information-responsibilities, and thereby their processes. It is posed a GRs hierarchal view enables them to govern tasks and information-flows of their employed organisations. This is in essence an extension as their own internal network as depicted within **Figure 5.36**.

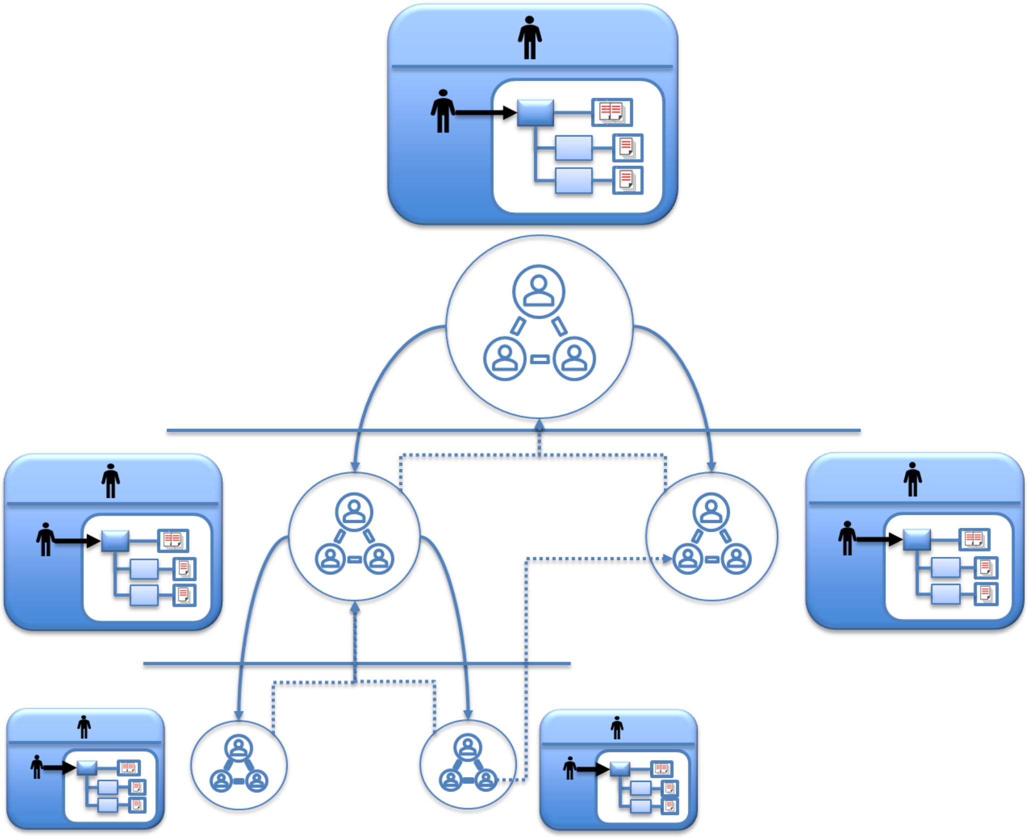


Figure 5.36: Hierarchal Governance Perspective

Figure 5.36 depicts that appointees' processes are increasingly decomposed in terms of: (a) organisational and (b) information-planning level of tasks and sub-tasks. It also implies GRs are able to track and govern information-flows at increasingly decomposable levels from an organisational perspective of the uppermost client level to the lowest tier of SMEs. This creates a comprehensive and atomic chain of information-flow governance. Also, and in line with the evolutionary perspective noted in **Section 5.3.6.3**, an organisation is also able to possess comprehensive and evolving visibility of their appointment-chains. This includes:

- Whether information-planning / actualised transactions are aligned to what must be delivered from an information-suitability perspective by being able to govern information-flows at any level (team / task).
- I.e. ensuring an appointee is meeting the question that needs to be met throughout the lifetime of the appointment, where it can be tracked and audited from / to any point in time.
- Whether information-transaction being queried by appointees are being appropriately upheld in terms of security-risk governance i.e. governance over GRs.
- Each appointee at each tier is aware of what appointers intend to share with them. In also considering a pull-context however, the appointee is also able to pull information from the appointers themselves, and other appointees. This is also depicted in **Figure 5.36**.

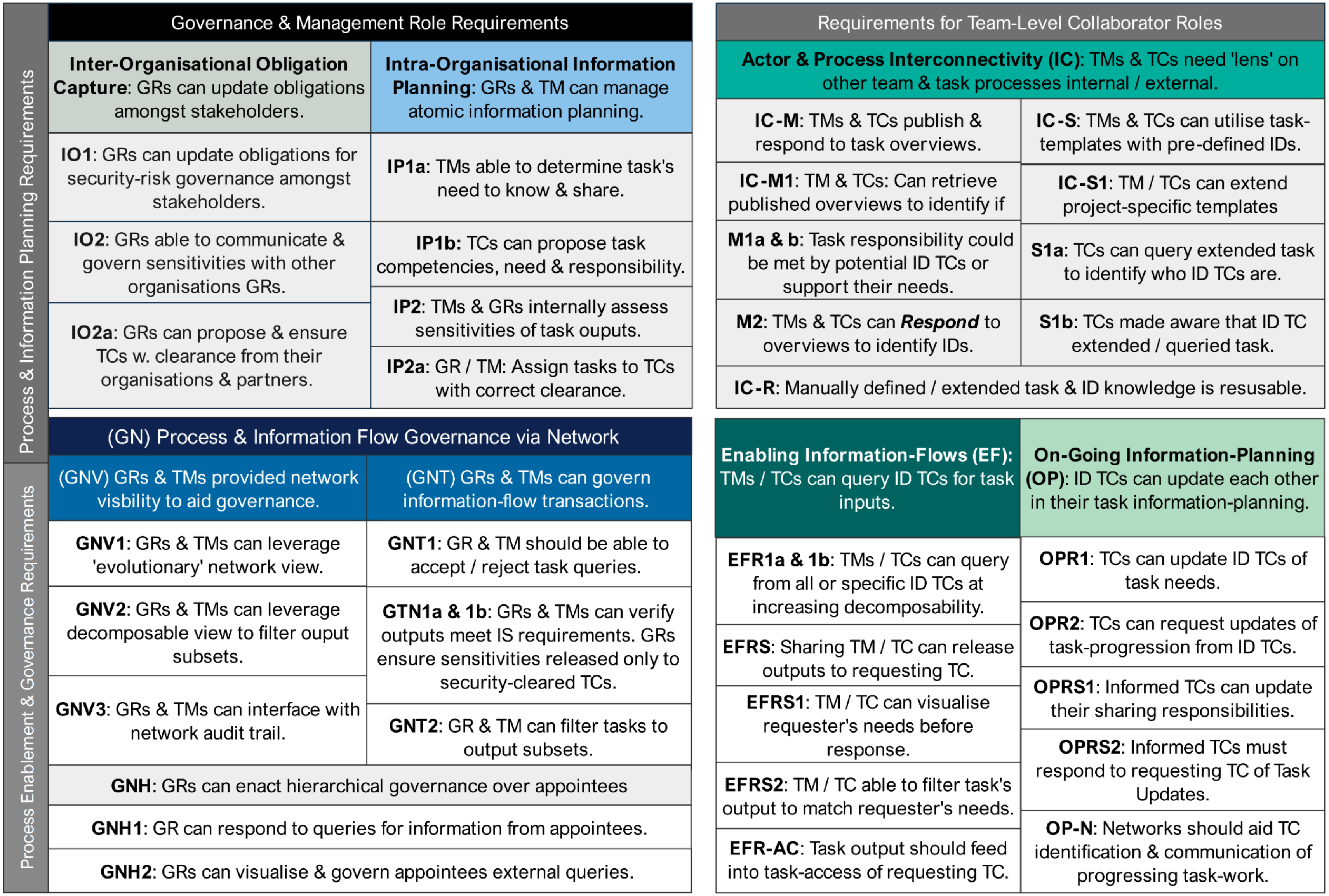
Summary: It is noted the framework posits hierarchal governance as a 'chain', *between* appointer and appointer, where the chain of responses in answering an appointee is fed back up. An implicit potential of the frameworks methods is to provide understanding of atomic overlaps between the appointments present (within and across chains). It should also be noted however that the contractual implications of such an idea having not been fully appreciated until the conceptual solutions based upon and linked to this idea were validated. Critical factors of feedback were captured with respect to this perspective and are detailed within **Sections 6.3.6.**

5.4 Governance Framework Summary

Section 5.3.6 explored high-level conceptualisation of benefits that may be present in professionals being able to reconcile their overlaps in needs and responsibilities amongst each other. This extends to the proposed potential for actors to utilise the inter-connected nature of a network in delivering inferences to ensure suitability of exchange information. The potential benefits of networked architecture also pertain to governing cascading and evolving requirements. The general procedure as a concept in itself, and its relevancy to ensuring governance over information-flows was explored. The network concepts are also aligned to core ideas of the framework of atomic and pull-based information-flows. A networked architecture would underpin these benefits as a network of inter-connected tasks captures relationships. This links to Chapter 5 as a whole having presented requirements of the proposed approach for enabling secure collaboration and has expanded the requirements in more depth via the concepts to shed light on the nature of the proposed method. As both requirements and detailed exploration of the concepts have outlined, this implicates the general BIM methodology of process-setting, enablement and governance, and also of future technologies implementing such methods. The high-level nature of the requirements is acknowledged, and further validation is required the ideas are relevant and sound for their potential implementation. This is noted as the purpose of Chapter 6. The next section however provides an overarching view of the requirements as a whole.

5.4.1 Overarching Framework Representation

The following diagram provides an overarching view of requirements. It should be noted that that inter-connections within domains are omitted to provide as simple a depiction as possible. The inter-connections between the requirements domains are noted however to simply depict that all areas are related.



Process & Information Planning Requirements

Governance & Management Role Requirements

Inter-Organisational Obligation Capture: GRs can update obligations amongst stakeholders.	**Intra-Organisational Information Planning**: GRs & TM can manage atomic information planning.
IO1: GRs can update obligations for security-risk governance amongst stakeholders.	**IP1a**: TMs able to determine task's need to know & share.
IO2: GRs able to communicate & govern sensitivities with other organisations GRs.	**IP1b:** TCs can propose task competencies, need & responsibility.
IO2a: GRs can propose & ensure TCs w. clearance from their organisations & partners.	**IP2**: TMs & GRs internally assess sensitivities of task ouputs. **IP2a**: GR / TM: Assign tasks to TCs with correct clearance.

Requirements for Team-Level Collaborator Roles

Actor & Process Interconnectivity (IC): TMs & TCs need 'lens' on other team & task processes internal / external.

IC-M: TMs & TCs publish & respond to task overviews.	**IC-S**: TMs & TCs can utilise task-templates with pre-defined IDs.
IC-M1: TM & TCs: Can retrieve published overviews to identify if	**IC-S1**: TM / TCs can extend project-specific templates
M1a & b: Task responsibility could be met by potential ID TCs or support their needs.	**S1a**: TCs can query extended task to identify who ID TCs are.
M2: TMs & TCs can ***Respond*** to overviews to identify IDs.	**S1b**: TCs made aware that ID TC extended / queried task.

IC-R: Manually defined / extended task & ID knowledge is resusable.

Process Enablement & Governance Requirements

(GN) Process & Information Flow Governance via Network

(GNV) GRs & TMs provided network visbility to aid governance.	(GNT) GRs & TMs can govern information-flow transactions.
GNV1: GRs & TMs can leverage 'evolutionary' network view.	**GNT1**: GR & TM should be able to accept / reject task queries.
GNV2: GRs & TMs can leverage decomposable view to filter ouput subsets.	**GTN1a & 1b**: GRs & TMs can verify outputs meet IS requirements. GRs ensure sensitivities released only to security-cleared TCs.
GNV3: GRs & TMs can interface with network audit trail.	**GNT2**: GR & TM can filter tasks to output subsets.

GNH: GRs can enact hierarchical governance over appointees

GNH1: GR can respond to queries for information from appointees.

GNH2: GRs can visualise & govern appointees external queries.

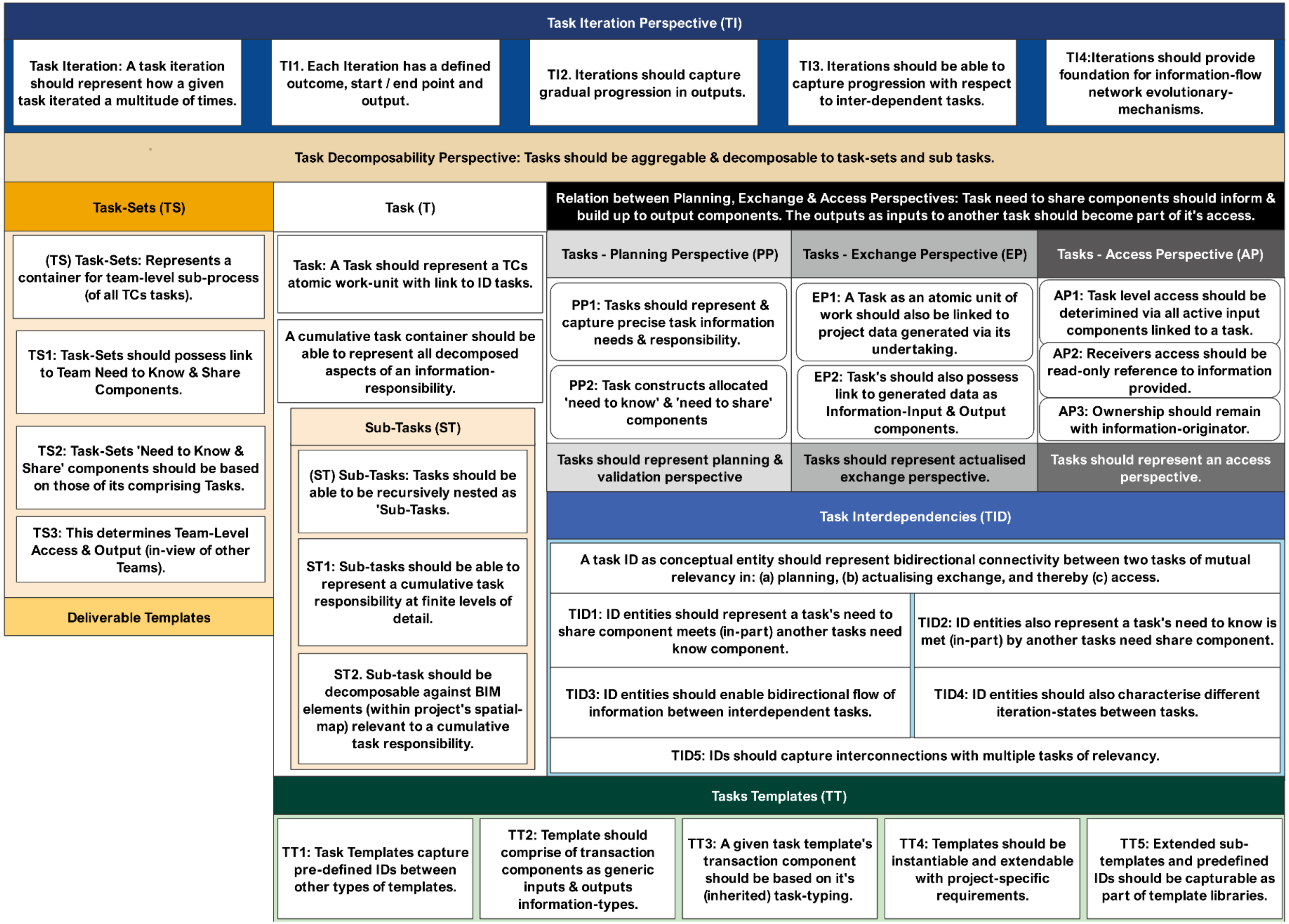
Enabling Information-Flows (EF): TMs / TCs can query ID TCs for task inputs.	**On-Going Information-Planning (OP)**: ID TCs can update each other in their task information-planning.
EFR1a & 1b: TMs / TCs can query from all or specific ID TCs at increasing decomposability.	**OPR1**: TCs can update ID TCs of task needs.
EFRS: Sharing TM / TC can release outputs to requesting TC.	**OPR2**: TCs can request updates of task-progression from ID TCs.
EFRS1: TM / TC can visualise requester's needs before response.	**OPRS1**: Informed TCs can update their sharing responsibilities.
EFRS2: TM / TC able to filter task's output to match requester's needs.	**OPRS2**: Informed TCs must respond to requesting TC of Task Updates.
EFR-AC: Task output should feed into task-access of requesting TC.	**OP-N**: Networks should aid TC identification & communication of progressing task-work.

Figure 5.37: Overarching Framework Requirements

5.4.2 Governance Schema Requirements

Having explored both the overarching requirements and the concepts, this section provides considerations of requirements of a schema, in eventual view of a model capable of representing, capturing, and underpinning atomic, pull-based information-flows and governance thereof. I.e. in underpinning the frameworks overarching approach.

Figure 5.38 depicts a high-level breakdown of requirements of such a schema where the central 'task' entity is related to different perspectives in planning / enabling information-flows. The governance aspect is implicit. This is as a model would simply need to *represent* and *capture* TCs tasks. This by extension provides GRs an overlay of atomic information-flows for them to govern as **Section 5.3** as a whole has as explored the general patterns.



Task Iteration Perspective (TI)

Task Iteration: A task iteration should represent how a given task iterated a multitude of times.

TI1. Each Iteration has a defined outcome, start / end point and output.

TI2. Iterations should capture gradual progression in outputs.

TI3. Iterations should be able to capture progression with respect to inter-dependent tasks.

TI4:Iterations should provide foundation for information-flow network evolutionary-mechanisms.

Task Decomposability Perspective: Tasks should be aggregable & decomposable to task-sets and sub tasks.

Task-Sets (TS)

(TS) Task-Sets: Represents a container for team-level sub-process (of all TCs tasks).

TS1: Task-Sets should possess link to Team Need to Know & Share Components.

TS2: Task-Sets 'Need to Know & Share' components should be based on those of its comprising Tasks.

TS3: This determines Team-Level Access & Output (in-view of other Teams).

Deliverable Templates

Task (T)

Task: A Task should represent a TCs atomic work-unit with link to ID tasks.

A cumulative task container should be able to represent all decomposed aspects of an information-responsibility.

Sub-Tasks (ST)

(ST) Sub-Tasks: Tasks should be able to be recursively nested as 'Sub-Tasks.

ST1: Sub-tasks should be able to represent a cumulative task responsibility at finite levels of detail.

ST2. Sub-task should be decomposable against BIM elements (within project's spatial-map) relevant to a cumulative task responsibility.

Relation between Planning, Exchange & Access Perspectives: Task need to share components should inform & build up to output components. The outputs as inputs to another task should become part of it's access.

Tasks - Planning Perspective (PP)

PP1: Tasks should represent & capture precise task information needs & responsibility.

PP2: Task constructs allocated 'need to know' & 'need to share' components

Tasks should represent planning & validation perspective

Tasks - Exchange Perspective (EP)

EP1: A Task as an atomic unit of work should also be linked to project data generated via its undertaking.

EP2: Task's should also possess link to generated data as Information-Input & Output components.

Tasks should represent actualised exchange perspective.

Tasks - Access Perspective (AP)

AP1: Task level access should be deterimined via all active input components linked to a task.

AP2: Receivers access should be read-only reference to information provided.

AP3: Ownership should remain with information-originator.

Tasks should represent an access perspective.

Task Interdependencies (TID)

A task ID as conceptual entity should represent bidirectional connectivity between two tasks of mutual relevancy in: (a) planning, (b) actualising exchange, and thereby (c) access.

TID1: ID entities should represent a task's need to share component meets (in-part) another tasks need know component.

TID2: ID entities also represent a task's need to know is met (in-part) by another tasks need share component.

TID3: ID entities should enable bidirectional flow of information between interdependent tasks.

TID4: ID entities should also characterise different iteration-states between tasks.

TID5: IDs should capture interconnections with multiple tasks of relevancy.

Tasks Templates (TT)

TT1: Task Templates capture pre-defined IDs between other types of templates.

TT2: Template should comprise of transaction components as generic inputs & outputs information-types.

TT3: A given task template's transaction component should be based on it's (inherited) task-typing.

TT4: Templates should be instantiable and extendable with project-specific requirements.

TT5: Extended sub-templates and predefined IDs should be capturable as part of template libraries.

Figure 5.38: Task Governance Schema Requirements

In providing further context to **Figure 5.38**, the requirements are in view of process and project data being tightly inter-twined. The nature of TCs tasks and information-flows between them are also interlinked. As such, a type of inter-linked model is necessary that can represent these features, and also underpin the eventual opportunity of implementing networked atomic information-flows, and further automation benefits that may be derived. Finally, it is assumed these high-level requirements would be implemented via vendor-specific methods, whilst upholding core considerations defined within this Chapter. The following tables provides initial consideration.

Table 5.8: Schema Requirements (1)

Code	Task Schema Requirements	Details / Associated Requirements
T1	Task Construct: Tasks as a data construct should be able to represent the capture of atomic work responsibilities and information-flows between IDs.	
PP1	**P P1 - Information planning and requirement verification perspective**: Task constructs should represent and capture precise task information needs and responsibility.	Tasks from an information-planning perspective should represent detailing of: • Information needed to undertake a given unit of work (from who and why). Information required as outputs (to who, and why). • The capture of the who and why aspects should detail verification

		constraints (before information is received / output).
PP2	Task constructs allocated 'need to know' and 'need to share' components	These associated components should enable precise capture of a task's information-needs and information-responsibility in view of other tasks. • I.e., a given task's need to share component should be linked to the need-to-know components of one or many other tasks.
EP1	**EP1 - Information generation and exchange perspective**: A Task as an atomic unit of work should also be linked to actual data generated via its undertaking (by a TC).	**EP2**: Task's should also possess link to generated data as Information Input and Output components. • Generic process containers (templates) should also be linked to actual project-data generated.
	Relation **between Planning and Exchange**: Task need to know and share components should inform and build up to its information input and output components respectively.	• Task outputs, as inputs to another task become part of its access. • There is a forward-facing link between a task's planning

		components and its realisable exchange components.
AP1	**AP1 - Task Access Perspective**: The total access provided to a task should be determined via the input components of all active tasks they are currently assigned to.	- **AP2:** Receiver's access should be read-only reference to information provided. - **AP3:** Ownership should remain with originated user, unless otherwise delegated.

Table 5.9: Schema Requirements (2)

Code	Task Schema Requirements	Details / Associated Requirements
	Task Decomposability Perspective: Tasks should be aggregable and decomposable to task-sets and sub tasks.	Purposes of planning (i.e. structuring) and enabling atomic exchanges at an object and attribute level.
T2	A given task should be able to represent all cumulative aspects of a TCs information-responsibility.	A cumulative task is mapped to sub-tasks which reference all BIM data elements relevant to a (TCs) task's responsibility and thereby outputs (ST2).
ST	**Sub-Tasks**: Tasks should be able to be recursively nested as 'Sub-Tasks	**ST1**: A schema must represent how a cumulative task responsibility can be increasingly decomposed. • Tasks should be recursively nested against the cumulative task container.
ST2	Sub-task should be decomposable against BIM elements (referenced within the project's spatial map)	• Sub-tasks should also reference project's spatial 'map' to structure a cumulative responsibility against

	relevant to a cumulative task responsibility.	specific elements of work part of a task responsibility. - Mapping is determined by information-planning requirements and constraints of a task.
TS1	**Team-Level Task-Sets**: Task-sets should represent a team-level sub-processes, and collection of all tasks assigned to a given team's TCs.	- Task-Sets should provide for a 'higher-level' of collaboration between teams. - This may be for the managed delivery of information (i.e., deliverable templates).
TS2	Task-Sets should possess link to Team-Level Need to Know and Share Components.	- **TS3**: Team-Level access / outputs should be based upon all on-going tasks of TCs.

Table 5.10: Schema Requirements (3)

Code	Task Schema Requirements (Interdependencies)	Details / Associated Requirements
TID	**Task Interdependencies**: An ID as conceptual entity should represent connectivity between any two tasks of mutual relevancy in: planning and actualising exchange, and thereby access.	
TID-1 and TID-2	• **TID-1**: entities should represent a task's need to share component meets another task's need know component. • **TID-2**: ID entities should also represent a task's need to know is met by another tasks need share component.	
TID-3	ID entities should represent exchange can thereafter be bidirectional between tasks if tasks are mutually relevant.	ID entities should enable bidirectional (on-going) planning and exchange of information between interdependent tasks.
TID-4	ID entities should also characterise different 'states' between tasks of mutual relevancy.	• This should represent the lifetime status between tasks of mutual relevancy. • Includes capture of initial upstream / downstream states. • Different types of providing / receiving states should also be defined.

TID-5	A given Task should be able to possess multiple IDs to capture the interconnections with multiple tasks of relevancy.	• This is based upon all active adjoining tasks. An ID component should exist for any two tasks of mutual relevancy.

Table 5.11: Schema Requirements (4)

Code	Task Schema Requirements (Iterations)	Details / Associated Requirements
TI	*Task-Iterations*: Task Iteration: A task iteration should represent how a given task is iterated a multitude of times over its lifecycle.	Tasks should enable an implicit workflow control mechanism of information-outputs. • A task as an iterative process-container provide capacity to view a given task's inputs and outputs over time. • Also provides a building block for overlay of decisions made over responses.
TI-1	Each Iteration has a defined outcome, start / end point, and output.	
TL-2	Task Iterations should represent the gradual progression in output assurance and detail via progressive iterations.	• Iterations should be able to capture the intrinsic change-management from the perspective of the requirement itself, throughout its lifetime.
TI-3	Iterations should be able to capture progression with respect to interdependent tasks.	• Iterations should also capture (over lifetime of given task) how

		its requirement overlaps with multiple other interdependent requirements.
TI-4	Iterations should enable implicit information-flow network evolutionary-mechanisms.	- In addition to explored concepts, this includes the ability to change-manage the network in-part or as a whole.

Table 5.12: Schema Requirements (5)

Code	Task Schema Requirements (Templates)	Details / Associated Requirements
TT	Task-Templates: Task-templates should be implementable by TCs as a predefined *type of information-responsibilities* for professionals to undertake.	
TT-1	Task Templates capture pre-defined IDs between other types of templates.	• As tasks hold IDs, a template would capture pre-defined IDs between other task-templates.
TT-2	A template should comprise of transaction components which are generic inputs and outputs information-types.	TT-3: The generic input and output type would be based upon the templates disciplinary task typing.
TT-4:	Templates (and tasks by extension) should be implemented such that sub templates could be extended from parent templates with project-specific requirements (still linked to the core task-type).	
TT-5	Extended sub-templates and predefined IDs should be capturable as part of template libraries.	• Generic process-library which may be utilised for industry and project-level optimisations of (a) information-flows between actors and (b) the disciplinary-processes themselves.

6 Validation of Research Findings and Proposals

6.1 Introduction

This chapter will explore the feedback of experts invited to validate the research-findings and proposals. Rigorous validation and feedback were necessary as per the design-science methodology (Hevner et al., 2004). This was to ensure relevancy and accuracy of the conceptualisation of the problem-environment. It was also to ensure the alignment and applicability of the research-artefacts to advance secure-collaboration for the AEC sector, and provide other aligned benefits.

The participants include A1, A6, A8, A9, A11 who took part in the initial interviews. Their input was analysed within Chapter 4 and the identification of gaps also formed the requirements of the framework explored within Chapter 5. The validation sessions also included B2, B3 and B4 who were invited due to limited availability of other initial participants. These additional experts and their areas of experience are delineated within **Section 3.5.1** alongside the new coding applied to initial participants involved in validation. In brief, the participants A9, A11, A1, A6 and A8 are now coded as B1, B5, B6, B7 and B8 respectively.

Feedback was captured via two separate workshops which include B1 and B2, and B3 and B4 respectively. In addition, experts B5, B6, B7 and B8 were interviewed individually. These workshops / interviews ranged between 2 – 3 hours where findings of the problem-environment and the framework were portrayed via a presentation. The following **Sections 6.2** and **6.3** will further detail validation of the research-findings and the proposals of the framework respectively. The approach for validation is also detailed within each section.

6.2 Validation of Findings: Key Challenges to Secure Collaboration

The feedback of analysis and findings of the problem-environment will be explored in this section. The following were the core themes that were portrayed to and validated by the experts.

- **Socio-Organisational Themes**: These included non-collaborative, non-digital and security-incognisant sub-themes which were explored throughout **Section 4.3.** It comprised all overarching types of mindset and behavioural issues belonging to these themes, including key inferences that were discussed within **Section 4.3.4** of the influence of socio-organisational issues at the project-level.

- **Process and Technological Themes:** This aspect of validation summarised analyses from throughout the subsections of **Section 4.4 and pulled upon key issues to discuss** from the perspective cascading process-issues at project-setup (**Section 4.4.5.2**). In addition, 'enablers' and 'barriers' of the tensions were portrayed (**Section 4.4.5.3, 4.4.5.4**), and gaps for implementing secure and collaborative BIM (**Section 4.4.5.5**). This led to portraying a critique of the 'as-is' (**Section 4.5.3.1**), and high-level portrayal of the 'industry-needs' for better approaches (**Section 4.5.3.3**).

Issues were presented to participants, following which their feedback was captured. Validation criteria included the accurate and representative capture of these barriers, including those posed by current BIM approaches, which frame the needs of the framework. The following method was utilised for structuring feedback.

- **Verification**: An acceptance of portrayed issues. The factors must have been considered by the researcher and fall within the scope of the themes that were presented. This also includes *refinements* i.e. an overall acceptance of issues. However, slight refinements, or additional considerations of the presented theme may be provided.

- **Additional Issues**: Feedback that provides insight into novel issues, or slight additional slight nuances related to the original theme. These must be within the scope of themes initially captured or are related to them. It should also be noted refinements and additional issues overlap to an extent.

- **Exceptions:** Feedback provided by participants which provide a divergent point of view to an issue portrayed. This may also comprise feedback that causes reconsideration of the extent of, or dimensions of issues faced. This may also include invalidations i.e., feedback that negates the themes, ideas and issues proposed by the researcher.

This section thereby expands upon issues that were portrayed to experts, and additional nuances were captured as feedback in a complex and overlapping domain. Furthermore, no invalidations were encountered, as an overarching consensus was captured by all participants of the problem-environment. Rather, issues and exceptions were captured, both serving to refine the original understanding of the problem-environment.

As initially noted within **Section 3.2.1**, the evaluation approach was adopted from a joint academic and industry research alongside other research projects. The choice was also based upon an in-depth review of evaluative methods for conceptual artefacts in-line with recent interpretations of design-science research. It was utilised due to its applicability for analysing complex overlapping industry issues of the problem environment that do not possess easily quantified feedback. Also, based upon initial interview-analysis, it was noted participants perceptions of issues are subjective and linked to specific project-contexts. Accordingly, in-depth qualitative feedback was deemed necessary for the researcher to capture in-depth knowledge and feedback of the problem-environment. This would enable critical analyses to understand if the problems had been captured appropriately, and if a need was present for improved methods. This would thereby ensure the reliability and validity of the findings from the interview-analysis, whilst providing the groundwork for future design-iterations.

6.2.1 Validation and Feedback of Socio-Organisational Themes

This section of feedback analysis focuses on socio-organisational issues. The inter-relation with process and technological themes will be noted where appropriate. A key factor of feedback pertained to security-mindedness within industry broadly but were also contrasted with higher security-profile environments where relevant. The first section details feedback where security-mindedness is the central theme.

6.2.1.1 BIM and Security Compliance

In response to issues of limited client and supplier accountability (**Section 4.3.3.3** and **Section 4.3.3.4**), additional issues were identified. Firstly, all experts verified limited guidance of *holistic and integrated* security-minded BIM is sought from project-onset in the sector. Such approaches were a feature noted by B1 that the broader sector was still coming to grips with; B4 verified this approach must occur at the project-onset, or that it would be too late after a negligent lead-supplier has been chosen. They verified this issue especially pertinent within broader practice, where B6 verified limited client-prerogative to be linked to limited industry compliance mechanisms.

B6 also noted B6s sub-sector defined strict rules and regulations over secure IM. B6 did not necessarily perceive this within other general or even 'high-profile' projects that may implicate security-risk sensitivities. B3 and B4 however posed that compliance and knowledge overlapped in that it was necessary for project-sponsors to possess legal-responsibilities for security-minded management of their projects, in order to seek this guidance in the first instance. B1 and B7 verified this especially important for where safety-risks may be present to vulnerable asset-users.

6.2.1.2 Tensions in Definition of Proportionate Security

This section expands upon issues explored within **Sections 4.3.3.3** and **4.3.3.4** such as indifference and limited cognisance presented via board-level entities. These factors were verified by B4, B5, B7 and B8 as in the whole being appropriately captured. They did, however, exist additional issues, as further nuances of mindset issues that further consolidated and refined previous analysis. These additional nuances of mindset issues of board-level entities were captured via B5, B7 and B8. These include: (a) seeking security-guidance for solely compliance purposes i.e. a 'rubber-stamp' approach; (b) neglection of security-guidance when gained due to cost and bidding implications; and (c) averseness to reconcile proposed security-measures with other project-motives as part of balanced approaches. With respect to the latter issue, B8 perceived advice is not sought from a 'middle-ground' between project-efficiency and security-risk mitigation perspectives (See **Appendix B.8.1**).

Correspondingly, B8 suggested that the latter type of mindset issues also apply to security-professionals from the opposing spectrum where their focus appears constrained towards the 'absolute' mitigation of security-risk. This is as opposed to also understanding, and thereby reconciling, the implications of their proposed measures upon effective, quality and timely project-work. B8 verified this an especially problematic tension of security-minded projects; however, B8 noted it common amongst such professions in general. B8 also noted such security professions such as chief information security officers (CISO) are present within projects of the broader built-environment but are disconnected from influencing BIM-centric directives of design and construction.

Similarly, B7 validated that governance and risk-management for board-level initiatives is focused solely upon time, cost, and quality. This however needs to be reconciled with information and security-risk governance. B7 verified this would only occur if board-level entities, including AEC clients include inputs from such security-professionals. The overlapping factor between board-entities vs security-professionals appears to be that it is not part of eithers job-specs to consider the other's professional motives. B8 in-particular perceived it necessary to bring them into the 'wrestling-match' in balancing financial and security project-motives. Overall, the reconciliation between security-risks, along with other types of project-risks were captured as exceptions. It also requires information-security professionals to better convey the pragmatic underpinnings for appropriation of security-minded measures.

6.2.1.3 Security Incognisance within Online Environments.

This section expands upon additional issues uncovered from the portrayal of security-incognisance at the level of individuals (**Sections 4.3.3.1**). B1 posed an exception as to whether the implications of providing asset related information via online avenues had been considered. B1 posed an example pertaining to the digital publication over certain types of assets implicating vulnerable users, and correspondingly the ease with which such information can be accessed online (See Appendix B.1.1). B1 also posed such incognisance in the context of owners and operators not correlating (a) limited IS security / privacy throughout the asset-lifecycle to (b) safety-implications posed to vulnerable users. B1 noted assets such as schools, and their on-going operations as an example.

It is also linked to scenarios of online IS which are of little commercial, privacy or security-risk in most instances. This was however inferred indicative of additional nuances of security-incognisance, where individuals or organisations are unable, or do not care to discern what should not be communicated via increasingly available digital avenues. Similarly, B7 noted an additional issue where entities not involved during the design and construction phases, could disclose information on social media. This closely aligns to B7s perception of 'publicity activities' during the operations of a high-profile asset. B7 stated the following pertaining to a scenario where camera locations had been made publicly available, however the asset-operator had not been aware of the exposure (See Appendix B.7.1).

B7's refinements of security-incognisance overlap with issues of limited perceived improvements of security-centric competencies relative to digital competence improvements. B7 also perceived concerns over decisions made by digitally competent, but not security-minded individuals. Furthermore, it overlaps with both B7 and B8s validation on the need for a security-minded approach throughout the whole project-lifecycle where additional overlapping issues have been extracted to be discussed.

Discussion: Firstly, individuals not directly involved during project-phases may be provided decision-rights over the publication of built-asset information. This highlights a need for increased training and communication with operations workforce. Similarly, B8 perceived it fundamental for security-professionals to provide 'crystal-clear' guidance of (a) the level and degree of risk, (b) the threat-actors, (c) avenues they may employ, (d) 'why' it is important and (e) actionable mitigation rules.

In addition, operational activities may be carried out internally, or via external procurement. In the latter scenario, the owner / operator should still employ an appropriate selection process for sufficiently secure management of their assets. Finally, these factors were related to validated mindsets of oversharing captured via B1, B3, B5, B7 and B8. Additional sub-issues posed by B1 include over-detailed BIM models and renders as opposed to the minimum information required to answer a client's question or a partner's requirement. The following section will expand upon newly identified socio-organisational themes which posed a significant overlap between collaboration, digital and security-centric factors.

6.2.1.4 Evolving Digital and Security Maturity within Industry

This theme broadly expands upon many areas initially considered **within Section 4.3** and **4.4** of organisational digital and security mindsets and competence. Firstly, B1, B2, B3, B4 and B6 contrasted the broader built-environments previous cultural perceptions of digital-working with its current state, which was in-turn contrasted with other industries. B2 posed it necessary to further define routes for industry to 'play-catchup' in optimising IS / IM and proactive consideration of 'data as an asset to contribute towards' (See **Appendix B.2.1**). This additional issue applies particularly to SMEs of lesser secure and digital maturity within appointment-chains, both as part of security-minded environments or otherwise.

In response to portrayed issues of limited competencies, B1 suggested a refinement that industry is challenged on many fronts, which implicates both clients and suppliers. Additional issues were captured of guidance centric factors, and how this relates to inexperienced clients who may be 'one-off' parties. B1 noted further difficulty for such types of actors as they must *be able to* understand guidance documents available to them, whilst also inferring whether a security-minded approach is applicable to them. This in itself is difficult as many clients are not versed in digital construction, let alone digital security-minded construction.

Related to themes noted in **Section 4.4.1.2** of the need for baseline security-risk governance, B5 similarly noted that prospective clients may possess vague understanding of the security-risks, but not an in-depth appreciation. Where an initial awareness is however gained, they must also rely upon guidance from suppliers. B1 noted another issue in that whilst suppliers exist within the marketplace who attempt to provide their best advice, they are not impartial and have subjectively interpreted the BIM standards to suit their own practices, and requirements. Repeat clients within the sector are also still normalising themselves to simply digital BIM practices. B6 as a client however posed an exception in contrasting their current and previous maturity. The previously limited planning of IM and IS activities, including the detailed categorisation of information required at different stages had now improved due to their prerogative to document task templates, which provided them increased capability to identify what specific information is required and when. Correspondingly, B1, B2, B4 and B6 perceived relationships between (a) organisational maturity; (b) perceptions of ensuring secure and effective exchange and (c) the industries evolution as part of, and beyond Stage 2 BIM. B2 posed an additional factor to consider was whether blockers for secure and optimal exchange evolve, or function differently across organisations of varying degrees of maturity, and if so, how?

Personal organisational maturity is a refinement factor as it influences the levels of pertinence with which secure IM is perceived internally, and thus the competencies displayed externally on projects. B2 also perceived that improving organisational perceptions, and thus competencies towards IM requires taking organisations and their workforce 'on a journey' of aligning improved cultural-values towards digital-working. This overlaps with resolving misperceptions. For example, B1, B2, B5, B7 and B8 verified issues noted within **Sections 4.3.2.1 and 4.4.4.1** where many organisations view software-suites as an ultimate solution, without governance of defining clear requirements of the types of information / data to be managed and in what manner to ensure appropriate suitability **(Section 4.4.2)**.

Summary: The underlying impressions being that whilst behaviours and competencies have improved throughout industry, it appears pertinent to further define routes for how organisations of lesser maturity can be bought up to speed in effective digital and secure working. Overall, it appears the challenge is taking organisations, especially clients and SMEs, through a journey to effectively be able to ask for and deliver the correct information in a secure manner.

6.2.1.5 Need for Enhanced Workforce Competencies

This section validates and builds upon findings noted within **Sections 4.3.2.1** and **4.3.3.1** of limited professional competencies of digital and security-minded BIM collectively. Firstly, B1, B2 and B3 verified issues of limited workforce competencies for facilitating effective and secure IM and IS and associated industry-level motives to increase practitioner competences. A mirroring theme posed from an industry and organisational lens was explored within **Section 6.2.1.4.**

B2, B3 and B4 perceived limited workforce competencies are linked to limited intra-organisational emphasis of the need for effective and managed digital working. B1 concurred that as an industry in transition, professionals and suppliers must grasp many digital competencies, but also gain the security-competence to securely uphold such digital skills. This perception was captured as an additional issue, wherein B1 posed that the AEC industry needs 'to get up to speed' with numerous competencies required to evolve digitally. Having to also learn how to apply such competencies in a security-minded manner further pressures organisations (See Appendix B.1.2).

B1 and B2 posed another factor to consider is that the skills necessary for (a) secure digital-working and (b) BIM IM (individually or in combination) are not regularly acquired during education or employment as a disciplinary professional e.g. architect. Correspondingly, B1 perceived that IM as an activity was initially considered to be applied as part of default-roles according to Stage 2 BIM guidance (See Appendix B.1.3). In reality, B1 perceived IM activities and procedures were not straightforward. They entail a tailored appreciation and competence of IM values such that professionals are able to ensure information generated of their particular discipline is also managed effectively. B7 and B8 similarly perceived a need within the sector to simultaneously advance both security and digital competencies of professionals. ensuring that information is managed appropriately for downstream actors.

Summary: Experts perceived that competency-gaps must be addressed in furthering industry evolution. The factors discussed also pertain to effective adoption of security-minded BIM which requires an effective hierarchal response to information-requirements throughout appointment-chains. Enhanced workforce competencies are thus pertinent, as contractually obligated deliverables for managed and secure information rely upon the internal workforce competencies.

6.2.1.6 Implications of Negative Early BIM and Security Adoption

Linked to the themes explored within **Section 4.4.3.2** of insufficient supplier BIM plans, B4 and B5 perceived additional challenges in enabling present, positive change in furthering the industries BIM and security competencies. B4 presented that many promises were '*made and broken*' by early adopters of BIM (See Appendix B.4). This was specifically in the context of consultants guiding the implementation of BIM processes. B4's retrospect is that limited knowledge, competencies and in some cases, opportunistic negligence within the marketplace, have negatively shaded perceptions towards present change. Opportunistic negligence appears linked to the promised level of guidance to be provided by specialists at the inception of Stage 2 BIM approaches. A sub-theme raised is that it is left to the responsibility of organisations to fill in guidance gaps not provided by specialists. In B4's case, this was both BIM and security knowledge-gaps over the necessary protocols to apply within projects.

Discussion: The discussed factors validate supplier negligence in some instances. B7 expanded upon this perspective and validated the additional nuance of appointees who consider themselves competent, but do not possess meta-cognition over their competency-gaps. This was particularly of holistic security-competencies. In contrast, B1 perceived the industry to still be in a period of evolution, and that some leeway should be allowed for the marketplace to address and come to speed with gaps presented of the required competencies.

6.2.2 Validation and Feedback of Process and Technological Themes

Current methodologies were portrayed in how standards and BIM systems are implemented within projects for the planning, enabling and governance of information-flows amongst stakeholders. This section validates these factors of the 'as-is' and overlaps issues in implementing ecosystems appropriately and project-level tensions. Correspondingly, cascading project-issues based upon ineffectual security-risk governance are also noted. Finally, it should be noted that some factors that were explored within **Section 4.4** and **4.5** have already been implicitly covered during **Section 6.2.1**. Some of these for examples include issues of stakeholder competencies as part of implementing project ecosystems.

6.2.2.1 Burden of Implementing Security-Minded BIM

This theme broadly expands upon blockers in defining project-level security initiatives and associated tensions between security-minded and open collaborative practices. All participants verified these themes and posed additional refinements pertaining to commercial and administrative burdens in employing effective security-minded BIM approaches.

Firstly, B1, B2 and B4 contrasted such burdens to a perceived ease of sharing *all information i.e. oversharing* in response to client's expectations or contractual obligations. This may be due to an additional issue which B1 and B2 posed of stakeholders perceiving the need to protect themselves from claims of not sharing (from client or partners). This exception is thereby a reversed perspective of under-sharing and over-classification, due to mindsets of avoiding potential blame within security-critical environments. This additional blocker overlaps not upholding security-minded requirements; however, the expectations to provide everything may also be present within security-conscious environments. This inconsistency/paradox in project motives is thereby an additional cause for IS tensions.

Similarly, B1, B2, B5 and B6 perceived an additional blocker in that employing security-minded approaches requires an exceptional cumulative commitment from all involved appointment-chains. B1 noted a 'burden of administration' is present which appears to weigh down those involved in a project (See **Appendix B.1.4**). This also links to additional issues of the degree of commitment required from actors in such environments, such as the need to commit to psyops forms. B1, B5, B7 and B8 also perceived that the level of administrative overhead required is a difficult factor to reconcile with other project-motives. Similarly, B1 and B8 verified that sufficient security adds friction to project efficacy and commercial attractiveness to potential appointees. An associated verification is the 'perceived burden' of applying security-minded measures, which applies for both projects of elevated and baseline security-risk. B1, B2, B4, B7 and B8 posed the *perceived* burden alone can deter bidders when required to rigorously manage their appointment-chains, and thus believed bidders would opt for 'non-secure' projects.

B1, B2, B6, B7 and B8 however verified ideas that projects without security-requirements still present a 'degree' of security-implication which are not captured within EIRs (**Sections 4.3.3.2, 4.4.1.2** and **4.4.3.1**). As such, profit-incentivised and 'burden-averse' bidders may opt for such projects without recognition of actual security-risk present (**Section 4.4.3.2**). In relation, B1 posed an exception of *'Temporary Project-Works'* within security-critical environments, which are erroneously considered to be of lesser security-risk, B1 faced difficulty in conveying to stakeholders the need for the same level security-mindedness.

Summary: These factors discussed appear to be additional cultural nuances as barriers to normalising at least baseline security-mindedness within BIM marketplaces. They are also pertinent further issues invoking tensions within environments aiming to be security conscious. Correspondingly, additional types of issues and exceptions which B1, B4 and B8 perceived are overlaps between financial implications vs security-minded motives. This theme closely overlaps with the perceived burden of security-minded BIM and security-risk governance procedures.

6.2.2.2 Security-Risk Governance Feedback

All experts provided positive feedback of the portrayed state of security-risk governance as an appropriate reflection of issues faced. These factors were broadly discussed throughout **Sections 4.4** and the discussion as **Section 4.4.5**. They included: (a) limited client-led security-risk assessment at project-onset; (b) cascading issues stemming from limited security-risk governance and (c) project-level security and collaboration tensions from limited capture of integrated requirements.

It was verified by B5, B6, B7 and B7 that governance towards mitigating security-risk is oftentimes neglected within the broader sector. Experts also verified issues of limited holistic security-minded approaches which are also difficult to achieve in security-minded settings and aligns to burden of administration (**Section 6.2.2.1**). Additional issues and exceptions were also captured of security-risk governance which apply to security-minded projects, which possess governance focuses to different extents. B7 and B8 posed refinements in terms of policy-setting gaps for information-governance; they perceived motivators are upon business governance, which is typically focused upon assurance of time, cost and quality. This is as opposed to a focus on security and information governance. B8 verified information-security decisions are often treated as foreign by board-level entities, outside their domain.

Similarly, B6, B7 and B8 also validated safety implications of ineffectual security-governance are missed due to limited alignment between health and safety governance and security-risk governance approaches. Their implication to implementation of project ecosystems (**Sections 4.4.5.2**) were also verified by B5, B7 and B8 who subsequently verified the ideal security-risk assessment and mitigation approach must reconcile factors of different types of security-risks in view of different types of design, and project information broadly. They also posed factors of 'likelihood of risk-occurrence', 'level of consequence' if a given security-risk is actualised, alongside 'cascading security-risks' that may be mitigated by one or many mitigation activities;

these latter factors were caught as refinements of factors necessary to consider as part of ideal mitigation within projects.

B8 perceived that whilst security-risk is rarely governed, instances are often treated as high-level / binary assessments. This as opposed to *probabilistic* assessment of likelihood and perceived level of impact for any given actualisation of a security-risk. Probabilistic measurements should in turn be reconciled with other project-risks and motives. Reconciliation of motives includes balanced decision-making of motives such as time, cost and quality which implicates effective yet secure running of other ecosystem areas. B7 and B8 verified this requires initial assessment and likelihood of security-risk governance to reconcile with integrated requirements planning.

B5's viewpoints were similarly aligned, considering it necessary to clearly define what 'types' of asset-information *could* be considered to represent elevated security-risk, but also reconciling with potential threat avenues and likelihood. B5 provided an example of where the total asset-information a client considered sensitive to be small. B5 stated that this assessment, however, took more than 10 years to appropriately undertake, in order to understand what information required increased governance in their practices due to vulnerabilities, likelihood and consequence of impact. This also aligns to issues B1 and B6 posed with project stakeholders and their GRs facing unclear scenarios of the potential for data-aggregation and potential vulnerabilities it may open for threat actors to utilise. This was within the context B1 posed of inadvertently elevating security-risk by accumulating / bringing information together, which inadvertently elevates potentiality and likelihood of a given risk-scenario occurring.

Summary: Overall, experts verified cascading issues arising from ineffectual security-risk governance approaches. They also posed additional refinements and exceptions leading to identification of further factors required in achieving positive change of security governance approaches within industry. These factors are combined with findings in **Section 6.3.3.1** to represent future work.

6.2.2.3 Implications of Information Planning Issues on Project Risk

This section relates to additional issues of project-risks, which is interrelated with validation of information-planning issues (**Section 4.4.3**). Accordingly, experts posed project-risks are linked to inadequate project process planning pertaining to which stakeholders must undertake which activities and when. This also however aligns to gaps in information planning of their correspondent responsibilities for IM and IS activities. The implications as B1 perceived are 'process-gaps' in the form of missing information and stakeholder activities not being completed, when necessary. This turn results in schedule and cost overruns.

B2, B2 and B6 believed a significant additional challenge in lessening project-risk is limited acknowledgement of the connection between how ineffectual IM and IS activities elevates project-risk. B2, B4 and B7 in turn posed underlying mindsets and cultural issues are also relevant such as the prioritisation of immediate project-issues. Such factors inhibit timely detection of potential gaps which are identified too late, thus elevating project-risk.

In comparison, they perceived limited forward-planning of IM activities to decrease project-risk; B1 and B2 posed a discussion of excuses or misattributed causes for the actualisation of project-risks (**See Appendix B.9.1**). Correspondingly, B1 and B2 believed it key for organisations to learn from issues within their previous projects that impeded effective information-delivery. Instead, B1 B2, B4 and B7 perceived improvements made are small, gradual, and not a reflection of actual process-gaps present.

This is as opposed to pragmatic initiatives to find the underlying issues, such as critical reviews of the gaps (activity / information) within previous projects in order to enable improved future project-planning. B1 also provided an experience in attempting to develop a cost-plan, requiring information from numerous stakeholders (See **Appendix B.1.5**). Elevated project-risk was faced due to allowances made for missing information, despite B1 having identified and communicated interlocking and detailed responsibilities to the relevant stakeholders.

B1 believed this to represent that gaps still arise even when some stakeholders produce quality information-requirements. This is due to misattributed causes and inadequate collaborator competencies where requirements invoke their activities and information. B1 perceived little ability to influence gaps, and instead, time and cost allowances are made. Furthermore, B1, B2, B4 and B6 posed project-risk factors are linked to gaps of requirement-capture methods and contractual mechanisms. This is to both *capture* the cascading information-dependencies that implicate other appointees, and contractually assure exchange as and when necessary.

Discussion: Experts posed complex relationships between: (a) ineffective information-planning, (b) cascading process and information gaps, (c) cascading project-risks, (d) project-allowances and (e) utilisation of contingencies. The latter factors of allowances and contingencies appear to be the industries 'catch-all' mechanisms for managing uncertainty and project-risk. Current norms comprise the allocation of 'contingency-pots' in advance of the realisation of allowances, and associated project-risks. This is as opposed to equating the implications of ineffectual information-planning on the escalation of project-risk, and utilisation of contingencies. A sub-issue is that project-risks are perceived unavoidable, instead of addressing them by increasing investment in information-planning and undertaking process-reviews. Finally, the *specific* allowances that collective cost-contingencies are based on are not linked to specific missing tasks / information. **Section 6.3.5** discusses feedback that networked concepts could be extended to govern project-risk.

6.2.2.4 Implications of Industry Norms on Information Delivery

B1, B2, B4 and B7 expounded upon additional issues which implicate effective information-planning and also, alignment to contractual obligations. These issues were captured in response to gaps in effectively reconciling the need to know and the need to share. This overlapped with stakeholder dysconnectivity and associated causes of push-based paradigms. B3 noted that design-norms promoted by design-standards such as BSRIA further contribute to the one-sidedness of push-based paradigms (See Appendix B.3.1).

B2, B3 and B4 perceived scenarios linked to norms wherein clients are told what to receive based upon supplier's 'best-guess' estimations. These approximations are based upon knowledge from past-project experience and disciplinary guidance documents to determine what LOI and LOD is suitable to deliver at particular stages in view of different types of disciplinary assets / components. This industry norm is an extra dimension for planning and exchange issues. B2, B3, B4 and B6 perceived subjective approximations of design-guidance leads to ambiguity amongst stakeholders of what information is appropriate to exchange / deliver at certain stages. These 'best-guess' approaches may also not be explicitly mapped against project-specific requirements, in terms of the reasoning behind approximations or assumptions. This leads to difficulty in communicating *why* assumptions have been made in view of requirements to another stakeholder.

B1, B2, B6, B7 and B8 also verified issues of limited BIM and contractual alignment. Conversely, B4 perceived inaccurate approximations may adversely influence the perceived fairness of obligations amongst collaborators (where contractual alignment does occur). B4 linked these issues to concepts of the 'design-freeze' wherein certain stakeholders would stop exchanging information, whilst continuing to iterate their designs (See Appendix B.3.2). Including non-collaborative behaviours, B4 mapped the cause of 'design-freezes' to ambiguities of what / when information should be exchanged, which is in-turn linked to assumptions of the

LOI and LOD required to meet a client or partners requirements. These erroneous assumptions are in turn translated to obligations which can lead to discrepancies amongst collaborators as well as providing excuses for problematic partners to refer to if choosing not to exchange with others past the point of agreed-upon exchanges.

Discussion: Additional dimensions of information planning issues centre upon ‘best-guess’ approximations via static knowledge representations and assumptions based upon design-standards and previous project-experience. This feeds into erroneous and ambiguous requirement-setting. Such approximations may lead to collaborators receiving information non-specific in meeting their own client-facing deliverables. If in some instances, alignment does occur, disagreements may arise amongst stakeholders when assumptions are disproven in view of actual project-requirements. This may lead to project inefficiency as progression is halted for some stakeholders, as obligations have already been agreed. This overlap obligations not being updated. Finally, issues captured feed into proposals for optimised digital methods of work as proposed in **Chapter 4** and expanded upon in detailing validation of frameworks concepts.

6.2.2.5 Evolution of Industry Guidance and Implications for BIM Methods of Sharing

This section mainly concerns information-delivery paradigms and guidance of BIM standards, arising in response to gaps of atomic and evolving responsibilities for pull-based exchange. These gaps were portrayed in-part linked to standards. More broadly, feedback also verifies issues of information-requirement setting.

Firstly, B1, B2, B3 and B4 agreed with aforementioned key issues which were also discussed from another perspective of issues of industry design norms in the previous **Section 6.2.2.4**. This feedback relates to recent BIM ISO standards, and how they will promote more mindfulness over atomic exchange to be received by a given party, and therefore generated and shared by others. B1 contrasted the reception of previous PAS standards which had presented issues of ambiguity and lack of clarity to BIM adopters. Detailed intricacies over optimal delivery had not been communicated as effectively as possible, which the ISO in turn aimed to rectify. These issues pertain to the following factors of hierarchal information-planning.

- Requirements set to deliver information by clients and lead-appointees at an overarching level, without a view of:
  - The specific and granular information-responsibilities to be undertaken.
  - How requirements should be defined in relation to a specific activity of a specific task-team?
  - How different task-teams should coordinate work and exchanges to ultimately deliver the information the client requires?

B1 perceived that requirements defined without this granularity and interconnectedness may have implicated exchanges in them not being meaningful and supportive in answering specific questions. On the other hand, B1 perceived the ISO standards now provide further clarity over requirement-setting guidance initially defined by the PAS standards. The differences between the standards as B1 perceived were an increased focus on a question framing the specific information required to answer it. This is as opposed to questions posed, without a clear specification of what information is required, and who specifically is required to generate it. In addition, B1 posed crucially, the ISO guides tighter hierarchal governance over information-requirement setting and delivery mechanisms. The ISO promotes the increased rigorousness over granular and hierarchal delineation of requirements set via clients. These should be broken down by the appointee, in view-of their own appointees further down their appointment-chain. As part of upwards-acceptance, appointers at each chain should also review their appointee's deliverables, prior to eventual information-delivery to clients.

Discussion: Additional step-changes posed of BIM IM methodologies were thereby captured as exceptions. The ISO aims to alleviate issues by increasing granularity and hierarchal rigour. It also aims to address issues of limited effective hierarchal dialogue between appointer and appointee. This such that both parties agree upon appointee's needs to dispense their responsibility. This may however be complex where 'back-to-back' arrangements cascade within, and potentially across appointment-chains. The implications of feedback captured of the ISO standard feeds into the discussion of **Sections 6.2.2.5**, **6.2** as a whole and the feedback of the framework in **Section 6.3**.

6.2.2.6 Feedback of Gaps of BIM Governance and Management

This section validates BIM governance gaps, linked to process driven methods of information-planning and CDE architectures for exchange and access. These architectures were portrayed to reflect standards for structuring workflows against organisational-level responsibilities, which are met via federation of files, or object-level information-container mechanisms. Architectures were posed to underpin push-based exchanges of high information-volumes as factors implicating: (a) dysconnectivity, (b) unsuitable and unsecure exchange / access and (c) elevated sharing latency. File based IS without the technical capacity to set granular control implicates issues of securing sensitive information (**Section 4.5.2.4**).

Experts agreed with the portrayal of the predominant process and technological paradigms, but also posed refinements. B1, B2 and B4 posed vendors provide different functionalities for IM. For example, B1 supported recent mechanisms that aid the communication of knowledge about information-containers, but also in upholding the need-to-know principle. In other words, helping to name files and folders in such a manner to communicate the pragmatic detail required.

Similarly, B7 refined inattentiveness of file-naming could lead to oversharing, further refining 'high-detail' of sensitive factors may be 'low-volume' of data. B7 provided an example, whereby simply naming types of control-systems during procurement activities implied a significant degree of security-risk. B7 did, however, verify the implications of manually filtering large volumes information via file-based exchanges. Feedback of file-based issues in particular leads to exceptions via B8 of file-level vs object-level federation / access mechanisms.

B8 posed such mechanisms may alter the degree to which issues are faced in industry of limited IS specificity and security, elevated IS latency and dysconnectivity. B8 posed architectures possess the technical capability to address limited specificity and elevated latency via rulesets which combine object-level (a) federation, (b) access-control and (c) meta-data labelling. Actors can be updated to information reaching certain suitability-levels, given controls were applied. B8 however verified the following governance factors are not commonly identified in defining such CDE policy.

1. What meta-data labels should be applied to different folders and information-containers? This should be based upon information-categorisation of: (a) container-type e.g. spreadsheets, (b) information-content e.g. costing and (c) statuses e.g. 'work in progress'.
2. Correspondingly, the manual definition of 'patterns' (i.e. templates) which capture what types of roles (internal and external) should be able to visualise what types of information categories? This is assuming meta-data labelling occurs as part of the IM approach.

B1, B5, B6, B7 and B8 perceived whilst some vendors provide technical capability for fine-grained management, they are not normally utilised effectively. As such, B8 posed labelling and constraints of a CDEs directory structure, and data therein arises 'organically' with limited governance focuses. B7 and B8 also verified GRs possess limited knowledge to make decisions for internal / external actors. B8 posed an example of client CDE hostage, whose GR may not possess knowledge of inputs required of appointees and thus how to structure policy.

Correspondingly, B5, B6, B7 and B8 verified stakeholders do not anticipate knowledge-centric difficulties in governing actors need to know and need to share. They thus verified needs for effective mapping of 'knowledge', i.e., straightforward discoverability over: (a) who needs to / is doing what; (b) who oversees what; (c) who knows about what and (d) who to ask about what. Answers to such factors should feed into governance of 'who needs to know and share what?'.

B8 verified the need for knowledge-mapping and discoverability but posed exceptions in that architectures enable actors to discover meta-data such as filenames and request them (See Appendix B.8.2). B1, B7 and B8 posed that this also however requires governance to be formulated as to what 'sharers' perceive collaborators to require in informing labelling. As verified however, governance to this extent is rare.

Discussion: Overall, portrayals were verified by experts. B8 posed object federation mechanisms as potential solutions which was noted as an exception. B1, B4 and B5 however verified issues where stakeholders do not federate updates even where such mechanisms are present. In addition, collaborators still possess limited recognition of other stakeholder's actual needs/requirements until pushed. B1, B5 and B7 also believed causes for limited control over appropriate suitability, security and timing of exchanges are broader than configurations available via a particular vendor's IM tools. Their beliefs of broader causes in turn verified factors of ineffective information-planning.

Correspondingly a disconnect between standards for information-planning, and enabling systems architectures was verified. The gap perceived via the recent ISO standards is that complexity of atomic requirements captured whilst following the ISOs principles would be difficult to govern via current CDE architecture. Standards, and thereby architecture norms still predominantly appear to align to notions of federated information-containers (file / object-based). An issue however is that exchange (federated or otherwise) relies on the *assumption* that all policies will be appropriately identified and governed. However, this factor requires stakeholders to possess the prerogative to conceptualise these factors themselves; this of course requires client-led direction. Whilst possible, B8 noted it is very uncommon. Finally, it appears that feedback has further refined an understanding of the best available method of policy-setting as a non-ideal reflection the complex and inter-locking nature of atomic information IDs between actors. This feeds into the need for knowledge-mapping as an essential ingredient for information-governance.

6.2.3 Validation: Problem Environment Summary

Overall, positive validation was captured of the problem-environment and the core analyses captured during **Chapter 4** were verified thereby ensuring the key criteria for evaluation of the problem-environment. Key verifications include projects of different security-profiles facing varying types and degrees of cultural tensions between project-motives, which include but *are not limited to* security and collaborative sharing. Cultural complexity is heightened with the additional dimension that projects of elevated security-risk must employ integrated requirements. However, this principle is also important for the broader industry as any project possesses the potential for security-implications; the core difficulty faced however is in increasing holistic and integrated security-minded focuses.

An associated exception was the 'burden' of security-minded BIM. In a sense, the burden is also a verification of both socio-organisational and project-level tensions in implementing ecosystems. However, nuances were also captured of the 'perceived' burden as an additional barrier in the dispersal of baseline security-minded competencies within the marketplace. It was also verified that regulatory mechanisms are required for stakeholders in the broader sector to uphold obligations for security-minded IM. Other nuances were captured of previously identified issues of negligence on part of appointees / specialists. These may be impeding future beneficial change as part of an evolving built-environment aiming to be digital and security-minded simultaneously.

Other key feedback includes verifications of overarching security-risk governance issues in security-minded domains. Refinements were captured of an ideal security-risk governance approaches which is probabilistic and is reconciled with other project motives and risks. This is of pertinence of both baseline approaches and those applied for security-critical environments as part of a refined security-risk governance approach that reconciles the overlaps between other project motives (such as time, cost and quality) with a view of the *degree* of how burdens / tensions may manifest as part of a more informed approach.

Feedback was also captured of recent ISO guidance. The key analysis is that the proposed step-changes are gradual and refine the previous PAS standards. Interesting alignments were also captured of the ISOs pull-based shift in information-planning; this is however mainly from a hierarchical client perspective. It does not elucidate an optimal method for how professionals (assigned responsibilities), coordinate to generate information *across* appointments. This inference links to comparisons between the frameworks proposals and the ISO guidance are noted within **Section 6.3.3.2**. Furthermore, it appears workforce IM competencies are limited within industry at each progressive 'chain' to manage both requirements and generated information with a view both to their appointer and appointees. This aligns to the 'burden' required solely for effective IM, let alone in a security-minded manner.

Discussion of the standards also feeds into factors of BIM norms (**Section 6.2.2.6**), which grouped difficulties present in reconciling the need to know and share. Experts agreed with considerations for strategic realignment, based upon stakeholders possessing limited consideration for information-governance, which is in turn representative of broader cultural issues, alongside gaps of current BIM paradigms. Experts agreed with overarching consideration of alternative methods for governing planning and exchanges which may help alleviate knowledge-centric blockers of secure IS, but also open further opportunities such as networked governance of project-risk. Such factors which are representative of the overarching needs underpinning the framework's methods feed into feedback of the framework in **Section 6.3.**

6.3 Validation of Governance Framework and Concepts

6.3.1 Introduction and Validation Approach

This section details feedback of the framework which was discussed after validating joint-gaps of current BIM methodologies and implications upon governing BIM processes and information-flows (**Section 4.5**). Feedback of these key themes provoked the following overarching questions that were presented to participants.

- Are 'as-is' methods non-ideal in tackling the lack of specificity, suitability and security of BIM processes and information-flows?
- If so, do they consider proposals for strategic step-changes of BIM methods to be valid, plausible and feasible in aiming towards an ideal approach?

The propositions noted of the framework within **Chapter 5** entail change in methods of conceptualising processes, their enablement and governance via information-systems architecture. The framework was presented and conveyed via both conceptual diagrams, and discussion around the core requirements, principles and concepts of:

- Atomic pull and task-based planning, transactions and inter-connectivity (**Sections 5.2.2, 5.2.3, 5.3.3, 5.3.4**),
- Process and information governance, including information-flow, and security-risk / sensitivity governance (**Sections 5.2.3, 5.2.4. 5.3.3**),
- Task-template approaches and overlaps in sensitivity governance (**Sections 5.3.5, 5.3.5.3**),
- Network concepts, including interconnectivity and enablement concepts (**Sections 5.3.6**) alongside considerations for implementation drawing from throughout **Section 5.3 and 5.4.1**.

In detailing the feedback, it is necessary to group certain facets / proposals of the framework accordant to their principle, and the issue/s they aim to resolve. This is partly due to emergent themes overlapping multiple areas, and limited time within sessions to discuss each detailed concept as presented within **Chapter 5.** The overall build-up of concepts were however conveyed in representing the framework and its approach as a whole. This included the linkage of 'framework principles' to relevant problems which enabled the interrelation between the framework's principles, the relevant issues and the expert's own critique. This choice thereby enabled rigorous and in-depth and rich analyses of the proposals to understand if the framework is an appropriate, viable and effective response within relevant contexts.

With respect to the evaluation approach from **Section 3.2.1,** the methodology informs artefact design and evaluation considerations. Petter et al. (2010) posed the evaluation of artefacts at any point in their lifecycle deepens insights into the artefact, which are central to the capture of information about an artefact's implementation, benefits that may be present from application and the boundary-conditions i.e., exceptions in deployment of an artefact. In linking such considerations from methodology literature to the research context, it is noted the artefact is early in its potential life-cycle, and concepts whilst detailed still require further evolution. Evaluation should provide the necessary external feedback to evolve and iterate the framework, whilst proving viability before full deployment. Accordingly, a high-level evaluative categorical approach was devised to enable the efficient categorisation of feedback where the high-level categories incite consideration from participants and the researcher as to viability, and if its realisation would alleviate issues. The following meanings were attributed for evaluation.

- **Verification:** Feedback verifying suitability, applicability and viability of a given / grouping of concepts in (a) alleviating issues and providing improvements over current approaches, and (b) providing benefit of other project-motives not previously considered e.g. health and safety. This includes further opportunities present.

- **Issues:** Feedback provoking further consideration of the framework and its concepts. This includes refinement or clarification of concepts posed and ideas that were initially considered. Feedback falling in this category thereby comprises comments to consider alternative perspectives of: (a) the concepts themselves; (b) the problems they seek to address and (c) how they seek to address them.

- **Exceptions**: Feedback outside of the scope of the initial research and findings of the problem-environment that may be required to actualise the concepts. These are thereby challenges characterised by their applicability and relevancy to the research as themes or areas not initially considered but must be incorporated / overcome to deploy the framework to its optimal benefit.

Whilst verifications are a categorical choice devised to prove general viability, they also deepen understanding of approach applicability in security-minded environments. Issues and exceptions are however further challenges to implementation within the purview of themes considered that may pose as opportunities for future work. Exceptions are based upon the knowledge that boundary-conditions will exist that would otherwise impede deployment or its full potential. Ideally however, exceptions act as fuel to evolve the applicability and utility framework, by in-effect incorporating and thereby exceeding exceptions captured such as tailoring a solution in accordance to meeting regulations in a given practice for deployment of cloud-based technologies (e.g. A1 and A4). As with the validation criteria for **Section 6.2** however, feedback that invalidated the plausibility and validity of the approach were not encountered.

6.3.2 Feedback of Pull and Task Based Information Exchange Concepts

This section captures feedback of task-level information planning and enablement of atomic exchange, in a pull-based manner. These are core proponents of the framework in response to limited ability for actors to transact at an atomic scale, only what they need to know and share. It was also in response to governance issues of limited knowledge of a given organisations / other stakeholders needs and responsibilities. Feedback of governance changes in planning and enabling information-flows is detailed throughout **Section 6.3.3.**

There was overall agreement amongst B1, B2, B3, B4, B5 and B6 that the proposed approach of pull based information-flows would result in sound improvements of security and suitability. More specifically, they verified the philosophy of reconciling any task-level 'need to know' with other tasks 'need to share'. Similarly, they verified the proposed alignment of: (a) pull-based information-flows based on (b) atomic needs / responsibilities of ID professionals. Their agreement was linked to verification of intended benefits.

This was firstly in that B1, B2, B3, B4 and B6 in particular perceived sharing issues of limited specificity and security could be resolved by shifting the current emphasis of organisational-level sharing to the level of task-based requirements of professionals who require information to be able to provide value to the design. They also verified this approach captures information (a) generation; (b) sharing and (c) access as one fluid procedure. B2 appreciated such benefits simply for internal information-flows, believing it could alleviate limited atomicity and specificity of exchanges which also occurs internally. In B2's context this was linked to elevated project-complexity.

B1, B3, B6 and B7 also perceived that reversing the current push-based information-requirements approach to that of a pull-based approach would enable improved clarity and specificity of requirements. This should ensure information generated is explicitly linked to what is required based upon a professional's specific purposes to derive value. In relation to current IM standards, B1 also perceived that whilst ISO based information-delivery plans for organisational-level partnerships should be more granular, the information-planning method may still not provide a bidirectional understanding of what the 'information-demands' are, to and from other parties as individuals, teams, or organisations (See Appendix B.1.6). B1's statements were also inferred as the ISO not explicitly prescribing a pull-based definition of information-exchange and delivery amongst actors. This is such that actors explicitly know what to pull from others, based upon clearly communicated information-demands amongst parties.

Also focused upon the 'pull-based' shift, B6 proposed benefits from the perspective of an appointer in providing information (See Appendix B.6.1). Expanding on B6's statement, B6 noted clear alignment between the need to know and pull-based concepts of transaction querying. Moreover, it appears that B6 noted pulling and sharing based directly upon the other's need to know was an appropriate response to ensure security, whilst maintaining the normality of the design-processes. This, as B6 agreed with, shifted many standard ideas of information-flow directionality. B6 did note further refinement in that the portrayal of concept could further emphasise the need to know is the chronological factor that determines other interdependent actors need to share. Finally, B3 and B4 posed other benefits of pull-based specification of precise LOI and LOD *amongst* suppliers would decrease disputes where information is required by collaborators to in turn answer a client's questions (**Section 6.3.3.1**).

6.3.2.1 Feedback of Task Decomposability and Mapping

It was verified against B1, B2, B5, B6 and B7 that the approach to decompose tasks based against the built-assets spatial-hierarchy was conceptually sound for majority of projects. This was in the sense of projects where the decomposition of tasks is in essence mappable to a 'model-view' of the asset. Correspondingly, B1 posed the attribution of different types of views, or 'representations' of data e.g. view of simply IFC / COBie data should be mapped based against a template's type of task. This could in turn mean that different *representations* of subsets are devised, which are specific to the requesting professionals needs.

Feedback of this sub-concept was inferred as a further opportunity as a function of task queries / exchanges that future exploration of template libraries, and systems would implement. Another issue for further consideration is B2 and B7's feedback that it is necessary to explore how this concept should be applied to for projects with non-standard spatial-break down such as infrastructure. The response provided to these experts was that further research would also consider applicability of other related IFC concepts in creating bespoke subsets for exchange; it is inferred this would overlap with the task-template concept as future work.

6.3.2.2 Summary of Feedback for Pull and Task Planning and Exchange

Positive feedback was captured of core concepts of atomic pull-based information-flows. B1, B2, B3, B4 and B6 posed the methodological shift it entails would ensure security is instilled front and centre and not as an after-thought. Also, in the context of the framework's propositions as a whole, experts perceived the implementation of these core concepts would create a 'vehicle' to generate a security-minded approach at a project-level by upholding the principle of sharing *only* what is required for an individual to generate value enables a security-minded project and information-flows by default.

Experts perceived that the concepts can be applied on a project, irrespective of their security-profile to implement base-line security-minded projects. All experts agreed that implementing security-minded projects would not be seen as an 'extra add-on' to the project's overarching requirements and could simply become a standard approach. B1, B5 and B6 in particular perceived the proposed shifts in principles would enable 'secure-by-default' information-flows. B6's practices upheld this principle; however, experts perceived that this shift was not a norm.

Finally, B1, B3 and B6 verified this necessity for BIM step-changes which link to alignment issues of atomic information-planning within systems to guide definition, communication, and governance of information-responsibilities and information-demands. This is further discussed in **Section 6.3.7**. Overall, experts believed these fundamental framework concepts were appropriate responses to tensions between openness and security. The following section expands with feedback of governance over atomic pull-based information-flows.

6.3.3 Feedback of Process and Information Governance Approaches

This section captures feedback of overarching principles of process and information governance. A key concept is that GRs govern incoming and outgoing task queries via their governance-network overlay. TM responsibilities were under GRs to ease conveyance of governance concepts. These concepts are linked back to issues of limited ability / efficacy of; secure governing of information-flows, security-risk governance (including appropriate governance of sensitivity factors), and definition of access-policy.

Firstly, experts verified the need for in enabling future BIM processes whereby experts perceived the benefit of future GR roles as combination of digital, BIM and security competencies which for general practice. Moreover, B6 and B7 also verified the need for GRs (i.e. human intervention) was crucial where queries may implicate sensitivities. GRs would be provided a starting point for decision-making such as in B6s practices. B6 also verified the additional layer of security-risk governance via GRs would aid their already security-minded practices, but also perceived a positive in providing by-default governance approach (suitability and security) for broader industry practice. B6 also perceived the concept of a GR as a default standard in possessing overlapping BIM and security competencies would be key to making pragmatic decisions.

This feedback also overlaps current issues. B1, B6, B7 and B8 verified of GRs possessing limited knowledge to make pragmatic decisions. B3 and B4 posed an exception in that competencies for security-minded IM that GRs must possess may (a) not be common-place and (b) may present a high-degree of accountability in view of potential mismanagement. This relates to a gap noted in **Section 6.2.1.2** of the 'side-lining' of security-professionals; however, this may also be because of disjointedness of security and BIM knowledge, and thereby competence within practice. It also relates to a need for evolving workforce competencies to instil baseline digital BIM security-competencies throughout industry **(Section 6.2.1.5)**.

In a similar vein, B3 posed a new outlook on the role of BIM technologies based upon the framework to alleviate potential knowledge gaps for GRs. B3 percieved the potential to aid human decision-making via the implementation of system-architecture with strong usability characteristics, automating different functions and providing more advanced interfaces than presently offered. Automated functions are also verifications that progressive responses could be semi-automated, but with further consideration in providing for streamlined governance. These factors are captured as additional systems-centric requirements.

Finally, B7 initially posed an exception that malicious actors could pull information; this exception was later rectified as a verification whereby B7 understood and agreed with the specificity principle of task-assignment in line with competencies, and professionals only receiving information as characterised against their need. B1 and B7 did however suggest refinements for 'audit-logs' against what information actors have been provided throughout their involvement in a network, and also capturing the decisions made by GRs. B1 posed such knowledge could simply be kept as meta-records against an instance of a task, throughout its lifetime.

6.3.3.1 Process and Information Governance of Sensitivity

This section further validates proposed methods in governing sensitive exchanges. This included the combination of constraints of: (a) clearances, (b) competencies and (c) a task's need to know. The approach combines these constraints with additional governance over queries so GRs can choose which professionals' sensitive information would be released to. This is whilst maintaining obscurity of sensitivity itself to requesting TCs. The general appropriateness of this approach was verified by experts. B6 indicated that it would be essential for GRs to govern the sensitivity classification and responses. B1, B2 and B6 also verified nuances the framework concepts represent in terms of a task not possessing sensitivity itself, and that sensitivity is only *determined* once the information-output of a task is provided actual project-specific context.

They also verified the proposals of a network providing evolving context over security-risk. This links to further opportunities. B1 posed concepts of templates and networks would be beneficial for GRs in enabling targeted identification of specifically what information is required and thus targeted allocation of clearances. B1 considered this important given time and costs in individuals gaining clearance. B1 and B2 discussed a security-centric opportunity templates may provide, concluding that continuous implementation and iteration of a task-template approach would enable contextual identification of when information becomes sensitive (See **Appendix B.9.2**).

In view of to the discussion, B1 and B2 believed this possible as templates present novel opportunities to capture *at what point* the outputs of tasks (extended via templates) are given project-specific context which make it sensitive. I.e., LOI and LOD reaching a degree that outputs provide a real-life representation of the sensitive aspects (to be installed / constructed), and thereby identifying at 'what point in time' does is information given context to represent real vulnerabilities (See **Appendix B.1.7**).

B1 and B2 thereby perceived templates would provide opportunities in planning *what, why, when and to who* information *became* sensitive, and thus at what point security-clearances *will* become required. B1 and B2 further posed templates, and a network could be used to trace when information associated with the task's outputs *became* sensitive and *why*.

This security-risk knowledge-capture in essence enables the pre-informing of clearance governance-decisions. B6 agreed with this idea but posed an exception as B6s internal practices possessed guidance of what types of asset-information present vulnerabilities. B6 however stated their guidance was rare and reflects compliance with regulation. As such, B6 verified opportunities for future work would be beneficial for other security-minded domains which may not possess clearly defined guidance or the broader industry which possesses limited cognisance of security-risks.

6.3.3.2 Feedback of Industry Guidance Relations to Framework

This section captures feedback relating to the ISO guidance. It overlaps with the governance-network and hierarchal governance for GRs. It also analyses B1 and B7's interpretations of the framework proposals. This is in their perceptions that professionals required to generate information would be able to *ensure* the specific information needed to dispense their responsibility is in turn delivered via other professionals (internally and externally). This was in turn a verification of a key idea. i.e. a direct atomic approach at the professional level enables, by extension, organisational entities to better coordinate work and information to ensure all parties can deliver their responsibilities. They believed the proposed approach to be slightly different from the ISOs hierarchal and client-centric perspective but verified it is ultimately in view of the same end-goal of secure and effective delivery to clients. They also raised exceptions whereby the framework's perspectives of information-planning of (a) TCs required to generate information amongst themselves (such that their and other collaborators can deliver their responsibility) should also be reconciled with (b) the ISOs client driven, hierarchal perspective of information-planning (**Section 6.2.2.3**).

B1 also perceived that networks offered opportunities to aid clients in understanding what specific information feeds into meeting a given question from across many project domains, and their interlocking implications. B7 similarly posed that all task-level requirements within a network should be in explicit view of hierarchal information-delivery to the client. B7 noted this as a client-centric 'super-process' where any task within the network ultimately feeds into answering a client question. Correspondingly, B7 posed that if a client's GR were to change a requirement, or to raise new questions, such changes should be percolated throughout the network to ensure all actors are working amongst each other with an updated view of what the client requires. This exception provides ideas for future-work in implementation of task-level exchange, and of hierarchal information-governance for the purposes of suitability.

6.3.3.3 Process and Information Governance Feedback Summary

In respect to the governance needs and concepts, all experts provided positive applicability of the approach. This was both for security-minded and broader domains. Opportunities were captured overlapping information-governance (by GRs), templates, and networks. These are factors for future work.

Overall, experts verified the proposal of information-planning at an atomic level provides (a) actors in need of information tangible recognition of the responsibilities of ID actors but also (b) ensures that GRs possess an explicit link to make an informed decision when requests are made (internally / externally). The overlap between templates, information-governance and network concepts via B1 and B2's feedback also presents new opportunities for informing sensitivity / clearance decisions. This would likely be achieved via governance of task-iterations, and the associated progression of LOI and LOD. These are thus further ideas that would enhance governance-networks.

Feedback in **Section 6.3.3.2** of a client super-process is an exception as it was not fully considered. The idea suggested embodies a perspective that actors should only undertake work providing value to clients. Clients GRs should be able to govern this via a super-process over the governance-network in directing higher-level change of requirements, and appropriate percolation to appointees and their professionals. Conversely, the framework's portrayed aim of information-governance was to ensure GRs possess visibility and security of internal / appointees. The general pull-based atomic concepts also ensure professionals receive the information they require such that the organisation can dispense their responsibility. The combination of the framework and client super-process perspectives however appears an ideal governance approach for both security and suitability. It also poses further opportunities to be discussed in **Section 7.2.**

6.3.4 Feedback of Task Template Concept

Templates carry over the intended atomic pull and task-based benefits and intended problem resolutions denoted within **Section 6.3.2**. Another purpose is to ease complexities in capturing IDs in task-level work by professionals, extending project-specific tasks from a template library. This concept was thus aligned to resolving and automating atomic discoverability (of relevant information, actors and processes) and reducing dialogue in identifying real-life IDs. Templated approaches were met with positive feedback by all experts. B1, B2 and B6 posed opportunities whereby many organisations already template their information-flows and associated design-processes. B6 and B2 posed their practices captured project-knowledge for the repeatable nature of atomic design tasks, with view of particular assets / components and IDs.

Abstracted generic templates were extracted via this knowledge in B2's practices. B6 undertook a similar approach which enabled them to capture both data from previous projects and the IDs between the templates. Abstracted and generic task-level work / information-flows was applicable for re-use and expansion across different projects.

Furthermore, B1, B2, B6 and B7 verified that whilst design and information-flows were largely similar i.e. non-variable, certain aspects were variable. This was a sub-principle that the template concept was built upon. This was in turn linked to the verified nature of task-level design remaining relatively formulaic across different projects. B2 considered the non-variable factors were the type of asset / component itself e.g. line-rail and types of information that are relevant to their design (e.g. line-speed). The variable, or project-specific factors however were the project-specific data-attributes i.e. the contextual 'slot' values of transaction-components themselves. These are defined in response to project-specific design requirements / constraints.

B2 and B6 validated additional situations templates may help alleviate. Firstly, whilst some digitally mature organisations may template ID task-level processes, it is not necessarily a feature of standards. Similarly, B2 suggested template capture was limited to their internal disciplines. Other external disciplines thus possessed an assumption of what information was required based upon previous project-practices (See Appendix B.2.2). These 'best-guess 'assumptions may be proved false, and information is not delivered as needed; this as B2 percieved is a symptom of not explicitly defining where the IDs lie, and what information is required to and from them.

It was also identified that non-project specific assumptions are made of what information is actually required. I.e. approximate, yet not fully project-specific responsibilities defined via static disciplinary guidance (**Section 6.2.2.4**). It is inferred templates would ensure professionals must 'show their working' when assumptions are made in view of not yet finalised project-specific requirements. The 'reasoning' behind assumptions would thus be explicitly communicated with other stakeholders. Finally, B7 further posed that task-level templates could be aggregated into 'deliverable' templates for delivery purposes. This aligns to the concept of team-level task-sets. B3 and B4 perceived automation opportunities such that systems implementing the approach make the extension process trivial. This overlaps with UI and usability considerations to provide users an effective manner to capture, extend and communicate requirements and thereby knowledge.

6.3.4.1 Feedback on Scope of the 'Task' and Task Template Libraries

This sub-theme relates to the frameworks intended, BIM centric scope, and captures feedback relating to broader project-activities. Firstly, all participants perceived that the conceptualisation of task-level requirements is appropriate for design-centric domains. They also verified relevancy for information-types relatable to built-assets in general, and other types e.g. infrastructure.

Firstly, B1 and B2 posed exceptions in that a tighter definition of concepts is required to better communicate the intended level of 'granularity' and 'types' of work-units to broader cross-sections of the AEC domain with differing nomenclature. B2 suggested to refine the initial terminology of 'root design process' to 'root discipline process' to convey templates would capture other disciplines relevant to the broader project information-model which may not be design-centric and occur in different stages. Similarly, B1 posed an exception of the need to link task-based concepts to PLQs in view of how clients pull atomic responses from professionals across a wider range of different project-activities than design (See Appendix B.1.8).

B1 and B7 also perceived tasks outputs, and networks as a whole, could also be seen as a response to meet client PLQs. They posed numerous activity types, from throughout the project occur to answer questions. Correspondingly, B1 posed such activities should also be mapped as part of the identification of real-life atomic tasks that are pertinent to answering the clients' bigger questions. B1, B2 and B8 thus supported future work to define archetypal templates and IDs for other project activities. They agreed a need to develop 'personas' of typical processes and information-flow for different disciplines and tasks throughout industry. B1 advised to reference RIBA stage activities to gain initial insight for future exploration in defining templates at industry level.

6.3.4.2 Task Template Feedback Summary

Experts verified principles of templates and their applicability in increasing connectivity, discoverability, and knowledge re-use. Different organisations already template their processes and associated information-flows. For example, B2 and B6's practices. Whilst similar, their approaches were different such as general methods to capture them, intended atomicity of their process-mapping, and differences in terminology. Correspondingly, B1, B2, B6 and B7 posed a common representation for atomic processes, requirements and IDs does not appear to exist.

Experts agreed templated approaches should be further explored at an industry-level in providing a 'common-language' for ID task-level requirements. They perceived standardisation was necessary for efficient communication that organisations are 'talking about processes in the same way' and by extension, information-planning requirements. Similarly, experts agreed current process-mapping methods for interoperability are difficult for general practitioners to utilise. This appears a significant factor for system implementation wherein machine-readable templates should follow a common schema that is representative of project-knowledge captured at overlapping internal, partnering and industry levels. Experts also posed such an initiative would be beneficial simply for standardisation of BIM processes. B6 stated opportunities linked to need to refine frameworks concepts in view of future work (See Appendix B.6.2).

6.3.5 Feedback of Network Concepts

This section mainly captures feedback of the general 'process-network' concept. Networked benefits posed include increased capacity in understanding what actors need to know and share in view of evolving BIM processes. It would also provide an overlay for GRs in governing atomic transactions for security and suitability motives; the governance-network functions specific to GRs were discussed within **Section 6.3.3**.

Firstly, B1, B2, B3, B4, B5, B6 and B7 verified overarching proposals in that the conceptualisation of atomic BIM information-flows as a network was an appropriate representation of complex inter-locking task-level processes within and between organisations. B1 and B2 further verified this perspective is not normally captured as information-planning focus are mainly between organisations (**Section 6.2.2.3**).

Accordingly, B1, B2, B3, B4, B5, B6 and B7 verified propositions for networks would alleviate difficulty in conceptualising processes at an atomic scale and capturing complex overlaps between requirements. This is as opposed to current methods e.g. information-delivery tables. B1 and B2 both agreed this often leads to an incomplete picture and further posed the evolutionary nature of networks would conclusively capture 'hidden' IDs between atomic actors (unknown from their perspective) and would thereby be fundamental to underpin benefits of atomic BIM processes. B1 stated: "*I think it's quite interesting because we talk about... an information-delivery-plan as though it can and will miraculously occur - and in a way what you're talking about is an* ***information-demand matrix*** *in order to enable that information delivery.*"

In this sense, B1 likened the bidirectional task-structure would ensure the capture of 'information-demands' upon other stakeholders and their professionals. This is in meeting any given requesters own responsibilities. As such B1 and B2 likened this concept to serve as an ‘information-demand matrix’. B2 further perceived a network to be the data-centric equivalent of an requirements-gathering workshop for information-planning (see Appendix B.2.3). With respect to B2’s statement, each party proposing a need, in essence invokes a cascading ‘discovery-process’ of which *other* parties are responsible for meeting said need. A network upholds this idea of identifying interlocking responsibilities both at appointment / assignment of an actor, which can thereafter be revisited and updated at any point. This is due to digital requirements captured as part of an interlocking and evolving network.

B6 and B7 perceived strong improvements in security and other areas such as health and safety could be gained via a network of evolving task-level requirements. This is from the client perspective of possessing comprehensive, evolving visibility over project-work as noted in **Section 6.3.3.2**. Finally, B4 posed the step-change of pull-based exchange underpinned by networks would provide benefits over latency of transactions, and increased optimisation of work. B1 also noted exceptions that such benefits pose complex re-consideration of industry norms to be reconciled as part of future-work.

6.3.5.1 Feedback of Networked Governance of Cascade Effects

This section expands upon feedback of capturing and govern the cascading implications of change in any given actors need to know and share. Firstly, B1 agreed implementing the optimal degree of atomicity via ISO guidance would require step-changes in governing complexity of initially capturing atomic inter-connected tasks, and the cascade effect of actors evolving needs and responsibilities. Similarly, B3, B4 and B6 agreed a network as intended would possess 'knowledge' of how tasks interlink and evolve. Likewise, B3 provided a construction-centric example of the underlying complexity of AEC processes, and correspondingly, the benefits of a network's 'absolute' and 'live' understanding of all IDs, and cascading implications throughout different stages (See Appendix B.3.3).

B3's example highlights human-level understanding of the implications of change at an attribute-level between only two actors and their tasks is limited. For example, changes in the plasterer's tasks implicate the painters' task and the updated information to be communicated by a managing party. If any factors change at an attribute-level, a butterfly effect occurs amongst professionals' tasks. This is over specific data attributes in the aforementioned examples. It is also of factors at a task, sub-task, or attribute level, still during design or ready for installation in this perspective. Moreover, B3 and B4 posed the cascade at an atomic level is often not identified. Correspondingly, if atomic IDs in task-level work are not identified, then the knowledge of implications of change does not exist in order to be communicated. B1 and B2 similarly agreed such factors are not captured which also implicate limited visibility of cascading design-change. In response to these considerations, B1, B2, B3, B4, B6 and B7 thus perceived the inter-connected nature of networked tasks would enable 'evolving understanding' of the cascading implications of actors need to know / share. B6 further posed a network would also be beneficial from a health and safety perspective would be able to capture such cascading implications.

Finally, whilst B7 provided an agreement in principle, an issue was also posed for future work whereby B7 posed it essential that mechanisms are in place to ensure TCs do not prematurely provide an update that cascades without effective management that may otherwise present commercial risks (See **Appendix B.7.2**). In other words, it being inferred TCs, and their TMs / GRs would require buffer-mechanisms to 'test the waters' of *how* their updated outputs cascades to affect others interdependent actors, and the broader project information-model, before green-lighting outputs. It is inferred this idea overlaps with the notion described in **Section 6.3.3.3**.

6.3.5.2 Multi-Directionality of Networks

This section expands upon **Section 6.3.5.1** from B1 and B2's perceptions that networks would provide actors a detailed multi-directional perspective of information they and other actors have published to the network. This theme overlaps with historical perspectives to understand change in a network leading up to a task's final state for the purposes of evolving templates (**Section 6.3.5.3**) and networked governance of project-risk (**Section 6.3.5.4**).

B1 and B2 posed networked information-flows would be beneficial from the perspective of an 'information-originator' to be aware of how their information has been utilised by other actors. This is within the context of new outputs having increased suitability. B1 considered other benefits a network should be able to underpin (See **Appendix B.1.9**).

With respect to B1's statement, B2 suggested benefits for originators to (a) possess awareness of reliance of outputs, to understand which actors require updates. An understanding of the indirect reliance is also necessary. In other words, even originators are unaware of cascading IDs and who / where information generated by them may have been indirectly relied upon. B6 verified a network should be able to capture these indirect IDs via the interconnectedness of networks, both procedurally, and spatially.

Taking B1's example into a pull-based context, requesters (direct or indirect) must understand what (a) the information outputted from a task was previously, and (b) whether it can still be relied upon; this overlaps with B2's perspective in that a network would provide the assurance capabilities to understand what new updated inputs are required and the historical context of inputs received. The latter factor feeds into informed decisions over design information-needs / requests and overlaps with a project life-cycle perspective for operations and maintenance stages. This could where the originators may no longer be active, but their delivered information-products will be relied upon by actors active in later stages.

For example, an actor assigned a task to retrofit specific components of a **MEP** system must be able to view the final output of the design-task. They must also thus possess a '*historical view*' of all tasks within the lifetime of a network that may have influenced the final output. This would be for the motive that actors can make present informed decisions on replacement components that do not clash with other task-level requirements, presently active or historic. Abstracting however, this would simply mean adding new / updated information with an informed view of what unintended consequences may be present, and thus being able to avoid them.

6.3.5.3 Evolution of Task Typologies

An additional concept B1 and B2 posed was of perceiving the evolving 'nomenclature / taxonomy' of templates. In essence, B2 posed project-specific tasks, and their associated outputs would change over time in line with how actor's ID tasks in the network overlap. In respect of these considerations, B2 provided the following statement (See Appendix B.2.4).

Expanding upon B2's statement, it was inferred it would be beneficial for GRs or TMs to possess an 'audit-trail' in the sense of B2's verifications that a network could capture tasks and the IDs between different task, but also from the points of (a) the point any given task is instantiated; (b) the point of the first information-transaction and (c) the point of the final information-transaction. The final being when the task is closed out i.e. a task is no longer providing information to counterpart TCs and their tasks.

This audit-trail would overlap with the network's in-built potential for change-management of the iterative transactions between IDs. It also overlaps with the governance audit-trail. Moreover, it appears B2 perceived an opportunity in being able to track a task's evolving scope between the aforementioned points in response to change would be beneficial for historical understanding of *what* decisions were made in deciding the final nature of a task and *why*.

B2 noted this for project-knowledge reuse purposes in the sense of an evolving taxonomy of how a given instance of a task could be historically tracked in understand evolution of a task. It also appears this specific historical perspective posed by B2 is also a further opportunity with being able to feedback into template-libraries.

6.3.5.4 Networked Governance of Project Risk

This additional opportunity arose via issues of information-needs not being met. **Section 4.5.3** proposed this creates a cascade effect and adversely implicates dependent actors in undertaking their own work. A network was posed to however provide cascading inter-connectivity and discoverability amongst inter-connected TCs and also aid validation whether actors have met responsibilities of ID tasks.

B1 and B4 verified a networked approach could capture cascading identification of which actors are required to provide missing / incomplete information. They also perceived opportunities in identifying 'who' is liable for project-risk. These perceived opportunities were linked to issues of assumptions being made for missing information. This is where tasks are incomplete e.g. ground-reports not undertaken, and an output is missing. The assumption itself and reasoning behind it is also not tracked throughout the process. Dependent stakeholders thereby must proceed at risk without information.

B1 and B4 verified benefit in templates possessing the potential to capture the 'demands' for what information is required via templates (from and to who). This feeds into a network concept aiding understanding at which point / task, placeholders (of assumed information) have been assigned. As such, all downstream task's utilising assumptions could be tracked via a network. It was posed this would be an opportunity to alleviate project-risk. This as when real-life project data is captured against incomplete tasks, all downstream tasks utilising assumptions can be notified to feed into informed decisions of where tasks may need to be updated.

B4 indicated that assumptions may be made because of a given actor's (e.g. sponsor) prerogative to not procure the necessary service to produce information. In this sense, it would be possible to assign project-risk according to liable entities. B4 also posed stakeholders could historically trace through the network to understand *where* process and information-gaps arose. This includes the cascading chain of incomplete tasks or information throughout the network. Correspondingly, B3 and B4 saw significant opportunities of utilising networks and machine-learning to learn from issues arising via previous project in thereby saving on costs for project-stakeholders, particularly the client.

6.3.5.5 Network Concept Feedback Summary

Overall, this section verified the intended benefits. also posed their own considerations and potential benefits that may be realised via networked approach that are applicable to other contexts such as the governance of project-risk. Whilst the intention was for simply the security and suitability, it appears many further benefits in other areas that require further exploration. This of course requires that such a networked task-structure exists in the first place but provides strong indication in working towards actualising the concept. The feedback captured provides indication the novelty of the concept is untapped.

From the opposing perspective of exceptions, B1 and B5 posed that as the network concept, and the frameworks implementation as whole posed such complex reconsideration, there would also be a need for future work to measure the benefit of proposed methods vs the as-is. Experts similarly noted that future work simply should capture worked examples of networked approaches. Despite challenges, B1, B2, B3 and B4 however verified the need for improved methods, and the associated benefits that could be gained. Perspectives demonstrated this section of feedback will be fed through to considerations of future requirements in **Section 7.2**.

6.3.6 Feedback of Contractual Implications

Experts raised questioned as to how the alignment of contractual methods would need to occur in view of frameworks proposed method of delivery, and how the approach could be contractually implemented on real projects. These questions assumed a system would uphold principles of atomic transactions, where crucial sub-factors include evolving atomic responsibilities, and outputs directly in response to another actor's requirement (i.e., a task's needs are met by another tasks responsibility). Based upon exceptions, it appears these principles require sufficiently aligned contractual mechanisms for deployment of methods as they implicate factors of contractual methodologies and organisational-level arrangements. The following subtitles will detail feedback from related perspectives.

6.3.6.1 Feedback of Implementing Atomic Contractual Information Deliverables

This section pertains to contractual implementation of atomic information-delivery. This concept arose due to issues of high-level responsibilities influencing tensions in effectively validating 'what is delivered?' vs 'what was actually required?'. Furthermore, there is limited alignment of BIM requirements to contractual obligations; both are barriers in ensuring optimal, cost-effective and secure delivery.

The framework however poses focus of exchange shift downwards to professionals and their task-level requirements. B1, B5, B6 and B7 agreed such an atomic shift contrasts with current contractual norms based mainly in view of organisational responsibilities. Correspondingly, an exception was captured of contractual complexities in implementing the framework on projects.

Conversely however, B1, B2, B3, B4 and B7 noted opportunities whether task-level responsibilities could act as the basis for defining more meaningful, specific and auditable obligations amongst stakeholders. This was also linked to feedback that specific PLQs of clients are based in view of many different task-level requirements (**Section 6.3.4.1**).

B3 and B4 perceived such atomic transactions could be facilitated by distributed ledger technologies. This comprised opportunities that principles of atomic exchange occurring in response to specific requirement / requirements could be translated into micro-contracts. They believed this would lead to significant benefit from financial, cost, and legal perspectives. B4 also posed the auditability of each transaction would lead to reduction in disputes due to nil ambiguity whether a transaction occurred and met other stakeholders' requirements. Furthermore, it is inferred that evolving requirements throughout networks could be trackable in their propagation to the relevant professional; this could in turn be amended to micro-contracts.

Summary: This section has provided initial considerations of how the feature of an atomic deliverable is implementable from a project perspective. This overlaps to an extent with system-level implementations but is distinct. The key requirement in deploying distributed ledger technologies for the built environment is to ensure their suitability. This as B7 posed, requires far more future in-depth consideration in ensuring alignment to the built environment's specific needs. This was respect to such technologies as a whole.

6.3.6.2 Implementation of Atomic Interlocking Contractual Arrangements

This section expands upon feedback of atomic deliverables within the context of appointees possessing limited recognition of obligations that implicate other organisations and their professionals within and across appointment-chains. In providing context, within the 'as-is' of current contractual paradigms appointers and appointees should *ideally* agree at appointment: (a) where these interlocking responsibilities will be present and (b) for appointers to procure information required by appointees. This should continue throughout the project-process in ensuring effective hierarchal information-delivery back to the appointer, and eventually the client.

B1, B2, B3 and B6 considered that such manner of obligations is not a standard feature of arrangements between appointer and appointee. In reality, the underlying detail of as aforementioned interlocking responsibilities are sometimes unknown at appointment and are not resolved until the last minute. This adversely affects appointees in getting information needed to deliver their own responsibilities. B2 also noted bidirectional responsibilities may also not be captured internally which leads to issues receiving information.

The framework's concepts propose that atomic bidirectional responsibilities are identified at an atomic scale between organisations but based on their professional's atomic information-flows. This is how their atomic needs / responsibilities overlap other organisations within and across appointment-chains. In view of these principles, B1 and B2 considered both opportunities and exceptions of contractual setting methods between appointments. B1 noted*: I'm also wondering... if the framework … as a 'Way of Working', would suit itself more to an 'Integrated Project Insurance' type-project than any other any 'Traditional Insured Project'…*

They considered benefits from upholding this principle of bidirectionality if an appropriate contractual methodology were implemented. The benefits overlap with B2's notion of a 'requirements-workshop' perspective of a network **(Section 6.3.5)** and is based upon agreements that change is required of how arrangements are set and governed. This is to ensure appointee's seamless exchange / access for the information that they need to deliver; this also provides the benefit that appointee's professionals are only pulling information required to do their tasks. Correspondingly, B7 perceived benefit from the appointer perspective in receiving the specific information needed to answer their questions, and thereby reducing project waste.

Discussion: Issues of information-delivery between appointments were considered as contractual barriers in ensuring actors receive the information they need to deliver and involves complex re-consideration of contractual arrangements between appointments. This is an additional nuance of an evolving problem-environment (**Section 6.2.2.5**) but also documented here as an exception as it overlaps proposed methods. This is not only in identifying cascading responsibilities between organisations (in view of their professionals), but also in ensuring these factors are amended to contracts between appointer and appointee. In other words, whilst verified in **Sections 6.3.5** that networks possess the potential to identify and *govern* atomic bidirectional responsibilities, this does not necessarily mean they *will be* appended as part of contractual responsibilities. In response to B7s consideration, this could be a potential use-case of distributed-ledger-technologies, as it would underpin contractual-governance alongside proposed information-planning and enablement.

6.3.6.3 Contractual and Procurement Methods for Implementation of Framework

This section will consider preliminary factors of procurement models that ensure the frameworks notion of bidirectionality is upheld within the *current* contractual paradigms. It will also explore future benefits and problems as side-effects that could arise via alterations in the degree of personal project risk faced by stakeholders. Firstly, B1, B2 and B6 posed exceptions via questions pertaining to current contract and procurement forms, and which would be best suited for implementation of the framework from the perspective of a 'method of working'. This is of principles of atomic bidirectionality between overlapping professionals feeding into the organisational level. Correspondingly, B1, B2, B4 and B7 posed opportunities whereby future work should consider how principles could be align-able to current models such as IPD, Traditional, D and B etc, or whether bespoke forms would be required.

This itself is in view of a combined opportunity and exception where proposed methods may potentially alter the level of personal project-risk any given stakeholder would encounter. This is based upon a verification of networks in governing cascading change whereby a network would provide inferences of cascading responsibilities, in turn detailing a more accurate picture of atomic responsibilities between organisations. Accordingly, B1, B2, B3 and B4 believed stakeholders may update the scope of their responsibilities in view of the updating network. This is such that appointees' professionals are provided information so the organisational entity can deliver its responsibility. This would occur throughout the process with the ultimate aim of project success, as opposed to individual organisational benefit.

On the other hand, evolving responsibilities may not reflect the original contractual signing, and thus what stakeholders assumed their personal risk to be. In other words, project-risk would be altered from the perspective of any given organisational-stakeholder. Alterations in the degree of personal project-risk after initial singing could lead to tensions between proposals and current mechanisms. This is in view of issues within industry such as: static contracts not updated based on evolving scope of work for (a) organisations and (b) information they actually deliver. This is either to the appointer or other appointees. Related issues comprise stakeholders refusing to share beyond certain points during project-stages.

In simultaneously applying the consideration of evolving personal risk to the question of procurement models, it appears necessary to enable shared project-risk amongst stakeholders. This was in the sense B1 posed IPD would be suitable to uphold bidirectional and evolving principles of work (See **Appendix B.1.10**); this was in response to B2s contractual considerations. As noted of A1's perceptions, IPD would be suitable because the project itself is insured, and stakeholders possess equal incentive in resolving project-work. In this sense, B1 indicated that 'lines (between organisational-level responsibilities) can afford to be blurred'. Other methods such as 'traditional with design' were also suggested; it is inferred however that whilst a network could inform actors of atomic overlaps, an appropriate contractual mechanism is still required to contractually enforce these factors. Conversely, B1 and B2 considered if project-risk is shared equally within traditional line structures, then appetite for methods of exchanges could be increased. This is perhaps more important to alleviate the *perception* of increased personal risk due to this manner of evolving responsibilities. This is in that project risk may be a fairer, and more distributed reflection of work amongst stakeholders.

6.3.6.4 Contractual Feedback Summary

It should be noted detailed contractual perspectives were not initially envisaged as feedback of the framework. Regardless, the research has aimed to accommodate feedback. Most notably, experts perceived as implanting the framework as 'method of work' in and of itself. This was an exception as the complexities in this regard were not fully appreciated by the researcher. Conversely, via analysis, opportunities are linked as are considerations for future contractual-centric work to tie into the framework's propositions. These are noted within **Sections 7.2**.

6.3.7 Information Systems Implementation of Framework

System implementation opportunities and challenges were captured via feedback throughout **Section 6.3** implicitly. Many areas having been discussed throughout validation implicitly such as governance feedback. As such, this section collates remaining factors. Overall, many of the areas were provided with positive feedback, and experts considered technical challenges and opportunities for implementation in view of usage on real projects. These challenges also considered deviations required of CDEs in implementing pull-based transactions, templated approaches, and networked information-flows. This also overlapped themes pertaining to data-hostage paradigms; blockchain technologies and automation opportunities.

Firstly, experts verified bidirectional task-level requirements, whereby access is met by ID tasks need to share requires step-changes of CDE architectures. B5 for example perceived such an approach is not upheld by system-vendors currently and the benefit in both latency, speed and security of subset exchanges would represent. B5 further verified the limitation at present for CDEs is that an accepted methodology does not exist to appropriately link process to data at an atomic scale for security and suitability perspectives.

Similarly, B1, B2, B3 and B4 raised considerations of data-hostage methods, contrasting centralised vs linked-data repositories. The latter where each organisation holds their own data-storage which is logically federated with other party's data-storage. It was agreed with experts that networked approaches could benefit from alignment to linked-data architectures which enable separation of: (a) the physical storage of data with real-life context to (b) the network as directionality of task-level transactions between professionals. In other words, linked data approaches could enable actors to understand the nature of the tasks and the flow of information between TCs, without needing to see the real project data.

Experts perceived this a benefit of both security and discoverability as context of real project-information transmitted via task-level flows does not need to be communicated. Instead, flows between professionals could be publicly published to networks. Another factor discussed with regards to implementation (via linked data-architecture), was the network as the process-map holding links to disparate 'cloud' datasets stored on separate physical sites. Accordingly, the process-maps of organisational stakeholders could be combined and stored on a 'demilitarised-zone'. I.e. a network infrastructure outside a given organisations scope. This could be used to route the flow of real project-data. B2 posed APIs could be used in conjunction with process-maps to route transactions. B2 also suggested system-vendors could potentially offer a service for 'demilitarized' storage of all stakeholders' data-stores. This would be a single governing cloud hosting the individual cloud data-storage of all project-stakeholders. This single cloud would route queries and response to the data-storage of appropriate organisational entities.

Alternatively, proposals may enable offerings of data-subset 'streaming' by vendors. This aligns to B3, B4 and B5's perceptions that filtered data subsets (in response to pull queries) would result in a decrease in data-transfer. This is as opposed to B4's experiences of collaborators sharing large files to update small percentages of information. B4 perceived that the majority of information shared was redundant, leading to inefficiencies in their practices for professionals to find relevant information. B3 also posed subset querying would be computationally simpler, and thereby 'cheaper' for data-hosting resource utilisation. Finally, B3 and B4 also posed considerations of how to automate many of the intended functions for information-planning and governance. They aligned templates to automation opportunities for usability characteristics, wherein systems should automate the bulk of actors defining / extending templates. This should ensure fluid definition of tasks from the perspective of the actor and overlaps discoverability requirements of previous project-knowledge within libraries.

6.4 Discussion of Framework Feedback

The research findings were validated via experts to ensure relevancy to a complex problem-environment. Validation occurred of both enablers and barriers to secure collaboration within industry from perspective of socio-organisational and project-implementation considerations. The associated recommendations for these factors will be noted in **Section 7.1** as considerations of recommendations for industry. A sub-theme of these recommendations being they are socio-organisational driven.

The governance framework was itself an example of an approach and validated within **Sections 6.3**. Overall, experts provided positive feedback of both, and the relevancy of the work was validated wherein experts related gaps presented of current methods to benefits of proposed divergent approaches. This cements the link to the 'as-is' in detailing conceptual solutions, which were contextualised as appropriate 'to-be' responses within the problem-environment of the AEC industry. This is as either existent security-minded practices or less security-competent practice in industry, which possess degrees of security-implications. Rather, experts perceived the cross-relevancy in the frameworks potential in moving the industry as a whole forward in achieving a base-line degree of security.

As such, the framework was also understood within the context of feedback by participants of its broader reaching nature of proposals at an industry level. Some of these factors however were not initially considered and caught as 'exceptions', I.e. the capture of the broader nature of challenges required such as contractual mechanisms to effectively implement the frameworks method of work. Issues were also captured as factors that should be considered in taking the work further. This joint design-science and industry-inspired feedback method has provided detailed analysis and categorisation of future work required to implement the inherent secure digital **BIM** methodology proposed alongside other opportunities captured such as improvements that could be derived in the governance of project-risk. This includes experts also provided overarching positive feedback of the potential that the framework represents from the system perspective. They also posed opportunities of the framework in setting the scene to explore future work via a proof-of-concept implementation of the approach.

In consideration of these factors, **Chapter 7** will inter-relate issues and exceptions as a high-level consideration of future potential work / research based upon analysis of framework feedback. The following section will however provide a further design-cycle iteration based upon the key contractual exceptions.

6.4.1 Framework Iteration to Address Contractual Exceptions

This section provides an overarching update to the framework's requirements based upon key exceptions captured. The aspects of the framework to update are in response to the contractual exceptions that were noted in **Section 6.3.6** to overcome in embedding the atomic IS methodology the framework prescribes. The updated requirements address the need for an appropriate and aligned contractual paradigm to underpin atomic actors in sharing across boundaries without contractual blockages that may arise due to emergent interdependencies between atomic responsibilities that cross organisations / appointment-chains. **Figure 6.1** provides an update to requirements initially denoted in **Sections 5.2.1, 5.2.3 and 5.2.4.**

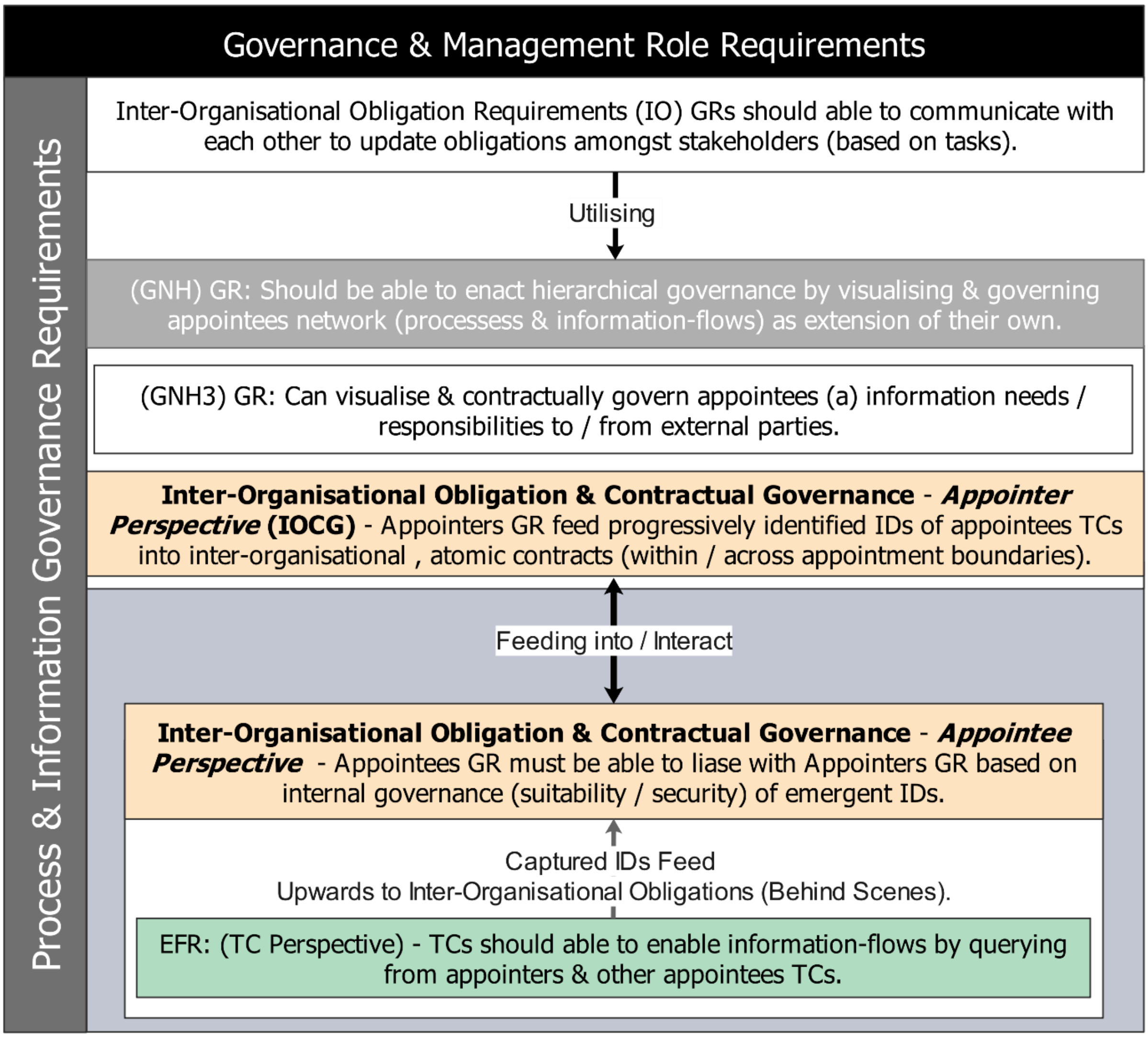

Governance & Management Role Requirements
Process & Information Governance Requirements
Inter-Organisational Obligation Requirements (IO) GRs should able to communicate with each other to update obligations amongst stakeholders (based on tasks).
Utilising
(GNH) GR: Should be able to enact hierarchical governance by visualising & governing appointees network (processess & information-flows) as extension of their own.
(GNH3) GR: Can visualise & contractually govern appointees (a) information needs / responsibilities to / from external parties.
Inter-Organisational Obligation & Contractual Governance - Appointer Perspective (IOCG) - Appointers GR feed progressively identified IDs of appointees TCs into inter-organisational , atomic contracts (within / across appointment boundaries).
Feeding into / Interact
Inter-Organisational Obligation & Contractual Governance - Appointee Perspective - Appointees GR must be able to liase with Appointers GR based on internal governance (suitability / security) of emergent IDs.
Captured IDs Feed
Upwards to Inter-Organisational Obligations (Behind Scenes).
EFR: (TC Perspective) - TCs should able to enable information-flows by querying from appointers & other appointees TCs.

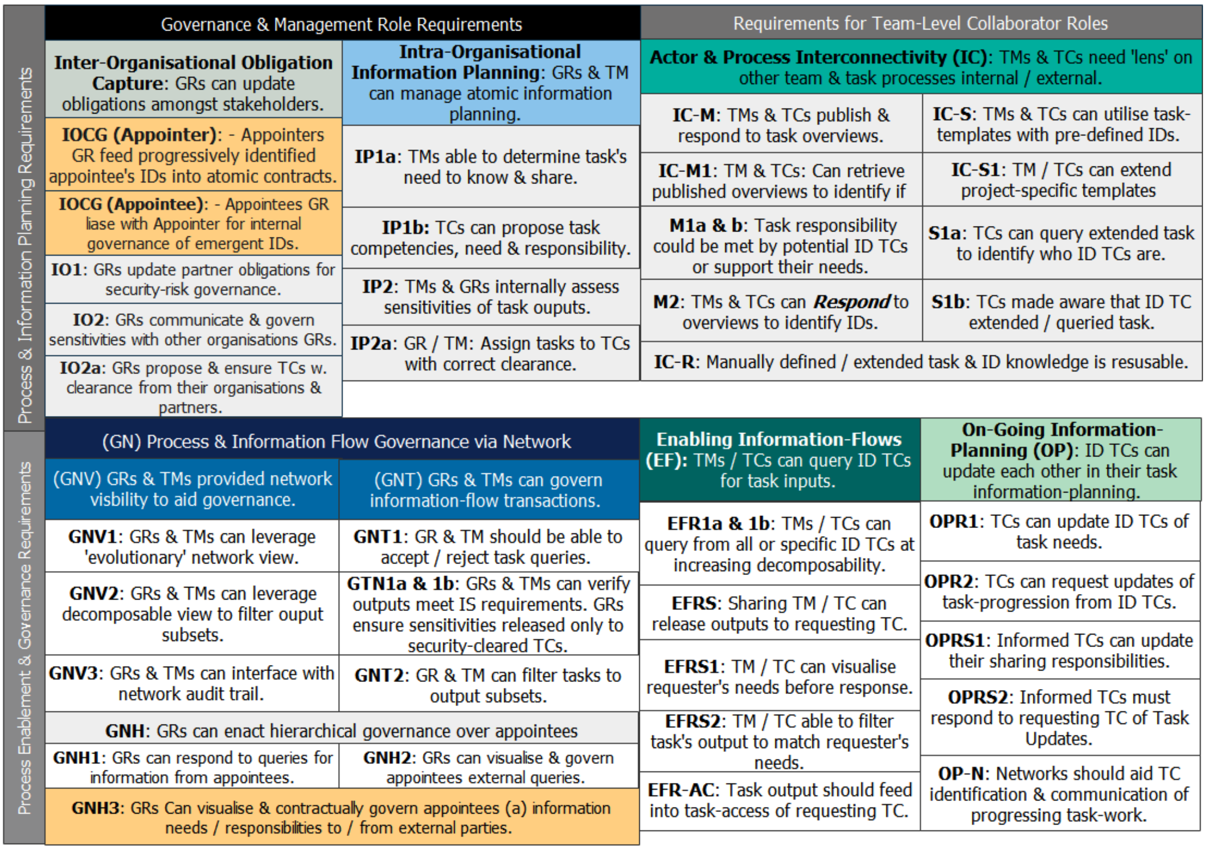
Figure 6.1: Framework Update (Detailed)

Firstly, it is noted with respect to **Figure 6.1** that only the relevant concepts from the aforementioned framework sections are utilised. In **Figure 6.1**, the overarching **IO requirement** '*to update task-level obligations amongst stakeholders*', should now utilise the hierarchal governance requirements that networked capabilities enable (GNH). They should be able to be made aware of changing information-needs at the appointee-level in view of their TCs **(GNH3)** for the purposes of inter-organisational obligation and **contractual** governance **(IOCG)**.

Both IOCG and GNH3 are new requirements that should support atomic contractual governance. The former is based upon a consideration that is split between *appointer* and *appointee* GR perspectives in overall view that TCs can query / respond to atomic transactions. However, any emerging contractual implications of atomic work should feed upwards to the relevant GR, who must in-turn liaise with their *own* appointers / client GR in manging an atomic contract. This should align to the atomic information-requirements and scope of a given task-interdependency. Contractual implications should also be hidden from the relevant TCs, and requirements of this actor-type should not change. GNH3 is also defined in-view of the need to contractually govern interdependencies and is an extension of hierarchal governance features.

The technical method by which both the IOCG and GNH3 requirements are enabled seems to be best facilitated by distributed-ledger-technologies as noted initially in **Section 6.3.6** and would be closely tied to hierarchal networked governance capacities. However, as also noted, what may be more pertinent is the need for an appropriate and aligned contractual framework to underpin potential enabling technologies. In addition, the competencies for GRs to be able effectively and appropriately govern atomic contracts will need to evolve in tandem.

Summary: A design-cycle update is completed based upon the exceptions that feed into key new requirements of the framework. Accordingly, the following **Figure 6.2** abstracts the key new requirements **IOCG** (Appointer / Appointee Perspectives) and **GNH3** are appended to the revised framework diagram, in their relevant sub-section. These are highlighted in the framework in orange.



Process & Information Planning Requirements

Governance & Management Role Requirements

Inter-Organisational Obligation Capture: GRs can update obligations amongst stakeholders.

IOCG (Appointer): - Appointers GR feed progressively identified appointee's IDs into atomic contracts.

IOCG (Appointee): - Appointees GR liase with Appointer for internal governance of emergent IDs.

IO1: GRs update partner obligations for security-risk governance.

IO2: GRs communicate & govern sensitivities with other organisations GRs.

IO2a: GRs propose & ensure TCs w. clearance from their organisations & partners.

Intra-Organisational Information Planning: GRs & TM can manage atomic information planning.

IP1a: TMs able to determine task's need to know & share.

IP1b: TCs can propose task competencies, need & responsibility.

IP2: TMs & GRs internally assess sensitivities of task ouputs.

IP2a: GR / TM: Assign tasks to TCs with correct clearance.

Requirements for Team-Level Collaborator Roles

Actor & Process Interconnectivity (IC): TMs & TCs need 'lens' on other team & task processes internal / external.

IC-M: TMs & TCs publish & respond to task overviews.	**IC-S**: TMs & TCs can utilise task-templates with pre-defined IDs.
IC-M1: TM & TCs: Can retrieve published overviews to identify if	**IC-S1**: TM / TCs can extend project-specific templates
M1a & b: Task responsibility could be met by potential ID TCs or support their needs.	**S1a**: TCs can query extended task to identify who ID TCs are.
M2: TMs & TCs can ***Respond*** to overviews to identify IDs.	**S1b**: TCs made aware that ID TC extended / queried task.

IC-R: Manually defined / extended task & ID knowledge is resusable.

Process Enablement & Governance Requirements

(GN) Process & Information Flow Governance via Network

(GNV) GRs & TMs provided network visbility to aid governance.	(GNT) GRs & TMs can govern information-flow transactions.
GNV1: GRs & TMs can leverage 'evolutionary' network view.	**GNT1**: GR & TM should be able to accept / reject task queries.
GNV2: GRs & TMs can leverage decomposable view to filter ouput subsets.	**GTN1a & 1b**: GRs & TMs can verify outputs meet IS requirements. GRs ensure sensitivities released only to security-cleared TCs.
GNV3: GRs & TMs can interface with network audit trail.	**GNT2**: GR & TM can filter tasks to output subsets.

GNH: GRs can enact hierarchical governance over appointees

GNH1: GRs can respond to queries for information from appointees.	**GNH2**: GRs can visualise & govern appointees external queries.

GNH3: GRs Can visualise & contractually govern appointees (a) information needs / responsibilities to / from external parties.

Enabling Information-Flows (EF): TMs / TCs can query ID TCs for task inputs.	**On-Going Information-Planning (OP)**: ID TCs can update each other in their task information-planning.
EFR1a & 1b: TMs / TCs can query from all or specific ID TCs at increasing decomposability.	**OPR1**: TCs can update ID TCs of task needs.
EFRS: Sharing TM / TC can release outputs to requesting TC.	**OPR2**: TCs can request updates of task-progression from ID TCs.
EFRS1: TM / TC can visualise requester's needs before response.	**OPRS1**: Informed TCs can update their sharing responsibilities.
EFRS2: TM / TC able to filter task's output to match requester's needs.	**OPRS2**: Informed TCs must respond to requesting TC of Task Updates.
EFR-AC: Task output should feed into task-access of requesting TC.	**OP-N**: Networks should aid TC identification & communication of progressing task-work.

Figure 6.2: Framework Update

7 Future Work

The purpose of this chapter is to briefly explore opportunities for future work and overviews the broader industry recommendations necessary to progress secure-digitisation maturity, and the challenges that are associated in deploying the framework.

7.1 Broader Industry Recommendations

Firstly, an overarching recommendation is to address socio-organisational and project-implementation barriers. This entails the overarching recommendation for the broader dispersal of baseline security-minded approaches within industry, where initiatives must account for concerns of a broader cross-section of different types of AEC stakeholders. Collective initiatives are also pertinent in distributing security-competence knowledge throughout industry in this regard. Industry-level initiatives are characterised as the following sub initiatives.

Security-Risk and Collaboration Contexts: Security-risk governance approaches should improve both projects of elevated security-risk and application of baseline security-mindedness. On the whole however, it appears industry requires BIM methods which ensure a degree of security-mindedness as a default when implementing project ecosystems. This overlaps the frameworks potential.

- Future initiatives should explore avenues whereby the secure-collaboration concerns of a broader outlook of different types of projects and stakeholders, throughout different stages can be upheld. This includes capturing stakeholder's concerns in interacting with other types of stakeholders and may also overlap with contractual approaches. Initiatives should further explore the overlap between holistic security-risk governance approaches, which can be reconciled with other project motives.

- In some CNI sectors (e.g. nuclear), guidance is already present of what asset-information presents potential for security-risks in deriving classifications. Such guidance is missing for the AEC industry, as are mirroring *incentives* and *repercussions* for not applying sufficient governance. This relates to the categorisation of many types of security-risks (resilience, commercial, IP, privacy, health and safety), within different types of projects, stakeholders, and asset-types, throughout different stages. This also includes specific types of asset-information that present generalisable types of vulnerabilities, and which should be governed more appropriately.

- Currently, clients must rely mainly upon specialists in effectively triaging applicable security-risks. As verified, negligence, limited competencies and non-impartial guidance are issues in the marketplace that adversely influence appointee selection, and thereby inappropriate implementation of project ecosystems. There exists a gap of an industry-level knowledge resource to guide prospective clients with significantly more clarity of the types of security-risks they may encounter, and thereby routes to avoid them.

- Security-risk templates (explored within **Section 7.2**) represent an overlapping area of future work. They would represent the culmination of a knowledge resource as a 'starting-point' for clients / asset-owners to understand applicable security-risks. This aligns to the need to provide a clear direction to stakeholders of measures to apply in implementing integrated, effective and sufficiently secure ecosystems in line with security-risk appetite and holistic reconciliation of project-motives. Knowledge is also currently constrained to limited specialists which may be leveraged in deriving such templates.

Integrated Project Requirements: At a project-level, improvements are required in how stakeholders, particularly clients, define requirements which integrate all stakeholders needs. A further prerequisite for integrated requirement-setting is effective assessment and integration of security-risk governance. Integrated requirements should limit project-level tensions associated with the inappropriate implementation of project ecosystems.

- This core recommendations of improved security-risk governance procedures also applies to projects of lower *potential* security-risk which feature limited adoption of baseline security-measures. This is to ensure as comprehensive as possible visibility of security-risk and assurance that appropriate mitigation has been applied.

Mindsets, Behaviours and Competencies: Further industry initiatives and research should aim to improve upon issues of limited competencies and cognisance amongst both internal and organisational actors. This includes factors pertaining to training of organisations.

- Senior-roles are the bridge between collaborators and the diffusion of internal competencies. As such, change must be driven at this level of the organisational hierarchy. This focus applies for both presently security-minded domains, and those within broader industry.

- Similarly, there is a need for governing-roles from an operational perspective (such as CISOs) to possess holistic skillsets. They must be able to convey at a project / internal board level, the need for integrated project-requirements which comprise the holistic governance of security-risk, effectively reconciled with other project-risks and motives.

- In addition, industry requires further upskilling of baseline professionals' competencies with regard to security and digital competencies. This is regardless of the type of AEC disciplinary education and may in turn comprise university educational programmes devised with such factors as part of BIM related modules.

Educational Pieces: The necessary educational pieces must be defined to guide inexperienced clients and senior-level roles in implementing projects in a secure and collaborative manner. Educational pieces should also be defined to guide prospective supplier organisations. These should be ‘dummy-proof’, straightforward guidance pieces towards implementing baseline security-initiatives.

Socio-technical Improvements: It was also identified that many socio-technical issues are in-part due to limitations of current technologies. Improvements are necessary in terms of how vendors interface with their customers (i.e. AEC organisations and professionals) with the aim to capture in more depth, how solutions can be provided to improve usability to deter unsecure behaviours, but also incentivise the usage of technologies within securely implemented digital-environments.

Contractual Development: This research has explored concerns such as ownership of security-risk and accountability in the event of risk realisation. Contractual concerns must be further explored for the built-environment. Initiatives at this level must be multi-fold in the following:

- Identifying what are appropriate contractual responsibilities and liabilities of all stakeholders. Legal factors should consider events of data misuse, exposure (from privacy, commercial or security-risk perspective). Indemnities should also be considered to aim to protect the client / asset-owner where appropriate. Contractual documentation must also better reflect BIM responsibilities.
- Future work should also consider responsibilities of clients in seeking guidance, and appropriate regulatory mechanisms for not doing so. This overlaps the need for educational pieces and development of security-models. The latter requires further categorisation of threat-scenarios to stakeholders. This includes those directly involved in actualisation of an asset, and from a moral obligatory perspective, the asset-users during operations whereby overlaps between security-risk realisation cascade to elevate health and safety risks. This is part of the development of clear example negligence scenarios to motivate industry awareness that baseline initiatives cannot be shirked.

Regulatory Mechanisms: As a sub-element of contractual and legal research, industry initiatives should aim to introduce change in how appointees engage with prospective clients within the AEC marketplace. This includes exploring the appropriate regulatory mechanisms (rules, guidance, best standard practices, duty-of-care) to incentivise appointees with the correct competencies and deter negligent suppliers who may otherwise apply inadequate security-competencies. Regulation should not deter the industry in moving towards best-practices for secure-collaboration; it should aim to incentivise lesser experienced organisations in gaining of competencies. This must also be in view and in consideration of SMEs. Future research should consider further analysis of such practices, in understanding the perspectives of SMEs.

7.2 Deployment Challenges of Framework

7.2.1 Roadmap to Deploy Framework Initiatives

Expanding upon the factors that a proof-of-concept implementation would require; it is firstly noted that a proof-of-concept implementation and deployment in this context should be the development of both a type of system artefact based upon the framework's concepts, and a detailed definition of a 'type' of project which a system artefact would underpin. It is envisaged these would be simulation projects wherein pull-based and networked approaches can be utilised to demonstrate agility, efficiency, and secure-by-default information-flows.

1. Such projects could feature IPD mechanisms whilst simultaneously considering how traditional contractual mechanisms should be appropriately disrupted to achieve progressive beneficial digital, collaborative, and security-minded change within industry.
    a. This is based upon exceptions captured within **Section 6.3.6**, of the need for contractual mechanisms to be aligned to networked motives of revealing the reality of any given stakeholders required scope of work, and thus responsibilities to each other in meeting the client's requirements (**Section 6.3.3.3**).
2. Correspondingly, in reaching this proof-of-concept stage for technological implementation, atomic process-maps should be captured i.e. the development of task template libraries. These must cover a broad range of different types of project activities that are generalisable to actors on BIM projects in generating and sharing information.
    a. At a project-scale, such libraries would be representative of generalisable tasks to be configured by actors for usage on real projects.

    b. At an industry-scale, templates would be shared within process databases that adopters would contribute to and utilise in a standardised, yet anonymised fashion as templates are not provided actual project-context until instantiated.

3. Networks (as process-maps) may also be sub-categorised based on the different types of assets (e.g. healthcare-assets) but should be aggregable from generic building-blocks (i.e. tasks) relevant to different types of projects and assets, regardless of specific sectors. This is possible as task-level processes are common across projects at the finer-scale of disciplinary activities and can be extended for use on real-projects.

4. The proposals for libraries could also be representative of a future stakeholder ecosystem comprised of industry partners / adopters, focused upon progressing collaborative advancements of digital BIM agendas in a security-minded fashion.

    a. In developing such an ecosystem, preliminary activities / case-studies with stakeholders will need to be undertaken to further viability of secure-by-default approaches; this includes the capture of libraries and the development of personas based upon different types of professionals, activities and organisational stakeholders.

5. Simulation projects or preliminary activities aiming to capture real-life examples of templates and process-maps can be extrapolated to further conceptual understanding, and thereby refinement of the data-schema of task-level concepts. This would ensure a refined and instantiated data-model (to finds the balance between generality and expressiveness, to be able to represent a wide-variety of projects, and their processes.

6. A number of system-level factors are overlapping in achieving the frameworks implementation. Overlaps with existing initiatives will be applicable such as the Uniclass 2015, and interoperability initiatives of IDM and MVD.

   a. System implementation of the exchange functionalities should consider how task-level processes provide additional context to the nature of professionals works and thereby act as a semantic map onto IFC outputs authored from design / BIM software. This could be utilised for semi-automated interoperability purposes by inferencing the intended output and provide the author potential corrections to be fed back into the authoring tool.

   b. This as opposed to IFC outputs which do not fully capture the authors intentions. This mapping could also be bi-directional with the IFC subsets being used to propose the generation of professional's tasks.

7. Other aligned technologies may also be relevant to consider such as machine-learning to learn from how libraries are implemented and evolve on real-life projects.

   a. I.e. utilising machine-learning to gain a deeper understanding of the inter-connections between tasks in a network, including 'how', 'what' and 'why' change in information-requirements occurs over the course of the project.

   b. This is in order to capture further task-templates or process-maps as a whole. The machine-readable and standardised nature of templates would underpin this potential.

8. Benefits may also be realised from the layering of machine-learning for the purposes of deep understanding of previous gaps arising in projects. Distributed ledger technologies were noted pertinent by some experts as they would uphold the notion of an atomic task deliverable via micro-contracts, which would also negate issues caused via traditional contractual paradigms.

a. These technological centric considerations should also further the scope of a proposed task-level data-schema and system-level implementations for pull-based atomic process capture, enablement, and governance.

Summary: The discussion has provided a high-level road-map for deployment of the framework in view of both system and IM / IS considerations of a new type of approach to undertaking projects and their processes. The broader implications of why the discussed road-map is important therefore is in view of moving towards deployment of the framework's benefits. Furthermore, this road-map represents the broad reaching nature of future work that is now available after having validated the key needs underpinning the framework. The key questions were whether strategic step-change was valid, and necessary to progress secure-collaboration agenda? If so, whether experts agreed with the concepts and principles denoted by the framework (as a whole) as a valid avenue to achieve this? B1 summarised the key point in this regard.

B1: "I think as well that you're doing this from a security-minded approach - that's what's triggered it all hasn't it - and well actually - it's relevant for any project - whether it's security-minded or not, what you're doing is creating the vehicle to generate a security-minded option - if you wanted - but actually you would do this for any project."

The research therefore remains cognisant the motivation was of exploring secure-collaboration, and accordingly, experts agreed the implementation of the approach would achieve secure BIM projects, by default, whilst optimising potential from efficiency and collaborative information-sharing perspectives. Information-flow security is achieved implicitly and not added as an afterthought whilst opening up other benefits experts perceived of the approach. As such the initial validation sets a strong argument for future research around these ideas. The following sections will explore some proposals in more detail.

7.2.2 Deployment of Framework Concepts

Based upon validation analyses throughout **Chapter 6,** this section will briefly overview considerations for future work of relevancy to instantiate and deploy the framework's concepts, linking to captured verifications issues and exceptions where relevant. Some of these ideas will expand previously delineated concepts, whilst others will summarise extrapolations of new concepts based on feedback.

Template Concepts: Template concepts should be further explored to easily deploy the proposed method of exchange within projects. The key goal for future research should be to capture and abstract the minimum number of project process maps in order to create template library/s for use within a proof-of-concept project and system. The capture and abstraction of process-maps will also feed into the refinement of the data-schema to represent atomic processes and data as a representative data-structure is required to ensure the agile extension of task-templates within projects. The following factors should be explored as part of future work.

- As noted in **Section 6.3.4.1**, the capture of process-maps and by extension, template libraries will likely require industry exploration of different types of activities within different types of project and asset contexts. A key requirement therefore is to capture the atomic IDs between different types of tasks. As a first step, this includes exploration, abstraction and extrapolation of the process-maps belonging to different disciplines.
- Exploration would be in view of common task-level requirements that can be extrapolated across different projects. I.e. identifying common building-blocks that can be manipulated for application and usage within different project-contexts.
- Experts perceived new ecosystems and atomic process initiatives may be derived given that a rich-environment of AEC process knowledge may be mapped internally within

organisations. This is as B6 noted however, is without a common schema or language to 'know we're talking about the same things' at a project and industry level.

- Experts also verified standardisation of this method of task-level capture is itself a significant step-change that is required. The linked benefits are the potential for improved capture and reuse of process maps across different projects, and also simply within the scope of individual organisations.
- Interoperability initiatives noted in **Section 7.2**. are also especially pertinent. Templates may align to this purpose, but in a crowd-sourced manner which can be adapted in an agile fashion. This is based upon the methodological changes required to ensure IDM and MVD initiatives are scalable with expanding requirements for interoperable exchange between different AEC domains.
- The template concept also adjoins to developing a schema which represents different project-activities in a standardised manner. It may for example be identified that characteristics of certain types of tasks are dependent and constrained by their activity-type e.g. structural analysis. These factors can in turn be captured to represent logical constraints in the definition and interlinkages of tasks.

Security Risk Templates: Templates should be captured of generalised security-risk knowledge of 'types' of assets and asset-information. Such templates should capture *what* represents the *potential* to be sensitive, *why, how, to who* and *to what extent* (likelihood and potential impact given a range of cascading and interlocking types of risks). These templates would thereby facilitate stakeholder's intuitive understanding, when approaching project activities, what activities / information will require additional governance and what are necessary governance measures.

- Templates should be with respect to common vulnerabilities in generation of specific information types / values e.g. identification that specific types of spaces serve a physical security-function or are involved in handling asset / operational critical functions. This is in line with experts' perceptions tasks and associated sensitivities (i.e. security-risk) are only deemed sensitive when given project-specific and spatial context.
- They should not however derive *how* such vulnerabilities may be exploited. This information should not be accessible from a perspective of 'communicating knowledge' for the purposes of guiding key project-level stakeholder decisions such as the client. The overlapping knowledge of general patterns of how vulnerabilities arise (in understanding how to mitigate them) should not be publicly available.
- Rather, such knowledge would be foundational to upskilling of workforces such that GRs would make informed decisions over the direction of governance procedures. This is both a project and sponsor level and is representative of both guiding sponsors and ensuring inter-organisational governance amongst appointees. As such, an appropriate route to capture and represent the knowledge necessary for patterns for security-risk governance procedures must be identified.

Considerations for concepts overlapping network concept

Validation of the governance network concept has uncovered future work would consider how such a concept could be implemented to achieve this goal. This concept however ties into the system and data-schema implementation of network concepts. It thereby overlaps proposals for templates, and information and security governance. As such, the following sections overview future considerations captured throughout **Section 6.3** which overlap many areas.

Hierarchal Information Governance: Future work should consider the benefits and implications of change-management feedback in **Section 6.3.3.2** in terms of how appropriate stakeholders could 'change-manage' the network as a whole. This may be especially important for clients as a predictive feature for them to be able to understand how a change in their requirements may signify significant cascading change throughout the network i.e. a butterfly effect. Before green-lighting new / updated requirements, clients therefore need to be able to understand the potential cascade of atomic requirements that would be implicated. From a hierarchal perspective, clients and appointees must also be able to understand how the cascade influences other stakeholder's within and across appointment-chains.

Capturing Task Template and Process Network Logic: It was noted that process standardisation could enable the capture of 'logic' which underpins inferences pertaining to networks. For example, B2 and B6's approach to capture templates identified that certain types of tasks need to be completed before other types of tasks could logically commence. This corresponds to rulesets that are embedded within templates, in relation to other types of templates. Future work should thereby capture examples of such rulesets which will ultimately underpin the interconnections between instantiated tasks. This is also part of initiatives for expanding template libraries and may also overlap machine-learning considerations. Future work should also consider that a network is spatially oriented, and the implications of this feature.

Exploring Atomic Four-Dimensional Network Features: Multi-directionality and temporality (i.e. historical and evolutionary) perspectives of a network were captured throughout **Section 6.3.5** as considerations for network features. It is noted via analysis that both multi-directionality and temporality perspectives are entwined.

- Future work could consider how realised networks would serve as smart, adaptive information-flows between all actors. For example, it could be considered how networks could inform actors of how, when and where their task-outputs clash with other requirements, design-centric or otherwise. This was noted in **Sections 6.3.5.1** and **6.3.5.2**.
- This is also a consideration that extends throughout the lifetime of an asset for actors who should be able to infer whether new information (or planned requirements) represents a clash with present or historical requirements of other tasks.
  - Relevant feedback in **Section 6.3.5.1** entails ensuring that professionals are able to test the waters before greenlighting changes to (a) avoid unintended consequences and (b) communicate the potential impact of change with other stakeholders.
- In consideration of analysis within **Section 6.3.5.2**, networks would possess against each task transaction (a) who had initially required outputs of a previous task-iteration and (b) what was the status (reliability / assurance) of said outputs. System implementation of a network should provide interfaces for actors to be aware of these factors, prior to initiating new queries, or in providing outputs.
  - Automation opportunities include smart-content delivery capabilities which could present relevant inferences to guide actors decisions of what information will be necessary to which other actors, and when; this may be achieved via machine-learning of information-transactions throughout process-networks (present / past projects). Future work could explore how such mechanisms would be provided.

- It was noted in **Section 6.3.5.2** that organisations and their professionals could identify how atomic information-products (i.e. outputs delivered to the asset-owner) ‘came to be’ and thereby gauge their reliability prior to making new decisions. This can be achieved as all iterations of an information-product persist within a given network, and actors may be able to trace from the ‘inception’ of a given information-product, to its final state, all tasks, professionals and adjoining requirements / outputs that have influenced it.

Capturing and Expanding Atomic Process Knowledge: Future work could consider providing interfaces to help actors to understand why certain variables / requirements of a given instance of a task change throughout its lifetime. As noted within **Section 6.3.5.3**, this is part of leveraging the four-dimensional nature of a network to support decisions in expanding template libraries. It is envisaged that the standardised and machine-readable nature of templates would help facilitate this semi-automated knowledge expansion.

Based upon verification that processes at an atomic scale can utilise common templates, future research should also explore opportunities to enable the on-going capture of process ontologies for different types of projects and built assets. This is to provide stakeholders 'starter networks' of different types of assets. Implementation should consider appropriate user-interface and automation mechanisms to abstract complexity and enable stakeholders to simply achieve these extension procedures.

- Given the complexity of defining and implementing atomic BIM processes, B1 suggested that different types of 'formulaic' projects could be templated based upon individual tasks as part of preliminary deployment activities. This would prove that the framework's methods are viable in structuring processes efficiently for real usage.
- After the initial abstraction procedures to capture 'starter networks' for specific project-contexts, more specialised maps could be developed from base task-templates comprising a network. Future work could explore how to achieve this idea.
- A security-centric benefit may be for clients to possess starter-packs of different project contexts to understand common types of activities (from project-onset) that factor into security-risk governance and steps to implement their project ecosystems. This overlaps with the security-risk template concept.

Enabling Governance of Project Risk: Feedback of networks as an opportunity to govern project-risk was explored within **Section 6.3.5.4**. This future concept will likely overlap with automation initiatives and functionality for stakeholders to utilise networks in temporal contexts.

- Networks could be employed for predictive benefits and future work could consider functionality and interfaces for informing appropriate actors of elevating project-risk, such that it can be avoided. Functionality should also be considered in enabling actors to trace through previous networks to understand process and information gaps that could have been avoided.
- Alterations of project-risk tie into considerations that liability could be attributed to specific stakeholders in not procuring an activity or providing information. Whilst such an opportunity opens up benefit in informed and frank stakeholder discussion, cultural barriers may need to be overcome to implement such mechanisms. Research could consider where such disruptive benefits may create other tensions and how they would be eased.

Future research may also consider how networked governance of project-risk overlaps with procurement or insurance considerations (in view of alterations of personal project-risk). An associated consideration is discussed in the following area of future research pertaining to procurement and contractual methods.

Exploration of Procurement and Contractual Methodologies: Aligned methodologies may be required to enable the framework's proposed methods. Whilst alignment of contracts based on atomic deliverables would require significant change, it may provide benefits of more integrated and secure project work, whilst negating issues of current contractual mechanisms. Questions must be answered as to how atomic information-delivery would feed into the responsibility of any given organisation, and the most appropriate procurement forms to underpin proposed methods.

Future work should consider how appointers and appointees would define atomic obligations between themselves, but also of other stakeholders within and across appointment-chains. It would also need to be considered how these would feed into updated organisational contracts. Appointers may for example act as a contractual intermediary of information their appointees query from other bodies; agreements with appointees would be updated iteratively as a feature of hierarchal governance underpinned by a contractual framework in defining that could be aligned to micro-contract and distributed ledger considerations.

Research should also explore which procurement forms would be appropriate to underpin proposals for bidirectional, iteratively captured responsibilities which may benefit overall project-efficiency, but also potentially alter project-risk encountered by stakeholders. Correspondingly, it must also be considered if bespoke procurement forms or novel contractual frameworks are needed.

Questions over procurement forms also overlap consideration for how atomic task-level activities would be managed in ultimate view of effective information-delivery to clients. Aggregation capabilities of task-sets may provide constructs for managed information at a higher-level in preparation for delivery; the question to be answered is *when* should information be delivered? In providing context, it is envisaged the lower latency of transactions could enable higher degrees of project-work efficiency, and thereby a decrease in time required for information-delivery cycles between stakeholders. Were such other benefits (noted within **Section 6.3.5**) to be proven via preliminary testing, future work could consider broader questions over how digitisation advancements would implicate current deliverable timescales and other contractually related factors such as stage-based deliverables.

Exploration of Distributed Ledger Technologies: Procurement and contractual exceptions also overlap whether such technologies could be utilised to facilitate the alignment of atomic deliverables, and process-networks as a whole with equally atomic, 'micro-contracts'. This may enable significant suitability and auditability opportunities but requires use-cases to be defined.

- Research may explore questions such as whether micro payment structures based upon task-level micro-contracts would incentivise (a) delivery of the correct information to the client, but also (b) secure exchange amongst stakeholders to enable their delivery.
- Further questions may also include whether 'value-mapping' (and thereby payment) can be captured based upon how a given aspect of project-information is cascaded and utilised by other professionals' stakeholders through the network.

If well-defined use-cases are identified, further questions would comprise 'how' such technologies would implement atomic, pull-based information-delivery at the level of the individual task. This may include corresponding questions such as how atomic task-level deliverables would be implemented via distributed-ledgers. Questions need to be answered how the client and project-stakeholders approach and govern this from contractual perspectives.

- Other factors overlapping networked approaches include considerations of how any given actors' micro-contract would evolve accordingly in view-of changing scope of responsibilities (identified and communicated via a network).

8 Research Conclusion

This chapter concludes the thesis with a critical discussion starting with a reintroduction of the research aim based on the problems faced. This is followed by an individual review of each research objective which summarises findings, explores the undertaking of each objective in meeting the overall research aim and summarises relevant implications, contributions, limitations and future work. This chapter will conclude with an overall review of the research undertaken, summarising key contributions, implications, limitations and discuss the answers found in response to the research questions.

8.1 Research Aim and Problem Restatement

The research aim was to develop a conceptual process and data governance framework which can be applied to enable secure collaboration for BIM projects. Related research questions were posed in the need to explore the nature of tensions arising between security and collaboration, whether a process and data governance framework would resolve such tensions, and what the nature of such a framework would entail. The aims and questions reflected the challenges of achieving secure collaboration for security-minded BIM projects. The framework in turn represents the need for a method to deliver BIM projects which enables security by default, whilst also providing a route to further optimise the efficiency of processes and information-flows. This aim was met via the completion of the individual research objectives, each addressing an aspect of the overall research aim.

8.2 Review of the First Objective

First Objective: *'To conduct a thorough study (primary and secondary) to identify the key security and collaboration barriers within complex security-minded projects and to identify the corresponding enablers for secure collaboration.'*

8.2.1 Completion Overview of First Objective

A thorough literature search (secondary study) was carried out, identifying academic initiatives which have explored the overlap between collaboration and security motives within the scope of the built-environment and security-minded environments such as nuclear and infrastructure. In addition, a thorough primary study captured security concerns for the stakeholders interviewed as barriers to secure collaboration. Enablers were also captured based upon approaches presently utilised within their practices, or potential approaches which could improve issues; both enablers and barriers further served to frame the requirements of the framework.

8.2.2 Undertaking and Meeting of First Objective

Firstly, with respect to the literature search, many themes were captured from the literature such as data-management, data-security, cloud-based IM solutions, BIM interoperability etc. The literature-review painted a picture of the overall digitisation agenda for the sector, alongside academic focuses on deploying data-security mechanisms for IM solutions. The key gap identified of the knowledgebase was that there exists limited research that explicitly explores the links or overlaps between AEC collaboration and security focuses (as noted within the interview research-design). A hypothesis was thereby devised that the missing knowledge that will further secure collaboration agenda may be extracted from within real industry practice. Furthermore, given the recent industry push towards security-mindedness, it was also hypothesised that viable industry avenues towards secure collaboration would be evolving in real-time. This led to a thorough primary study to capture secure collaboration concerns in specific practices.

These hypotheses were proven via the wealth of primary knowledge captured through experts who are involved in delivering or guiding BIM digitisation, collaboration, and security agenda for security-minded projects and the AEC industry broadly. Their key concerns were linked to the project-specific nature of assets such as nuclear and rail, wherein exposure of sensitivities makes available or widens threat-avenues. This was however the simplest security-concern commonality identified across stakeholders interviewed. Rather, capturing the security concerns of any *sole* interviewed stakeholders was not representative of the cross-section of concerns across different CNI domains, where security was identified to be a focus, but to varying degrees of holism.

In order to therefore overcome both the 'barriers' and define pragmatic 'enablers' to secure collaboration, a core consideration was captured. This was the need for integrated project implementation requirements over overlapping project ecosystem dimensions. This is essential from the perspectives of security-minded projects in maintaining security whilst also being efficient, cost-effective, and commercially attractive (for both sponsors and appointees). In other words, such an approach is a necessity for reducing tensions faced in the implementation and operation of projects. Via the in-depth consideration of how to ensure project ecosystems are implemented with integrated requirements, the research captured the key enablers and barriers for projects with a higher degree of security concerns **(Sections 4.5).**

Abstracted socio-organisational and project level enablers and barriers (for security-minded projects) are also however relevant to the built-environment as a whole. In reaching such conclusions, it was necessary to understand *why* the identified barriers and enablers possess cross relevancy across (a) the security-minded projects interviewed, (b) other sensitive domains explored based upon expert's experiences (e.g. mining), and (c) the broader industry's present (overall) digital and security maturity. This in turn required an understanding of both the commonalities and variances of issues across the different domains, as well as capturing the wider picture of issues relevant to the built-environment; this is whether practices currently possess security-minded competencies, are aiming to instil them, or are still incognisant.

The questionability of the digital and security maturity of the broader industry was considered but had not been fully appreciated until the analysis was undertaken. In turn, it was identified that it was necessary to understand the overlap between the concerns for security-minded environments and the broader industry. This is as the two perspectives cannot be separated. Capturing the enablers and barriers in security-minded domains could not be achieved *without also* considering broader industry maturity. The reality is that CNI domains, alongside other projects wishing to proactively instill secure collaboration measures are both tied to the market force of the industry, and thereby the readiness of appointees and their appointment-chains in the built-environment. Furthermore, *any* project possesses the potential to possess security-implications. The researcher was required to understand this in order to posit solutions in pursuit of the evolution of secure collaboration maturity for the built-environment, and the intended security-minded domains by extension.

8.2.3 First Objective: Summary of Implications

A comprehensive literature search uncovered many themes such as sensitive information, privacy and limited stakeholder trust relevant to the overarching of secure collaboration. They were included within a research interview guide which explored how relevant themes may 'overlap' from the perspective of achieving secure collaboration, alongside how governance mechanisms may resolve barriers. A combination of implications, including **contributions, limitations and future work** include the following:

1. **Contribution**: The research interview guide is based upon the hypothesis that themes overlap across parent themes of collaboration and security. This is a unique approach

and lays the foundation for future analysis into organisational / project settings with a deeper appreciation of the complex inter-relation of project motives.

2. **Future-work:** This research interview guide could be expanded for follow on research to further explore how these themes overlap in specific practices, and how improved process and data governance practices / mechanisms could enable resolution of issues. Its contribution is that it acts as a research-interview framework for targeted exploration of issues and interventions in specific organisations and projects.
3. **Limitation:** Future literature reviews may also attempt to address partial limitations by further exploring a perspective of project structuring, contractual and contract management overlaps between collaboration, efficiency and security motives.

In addition, the numerous nuances and patterns surrounding how such tensions arise were documented if holistic security-risk governance is not integrated into other project-motives.

1. **Contribution:** These findings are applicable as contributions to both security-minded environments and the broader sector via the completion of an in-depth diagnostics process. This diagnosed an inclusive and abstracted representation of enablers / barriers, including tensions and how to resolve them. These findings can enable future targeted exploration in industry where the results of the diagnostics procedure also captured how individual issues create barriers, or interact within real-life projects to create tensions.
2. **Limitation and Future Work:** Future research may aim to address a partial limitation of how these issues overlap by considering other dimensions and overlaps to tensions beyond those of security and collaboration, such as political / public governance factors for publicly funded projects. The analysis findings can be utilised to further develop the initially devised research interview guide for exploring tensions in practice and other barriers to security and collaboration (either individually or in tandem).

8.3 Review of the Second Objective

Second Objective: *'To capture security and collaboration needs within a governance framework for enabling future secure collaboration on security-minded BIM projects.'*

The review of this objective will focus upon the requirements capture process for the security and collaboration needs, whereas the review of the third objective will focus further on attributing meaning to the framework's concepts.

8.3.1 Completion Overview of Second Objective

The needs for secure collaboration and the requirements of the governance framework were captured via an in-depth analysis of the issues and gaps presented within both the security-minded practices interviewed, and factors which are relevant to the broader built-environment. This is based on findings of relevance to the industry as a whole which were captured through experts who are involved in the development of standards for industry. The secure collaboration needs represent motivations for the framework to provide an improved approach to implement and govern BIM processes and information-flows to ensure secure collaboration.

8.3.2 Undertaking and Meeting of the Second Objective

Firstly, capturing the stakeholder's needs within a framework was more complex than envisaged. This is due in part to the need for the approach to be relevant for both security-minded environments and broader practice. This aligns to previous conclusions where the two perspectives overlap, and it is pertinent to consider that interviewees BIM projects comprised suppliers and SMEs from within the broader industry with no guarantee of security specialisms. Potential appointees of various degrees of digital and security maturity overlap the same marketplace. Stakeholders within security-minded settings must therefore be cognisant of negligence or inexperience of organisations with limited maturity.

Furthermore, security-minded initiatives utilise similar underlying BIM methods in how their information responsibilities amongst stakeholders are planned, enabled, and accordingly governed. Such initiatives have however implemented bespoke approaches in governing sensitive information where their practices were limited by normative BIM approaches. These norms were posed by experts to present non-ideal scenarios for IS governance approaches in broader practice also. For example, issues of push-based transactions influence difficulties in *reconciling specifically* what information stakeholders need to share, based on no more than what others need to know. For broader practice, such norms contribute to security-concerns of oversharing; for security-minded environments they also contribute to heightened degrees of tensions.

The solutions therefore needed to represent the needs of such environments, but also be applicable across ecosystems implemented without appropriate governance in order to rectify this issue. A generalisable approach was also pertinent as tensions are variable and not tied to any specific project and their implementation of BIM collaboration and security. A 'wicked problem' was therefore encountered in defining a common framework towards secure collaboration. Upon analysis however, the limitations of current methodologies were in fact the common thread between issues, gaps, and thereby needs overlapping security-minded initiatives and broader practice. Accordingly, this required the cross-analysis of the underlying gaps of approaches utilised within the intended environments and the broader industry.

In meeting the objective, the analysis approach interrelated the issues / gaps of security-minded domains to those of broader industry as part of an abstraction in representing generalisable problem scenarios **(Section 4.5.3)**. Issues identified from a cultural perspective led to similar conclusions which increased confidence that an appropriate analysis, and thereby the capture of the needs had been undertaken. The analysis was validated with experts in ensuring complex nuances of the problem-environment had been captured accordingly, thereby ensuring this objective was properly met. Experts recognised the necessity for an interrelated analysis as meaningfully meeting the objective required proposals to be relevant in exceedance of solely security-minded environments, or simply any given organisation. The applicability of issues and response is detailed within the review the third of fourth objectives.

8.3.3 Second Objective: Summary of Implications

The diagnostics process of the security and collaboration needs represents a detailed cross-analysis procedure of gaps, issues and requirements from all stakeholders for implementing and governing BIM projects, processes, and information-flows linked to limitations of common BIM IM and IS governance approaches. Implications of this include the following:

1. **Contribution**: The diagnostics is representative of a novel approach in considering how process and technological gaps overlap, as well as providing the generalisable 'sharer' and 'receiver' concepts which may be useful to stakeholders in assessing information-flow issues at any level of actor atomicity due to its generality.
2. **Contribution**: This lays the foundation for future research which analyses the underlying limitations of current or future BIM IM approaches as it possesses forward facing applicability. This is because actors will always fill the role of 'sharers' and 'receivers' regardless of how future guidance represents the standard BIM IM approach.

The framework was defined as a response to complex overlapping needs, and as a result the proposed approach can benefit the security-minded practices interviewed whilst also moving industry towards security by default initiatives. Further industry-level benefits include:

1. **Industry Benefits**: Security-minded practices would face lesser issues in the appropriate selection of appointees, as a baseline degree of security competence would be upheld by

suppliers. Clients in both security-minded and broader practice would also benefit from increased competencies and assurance of appropriate governance and security of their assets. Tensions may thereby reduce with respect to administrative and financial overheads of implementing security-minded ecosystems.

2. **Industry Benefits**: The secure by default approach also acts as a proactive step in tackling future implications of present security negligence. This is with a view that the security-risk landscape for the digital built-environment is still evolving, and stakeholders will be made vulnerable as attackers find novel ways to exploit present exposures / weaknesses if not addressed.

Finally, further areas of required change were identified after defining the overarching requirements of the proposed governance approach. Examples include the need to address exceptions captured of contractual factors, and associated requirements that must be accounted for such project areas in implementing the framework.

1. **Limitation and Future Work**: Future research may address a research limitation where it is envisaged that more issues may become apparent as openBIM practices progress. This includes interoperability mapping and IFC-based data querying capabilities becoming commonplace to support the framework's IS principles. There is a need for further research to understand the contractual framework to support this in practice.

2. **Limitation and Future Work**: An extension to this research will be required to capture SMEs concerns, needs and further implications of limited security maturity, directly situated within the lens of their own organisational practices. This is a natural research limitation as the researcher would not have been able to learn from experts to make such informed conclusions if a SME / lesser-maturity focused research direction was initially taken.

8.4 Review of the Third Objective

Third Objective: *'To explore the governance concepts that will be necessary in enabling future secure and collaborative BIM processes.'*

8.4.1 Completion Overview of Third Objective

The governance concepts were explored for BIM project processes and their corresponding information-flows. They are denoted within **Chapter 5**, covering information planning, enablement and governance focuses which represent framework proposals for atomic pull-based information-transactions such that stakeholders only share what others need to know. Governance concepts are overlaid over atomic transactions to ensure both security and suitability are upheld. These proposals would enable secure by default atomic processes, in response to presently high-level push-based workflows with limited governance over intended outputs. The concepts are incrementally developed as 'patterns' which can be applied for both software-development and project contexts for processes and IM / IS. These concepts are detailed, but are generalisable such that they can be applied in different project contexts of different types of assets / infrastructure. They are also applicable for projects aiming to instil baseline or greater degrees of security-mindedness.

8.4.2 Undertaking and Meeting of Third Objective

The framework represents in-part the overarching requirements for governing BIM processes and data. However, it was also necessary to consider the potential solutions in the form of the process and data governance concepts and patterns. This is as a fluid overlap of thought processes was necessary to accurately capture (a) what problems are present, (b) what should occur in response to the identified issues, and (c) *how* the issues could be resolved via the definition of generic solutions. This overlap was necessary to ensure applicability of the framework's approach as a valid response to the issues.

The understanding of the required approach was refined as understanding of the problem-environment progressed, alongside how the proposed solutions should engender beneficial change of the environment itself. For example, the framework comprises patterns to allow for governing roles to set constraints on data for both secure and efficient access. However, the development of such concepts was only possible via real-life understanding of the complexities of project-specific practices. For this concept, this entailed in-depth understanding of how knowledge-management is central for governing roles to accurately constrain data. They must be aware of how actor's information-needs overlap organisations, where the degree of overlap scales with a project's complexity over time. Conversely, the developed pattern is also valuable for knowledge-management, such as in enabling appointees to share knowledge on what an effective response to a client's questions and requirements should be.

This example characterises the broad reaching project focuses that were considered in the pursuit of improved information-governance capabilities and also represents strategic proposals for it to become a deeply interconnected parameter of BIM project processes. The proposals tightly couple information requirements, exchange and access into one approach for atomic actors and their work responsbilities. These proposed changes in how exchanges are planned, transacted and governed are based upon principles that governance is not solely an intra-organisational procedure, but overlaps partners processes and appointment hierarchies (in view of the atomic interconnections of professionals). They need information to generate value and should be able to provide to others without encountering boundaries, whilst knowing, and thereby providing only what is needed.

The objective was met where experts evaluated the developed concepts as an idealised solution to industries issues as secure collaborative motives would be 'built-in' to projects and their processes. The study also meets the element of the objective concerned with the exploration of *future* approaches, through expert-based as to whether the developed concepts were an appropriate, viable and beneficial response to the problems identified, and whether the proposals would provide benefits over current approaches to justify the needs for further deployment. In addition, validation over a number of workshops and individual sessions led to the iterative refinement of the developed concepts, with the finalised version of the framework being represented within **Chapter 6**. The proposed framework requires future work to reconcile the exceptions encountered which is outside the research-scope as this would be part of deployment activities. This perspective is further expanded upon in the review of the fourth objective.

8.4.3 Third Objective: Summary of Implications

As the framework is a response to the cross-section of issues faced by the sector, its strengths lie in its broad applicability to different project and system contexts.

1. **Contribution and Benefit**: The developed concepts enable suitability of transactions between atomic professionals who are required to generate value whilst providing the extra level of governance required for security-minded environments over sensitivities, and clearances.

2. **Contribution and Benefit**: The concepts are also applicable to projects which do not adhere to formal categorisation of sensitive information / processes. Such projects aiming for baseline levels of security-risk governance can thereby achieve this. This is particularly important in view of 'smart' assets which implicate public health & safety.

3. **Contribution and Future Work**: Features proposed of the framework as a whole should be enabled via future technologies. The method itself is not envisaged to be met as a singular response by any given vendor, but rather act as blueprints of common concepts to be further explored in their implementation.

The concepts and the capture of issues and exceptions has also set the scene for future refinements. The nature of changes proposed are complex however and are beyond the scope of the framework which is to carefully define an approach for future implementation.

1. **Limitation and Future Work**: A limitation of the broad-sweeping nature of proposed change is the need for future work and implementation in specific projects. This links to the exceptions captured, which for example require worked examples of a network of atomic requirements or further considerations upon contractual implications.
2. **Limitations and Future Work**: Accordingly, further refinements to the framework should come about in the context of moving towards its real-life implementation of it and its principles on real projects. As part of doing so, there is also a need to implement an information-systems artefact based upon the framework.

8.5 Review of the Fourth Objective

Objective 4: *'To validate the framework with a number of experts.'*

This review will feature a split discussion on the validation of both the problem-environment, including captured requirements (Part A) and the framework and its concepts (Part B).

8.5.1 Completion Overview of Fourth Objective

Validation comprised expert-based evaluation via two workshops and four individual review sessions with a total of eight participants. This comprised evaluation of the problem-environment, the needs underpinning the framework alongside the framework and its concepts themselves. The key concepts, principles and patterns were proposed, and feedback of concepts was linked to the problems they tackle. This helped to analyse the utility and grounding of the artefacts based against the real-world settings the experts represented.

The evaluation technique provided a high-level method to attribute shared meaning to findings captured of complex, contextual problems to further understand (necessary iterations within the scope of this study and future-work as part of larger initiatives to deploy the framework. The categorisation aligned to design-science in ensuring the research possesses validity, relevancy and rigour. For evaluation of the problems, this was necessary to capture a broad consensus of the wealth of barriers identified, and that an improved approach was required. For evaluation of the framework, the technique ensured reliability and validity of the validation was gained through an in-depth appreciation of whether the framework and its concepts can be matched to the stakeholder's real-life practices / projects, and whether they both represent, and would resolve problems accurately identified of their problem-environment. This is whilst also categorising the 'boundary-conditions' to overcome for future deployment and ensuring insights to drive design-science iterations for this project-scope.

8.5.2 Undertaking and Meeting of the Fourth Objective (Part A)

The validation approach required critique from the original set of participants and additional set of experts who were not involved in the initial research interviews. This diversified the pool of expert opinion, and limited bias in the evaluation of the captured issues and the artefacts. This also served to broaden the applicability of the research validation by accounting for the existence and context of issues in more domains. A qualitative approach was utilised for the evaluation, which comprised categorising feedback of both captured issues and the framework into three high-level categories of verifications, issues and exceptions. This approach enabled the fluid categorisation of feedback on numerous presented issues in a complex and overlapping domain.

Firstly, issues captured are evolving and are not tied to an individual expert and their representative stakeholder organisation or project/s. This means that evaluation of the captured issues was better suited at an overarching level as opposed to in either the context of a specific stakeholder's project or targeted exploration of individual issues, such as ineffectual appointments in governing security-risk. Whilst such issues were validated in-depth, a fully comprehensive discussion of each captured issue would require numerous individual sessions in their evaluation.

Accordingly, a higher-level approach was required to enable further refinement of findings, whilst ensuring a consensus had been captured on the correctness of proposed issues. Overall, experts verified both the existence of portrayed issues, and related them back to their individual practices, including those not initially involved in the research. For example, new experts at the validation stage recounted their own experiences of attempting to guide negligent partners. Such validations served to strength the applicability, relevance and criticality of the initial findings.

With respect to the proposals, a key question was posed to experts as to whether they perceived strategic reconsideration of **BIM** methodologies to be valid in view of how the gaps of current approaches act as barriers to secure collaboration. This was part of ensuring that experts verified the appropriate and accurate formulation of the needs of the potential solution. This crucial feedback was therefore a 'gateway' which was necessary to pass through in order to validate the framework, its concepts and overall principles.

Ultimately, based upon the analysis of barriers, a ***potential*** approach was presented. To this end, experts agreed change was required in some manner across the sector in furthering digitisation and security initiatives. For example, a key factor that experts validated was that governance overlaid over processes was rare across practice and difficult to effectively implement. Experts agreed current methods implicate key security gaps in security-minded environments which is also highly pressurised by other demands. For example, the motives to remain operationally effective via open information-sharing, whilst also needing to split procurement-route if sensitive information is present. Experts verified such tensions represent a gap of an approach which can unlock benefits to secure collaboration (without detriment to either motive), but also unlock other efficiency motives within such domains. This led to further key validations that improved approaches are necessary and that the application of the framework is pertinent to achieving such motives.

Overall, the aforementioned gateway was therefore passed through, as a result of verifying the issues and gaps presented by current paradigms, and a high-level consensus on the principles of the framework. Exceptions were also captured which led to refinement and further contextualisation of the problem-environment made possible via expert's 'real-time' perceptions of how industry is evolving to resolve leftover inefficiencies from non-digital methods whilst learning to do so in a security-minded manner.

8.5.3 Undertaking and Meeting of the Fourth Objective (Part B)

The overarching approach to validate the framework and its concepts was to capture expert-based qualitative evaluation. As part of this evaluation, the high-level principles and requirements of the framework was undertaken. This was alongside a walkthrough of the concepts that were mapped to problems of current methods they should resolve.

The evaluation of the conceptual artefacts sought an overall consensus that the frameworks patterns individually, and the proposed overall approach were conceptually sound in their appropriate relation to the problems identified, that the approach could work if deployed in practice. This was alongside the capture of refinements and exceptions that are necessary to resolve in implementing the framework in practice. Their overarching responses were considered which included their perceptions as to whether the conceptual solutions are valid, applicable and viable in addressing the problem-environment.

As with the evaluation of the problem-environment, categorisation of feedback was undertaken based against the categories of verifications, issues and exceptions. These were attributed refined meaning for the purpose of evaluating the framework. The intended scope of the framework, including the needs and principles underpinning the solutions were portrayed. Experts cross-examined the proposed methods and critiqued whether it could provide solutions to the problems posed. This was especially beneficial where certain experts were involved in defining the next iterations of BIM standards. It is also noted that whilst experts understood the intended purpose of a concept, they also derived their own perceptions of the frameworks approach. This dynamic element of the qualitative approach further required analysis to contrast the intended portrayal of a concept with the derived feedback.

Overall, experts verified the research possesses relevancy, and the divergent approaches posed are thought provoking in view of how experts had considered individuals elements of how improved BIM information-flows could be planned, enabled and governed. The framework's approach was verified as bringing together different aspects of the puzzle to more effectively and securely govern BIM processes and information-flows. This also included experts relating the concepts to areas that are currently being forwarded in other research arenas as part of digitisation agenda for the industry, such as security initiatives for digital twins.

Experts also provided feedback of the framework's concepts and principles which were categorised under issues and refinements (as a subcategory of verifications). These evaluation categories reflect critique of proposals where the intended purpose of a concept in resolving a problem had been considered, but not all angles relevant to a given concept had been identified. This is a given, considering the researchers relative inexperience in comparison to experts who were able to plug the researcher's gaps in understanding. This for example included the broadening of the initially posed atomic information-requirements to different project life-cycle activities. Accordingly, experts provided alternative perspectives that will enable further refinement of the framework's concepts as both refinements and issues require further consideration in embedding the 'requirements' they represent to refine the framework's scope, such as enabling governance of other project-activities such as costing. These as with general verifications of future opportunities are considered as part of future work.

Another category of feedback comprised exceptions. In order to distinguish this category from issues categories, it is noted that the meanings attributed to particular categorises enabled the separation of feedback on (a) the elements of the solution that had been initially considered, to feedback on newly identified elements of the solutions (outside the scope of what was initially considered). In other words, it is reflected that exceptions served as feedback which represent the need to reconsider what 'dimensions' of the solution, or the problem environment itself act as challenges to the implementation of the framework, and the method of work it entails. Most notably, this was of the contractual factors that must be fully appreciated to implement a proof-of-concept, and to provoke further beneficial contractual and procurement step-changes to the industry as a whole. Analysis of these exceptions fed into a further iteration of the framework which considers these areas. Similarly, exceptions also characterise a spectrum of issues that represents related, but novel spin-off areas. Experts also took away exceptions to their own 'accepted beliefs' of current norms and their considerations upon how change should be prescribed for the industry. The research is thereby a positive starting point in creating further dialogue between academia and industry to tackle the challenges such dimensions present of the broader reach of future work required for industry evolution. Finally, the researcher expresses thanks to experts in the time and commitment provided by them in furthering the researcher's understanding.

8.5.4 Fourth Objective: Summary of Implications

The implications of the validation for both problem-environment and the framework create a strong foundation for future exploration and implementation of these ideas in practice. This includes verification over whether utility could be derived via the framework's implementation to solve stakeholders and industry-wide issues. They thereby agreed with the core principles of the proposed type of solution and verified the approach possesses both relevancy to their domains, that it is viable for implementation and have also provided a roadmap to instantiate the framework based upon their feedback.

1. **Implication and Future Work:** Experts verified research into the problem-environment and the gaps provides a strong foundation in characterising further dimensions to still be explored as part of future work and spin off research areas such as educational pieces to underpin secure collaboration for the built-environment.

2. **Implication and Future Work:** Experts also verified the frameworks approach represents the basis for future work and implementation. Such considerations for future work were noted in **Section 7 as** beyond security or collaboration, individually or in combination.

    a. Numerous avenues for new research areas were identified such as exploring the contractual implications and requirements for project stakeholders in the application of improved security-risk governance approaches. These areas were also carefully considered as part of ensuring suitability that the research has future facing applicability.

3. **Limitations and Future Work:** A natural limitation of the evaluation approach is that framework was proposed in line with its conceptual nature. This was due to the need for a consensus on the generality of applicability within broader contexts, but also due to the

complexity of design instantiation that would require further technical expertise and the exceptions captured to be overcome.

a. The technique provided the raw fuel to refine the framework's concepts within the scope of this project, whilst driving understanding of *how* it should be applied to resolve problems and furthering appetite for deployment. It is noted therefore that the technique meets the design-science motive to ensure valid and reliable findings at this stage of its life-cycle that can progress the artefact through further stages.

b. Whilst the technique was thereby appropriate for the scope and context of this research (as reviewed initially), future design cycles of the artefact, and its implementation in real contexts would naturally overcome the conceptual based nature of the artefact by providing a tangible and testable information-systems within real=life project-contexts. Future methods of evaluating the framework could for example link to a positivist approach in developing metrics to test the artefact against in a security-minded dummy project as part of case-studies.

8.6 Research Contributions, Limitations and Overall Conclusion

This section will conclude upon the research contribution and limitations in view of the original research aims, with a focus upon answering the research questions noted within **Chapter 1 (Section 1.2)**. The former question will be addressed firstly, where the nature of tensions between (a) the greater connectivity and collaborative capability via open information sharing practices, between (b) the need to appropriately limit and constrain openness and connectivity at all levels of fragmented appointment-chains, are the sources of great frustration within stakeholder's practices.

At their core, tensions represent a misalignment between project-motives (within each dimension of the project ecosystem). This is alongside the cultural issues facing the industry broadly, the limitations posed of BIM methods adopted in practice, and overall limited digital-security maturity. This is where the degree and specific types of security concerns is contextualised within a given project, alongside other motives such as efficiency, cost, time and quality. Such factors are tossed into a melting pot of project motives within such environments. Problems thereby arise in effectively implementing a project's ecosystem, including common cascading issues and resulting tensions influencing how may projects may go awry if holistic security-risk governance is not integrated into other project-motives. The tensions between security and collaboration project motives limit the operational efficacy of each other, and the project ecosystem at all levels, including the difficulties that arise in being able to reconcile information-sharing tensions between actors. These include, but are not limited to the difficulties in coordinating information of various sensitivities between stakeholders, or the concerns presented by negligent stakeholders themselves that serve to lessen trust and openness.

Tensions on complex project are however often influenced by other factors, such as the politically charged nature of projects, and the need to make decisions to ensure progression. This leads to a consideration of the reasons as to why such tensions exist in industry broadly, which may be better considered as a symptom of the divergent nature of digitisation within the built-environment. For some projects with existing security cultures, the need to adopt collaborative and open IS practices to security-minded environments reflects the need to quickly evolve, to meet stakeholder, public and political expectations in a growing digital world. For other public CNI projects which feature the rapid alliancing of new parties for projects such as rail, the tensions are a result of the manifestation of many motives at once, overburdening both appointees and their fragmented appointment-chains with lesser competencies / resources.

In view of such issues faced, this research has filled a gap within the knowledgebase for secure-collaboration which is an under-researched area. This is by having undertaken an in-depth diagnostics process as to the nature of enablers and barriers to secure-collaboration (including tensions) alongside detailing how they may be overcome for both the intended environments and the broader built environment. Therefore, expanding upon **contributions** noted in the review of the first and second objectives, the results of this thorough diagnostics process answered the former research question, and may also lead other researchers to be able to answer similar such questions for future research and interventions. This is via the abstraction of core themes and issues to be considered that other researchers may ideally build upon. The nature of the blockers, enablers and the tensions serve as 'building blocks' of individual types of issues and solutions that researchers can consider.

For example, socio-organisational centric research may seek to expand on tensions between '*under and over protection*' within specific contexts, to identify other relevant factors or implications. Furthermore, the interrelation of how these factors overlap, as represented as the cascade of issues in-turn represent **contributions** of generalisable 'patterns' that researchers can apply to direct their reasoning towards how the issues may arise and develop within other security-minded practices. This can also be undertaken from many perspectives inclusive of information-systems, socio-organisational / technical and broader business-management perspectives relevant to BIM research. Future research may however attempt to address a limitation posed by the need for abstraction. This is by defining other patterns of tensions and overlapping motives, where other concepts such as public reputational concerns contribute to tensions, and that the patterns by which the issues emerge and relate to cause tensions may be differentiated within project-specific practices. The capture of more patterns would increase comparability, discussion, analysis and thereby refinement of understanding of tensions, which will only increase. This being said, tensions and barriers were shared across the different security-minded practices interviewed afflicting the ability to easily reconcile the need to know and the need to share. Such types of IS tensions are not readily resolvable via improvements in the integration of project-requirements alone as the nature and triggers of such tensions are tied to the limitations of common approaches in implementing and governing BIM information-flows.

This finding was pertinent to answering the second question, and achieving the *overall research aim* via the development of the process and data governance framework based upon the common needs of security-minded practices interviewed; the nature of the framework is of a blueprint to instill secure-by-default BIM paradigms that are embedded within industry processes and further enabled by novel information-systems (rooted in the framework's principles) that alleviate secure IM issues specific to the sector. Therefore, the result is the **contribution** of a new type of artefact that embeds and reconciles many principles of governance broadly; this includes but is not limited to project and process governance, security-risk governance, data-security and data-quality. This is amongst information-flow centric concepts such as embedding atomic pull-based approaches which optimise work and information-exchange efficiency and latency amongst stakeholders.

This framework also acts as a 'go-between' between both information-systems theory development (for BIM technologies), and a new paradigm for BIM process methodologies. It also provides a synchronised approach where both academia and industry can utilise these concepts as foundations for further research and implementation into spin-off areas, such as the need for automated, probabilistic and holistic security-risk governance based in view of the whole project life-cycle approach. The further **contribution** therefore is the framework bridging the gaps between AEC based technology development for security-minded IM, by providing a framework directly matched to the complex needs of these environments, through the provision of systems-design patterns that ease implementation and operation of security-minded BIM.

This is thereby beneficial for BIM design science researchers in guiding their knowledge, and to further appreciate the concepts and principles necessary to fully deploy the framework with experts in the fields of BIM project and security governance. This aligns to another **contribution** as the framework acting as a catalyst for strategic reconsideration within industry in how BIM processes and information-flows are conceptualised, and thereby implemented. In this sense, the framework's principle would be of value to BIM IM standards setters, with preliminary validations undertaken to support this by analysing and contrasting the strengths and benefits the framework entails over current approaches.

The core limitation to thereby be addressed is to move beyond the conceptual artefact, to its instantiation in practice. This research has however ensured that appropriate design and direction is embedded within the framework such that it acts as the blueprint for implementing secure by default project ecosystems, underpinned by system-artefacts also based upon the framework. The degree of work required to achieve such a goal having resulted in the findings detailed in this thesis whereas the goal of deployment will further require an ecosystem of adopters to achieve. The overall combination of the contributions, and delineation of future work as the road-map of initiatives and recommendations will however enable industry to achieve this goal to thereby evolve and instill a greater degree of secure collaboration maturity within the sector.

Overall, it is concluded that this research has achieved its aim, and it has set an agenda for further work towards a secure Digital Built Britain in exceedance of the intended environments. It is hoped that this is only one of many further research initiatives that this preliminary study has enabled. Crucially, a new sphere of research is necessary. It should not be seen as a niche, rather, it should be seen as an essential ingredient for safe and efficient evolution, for the built-environment and the society it serves. More focus is necessary to broaden academic discussion of secure collaboration motives, raising awareness of these emerging themes, and thereby supporting the built-environment in taking hold of the initiative and becoming the trend setter in creating and enabling a digitally secure future.

9 References

Abedi, M., Fathi, M. S., & Rawai, S. (2013). *Cloud Computing Technology for Collaborative Information System in Construction Industry*.

Abowd, G. D., Dey, A. K., Brown, P. J., Davies, N., Smith, M., & Steggles, P. (1999). Towards a Better Understanding of Context and Context-Awareness. *Handheld and Ubiquitous Computing*, 304–307. https://doi.org/10.1007/3-540-48157-5_29

Adamu, Z. A., Emmitt, S., & Soetanto, R. (2015). Social BIM: Co-creation with shared situational awareness. *Journal of Information Technology in Construction, Vol. 20*.

Afsari, K., Eastman, C., & Shelden, D. (2016). Cloud-Based BIM Data Transmission: Current Status and Challenges. *Proceedings of the 33rd International Symposium on Automation and Robotics in Construction (ISARC)*. https://doi.org/10.22260/isarc2016/0129

Ahmed, V., & Abuelmaatti, A. (2018). Collaboration environments for small and medium-sized architecture, engineering and construction enterprises: success factors in implementation. *International Journal of Information Technology and Management*, *17*(4), 313. https://doi.org/10.1504/ijitm.2018.10013506

Ait-Lamallam, S., Yaagoubi, R., Sebari, I., & Doukari, O. (2021). Extending the IFC Standard to Enable Road Operation and Maintenance Management through OpenBIM. *ISPRS International Journal of Geo-Information*, *10*(8), 496. https://doi.org/10.3390/ijgi10080496

Akintoye, A., Goulding, J. S., & Zawdie, G. (2012). Construction Innovation and Process Improvement. *Construction Innovation and Process Improvement*, 1–17. https://doi.org/10.1002/9781118280294.ch1

Alreshidi, E., Mourshed, M., & Rezgui, Y. (2014). Exploring the Need for a BIM Governance Model: UK Construction Practitioners’ Perceptions. *Computing in Civil and Building Engineering (2014)*. https://doi.org/10.1061/9780784413616.020

Alreshidi, E., Mourshed, M., & Rezgui, Y. (2017). Factors for effective BIM governance. *Journal of Building Engineering*, *10*, 89–101. https://doi.org/10.1016/j.jobe.2017.02.006

Alreshidi, E., Rezgui, Y., & Mourshed, M. (2014, February 2). Requirements for developing BIM governance model: Practitioners’ perception. Retrieved March 30, 2021, from orca.cf.ac.uk website: http://orca.cf.ac.uk/id/eprint/76293

Alshammari, K., Beach, T., & Rezgui, Y. (2021). Cybersecurity for digital twins in the built environment: current research and future directions. *Journal of Information Technology in Construction*, *26*, 159–173. https://doi.org/10.36680/j.itcon.2021.010

Arayici, Y., Egbu, C. O., & Coates, S. P. (2012). Building information modelling (BIM) implementation and remote construction projects: issues, challenges, and critiques. *Journal of Information Technology in Construction*, *17*, 75–92. Retrieved from http://usir.salford.ac.uk/id/eprint/22736

Arayici, Y., Fernando, T., Munoz, V., & Bassanino, M. (2018). Interoperability specification development for integrated BIM use in performance based design. *Automation in Construction*, *85*, 167–181. https://doi.org/10.1016/j.autcon.2017.10.018

Atan, R., Talib, A. M., Abdullah, R., & Murad, M. A. A. (2012). Security Facilitation in Collaborative Cloud Data Storage Implementation Environment Based on Multi Agent System Architecture. *Journal of Software Engineering*, *6*(3), 49–64. https://doi.org/10.3923/jse.2012.49.64

Atkins. (2021). *The value of Information Management in the construction and infrastructure sector The val ue of I nformati on Management i n the constructi on and i nfrastructure sector*. Retrieved from Centre for Digital Built Britain website: https://www.cdbb.cam.ac.uk/files/cdbb_econ_value_of_im_report.pdf

Autodesk Vault Professional. (2014). *Autodesk Getting More Value from your BIM Process with Autodesk Collaboration and Data Management Products*. Retrieved from https://villagebim.typepad.com/files/bim-data-management-and-collaboration.pdf

Azhar, S. (2011). Building Information Modeling (BIM): Trends, Benefits, Risks, and Challenges for the AEC Industry. *Leadership and Management in Engineering*, *11*(3), 241–252. https://doi.org/10.1061/(asce)lm.1943-5630.0000127

Bashir, A. M., Suresh, S., Oloke, D. A., Proverbs, D. G., & Gameson, R. (2015). Overcoming the Challenges facing Lean Construction Practice in the UK Contracting Organizations. *International Journal of Architecture, Engineering and Construction*, *4*(1). https://doi.org/10.7492/ijaec.2015.002

Baskerville, R., Baiyere, A., Gergor, S., Hevner, A., & Rossi, M. (2018). Design Science Research Contributions: Finding a Balance between Artifact and Theory. *Journal of the Association for Information Systems*, *19*(5), 358–376. https://doi.org/10.17705/1jais.00495

Baskerville, R., Pries-Heje, J., & Venable, J. (2009). Soft design science methodology. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology - DESRIST '09*. https://doi.org/10.1145/1555619.1555631

Beach, T. (2019). *D-COM: Digitisation of Requirements, Regulations and Compliance Checking Processes in the Built Environment*. Centre for Digital Built Britain.

Beach, T., Rana, O., Rezgui, Y., & Parashar, M. (2015). Governance Model for Cloud Computing in Building Information Management. *IEEE Transactions on Services Computing*, *8*(2), 314–327. https://doi.org/10.1109/tsc.2013.50

Beetz, J., Berlo, L. A. H. M. van, R. Laat, D., & P. Helm, V. D. (2010). Bimserver.org - an Open Source IFC model server. Retrieved March 30, 2021, from research.tue.nl website: https://research.tue.nl/en/publications/bimserverorg-an-open-source-ifc-model-server

Beetz, J., R. Laat, D., Berlo, L. A. H. M. van, & P. Helm, V. D. (2010). Towards an open building information model server: report on the progress of an open IFC framework. Retrieved March 30, 2021, from research.tue.nl website: https://research.tue.nl/en/publications/towards-an-open-building-information-model-server-report-on-the-p

Beresnevichiene, Y. (2003). *A role and context based security model*. Retrieved from https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-558.pdf

Berlo, L. A. H. M. van, Beetz, J., Bos, P., Hendriks, H., & R. C.J Tongeren, V. (2012). Collaborative engineering with IFC : new insights and technology. *9th European Conference on Product and Process Modelling, July 25-27, 2012. Reykjavik, Iceland*, 811–818. Retrieved from https://research.tue.nl/en/publications/collaborative-engineering-with-ifc-new-insights-and-technology

Berlo, L. van. (2019, December). The curious case of the MVD. Retrieved from blog.buildingsmart.org website: https://blog.buildingsmart.org/blog/the-curious-case-of-the-mvd

Bernstein, P., & Pittman, J. (2004). *Barriers to the Adoption of Building Information Modeling in the Building Industry.*

Best, R. A. (2011). *CRS Report for Congress Intelligence Information: Need-to-Know vs. Need-to-Share*. Retrieved from https://fas.org/sgp/crs/intel/R41848.pdf

BIM Interoperability Expert Group. (2020). *BIM Interoperability Expert Group Report*. Construction Innovation Hub.

BIM Task Group. (2015). *Digital Built Britain Level 3 Building Information Modelling - Strategic Plan*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/410096/bis-15-155-digital-built-britain-level-3-strategy.pdf

BIM+. (2021, July 9). Cyber attacks and BIM: how to be prepared. Retrieved September 22, 2021, from BIM+ website: https://www.bimplus.co.uk/dealing-digital-dangers-bim/

Bolpagni, M., & Hooper, E. (2021). *Information management according to BS EN ISO 19650 Guidance Part D Developing Information Requirements*. Retrieved from https://www.ukbimframework.org/wp-content/uploads/2021/02/Guidance-Part-D_Developing-information-requirements_Edition-2.pdf

Bolton, A., Enzer, M., & Schooling, J. (2018). *The Gemini Principles - Digital twins of physical assets*. https://doi.org/10.17863/CAM.32260

Boyatzis, R. E. (1998). *Transforming qualitative information : thematic analysis and code development*. Thousand Oaks (Ca.): Sage Publications.

Boyes, H. (2013). *Resilience and Cyber Security of Technology in the Built Environment*. Institution of Engineering and Technology.

Boyes, H. (2014). Building Information Modelling (BIM): Addressing the cyber security issues. *Engineering & Technology Reference*. https://doi.org/10.1049/etr.2014.9001

Boyes, H. (2015). Security, Privacy, and the Built Environment. *IT Professional*, *17*(3), 25–

31. https://doi.org/10.1109/mitp.2015.49

British Standards Institution. (2013). *PAS 1192-2: Specification for information management for the capital/delivery phase of construction projects using building information modelling*. London Bsi British Standards.

British Standards Institution. (2014). *PAS 1192-3: Specification for information management for the operational phase of assets using building information modelling (BIM)*. British Standards Institution.

British Standards Institution. (2015). *PAS 1192-5: Specification for security-minded building information modelling, digital built environments and smart asset management*. London Bsi British Standards.

British Standards Institution. (2017). *PAS 185: Smart Cities. Specification for establishing and implementing a security-minded approach*. British Standards Institution.

BSI. (2020). BS EN ISO 19650-5:2020 - Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM). Information management using building information modelling - Security-minded approach to information management. In *ISO*. Retrieved from https://www.iso.org/standard/74206.html

Building design process. (2021). Retrieved from www.designingbuildings.co.uk website: https://www.designingbuildings.co.uk/wiki/Building_design_process

Cabinet Office. (2016). *The UK Cyber Security Strategy 2011-2016 Annual Report*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf

Cabinet Office. (2018). *Government Security Classifications*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

Carson, T., & Baker, D. L. (2006). *Adobe® Acrobat® and PDF for Architecture, Engineering, and Construction*. https://doi.org/10.1007/1-84628-138-5

Centre for Digital Built Britain. (2020). *The approach to delivering a National Digital Twin for the United Kingdom Summary report*. Retrieved from https://www.cdbb.cam.ac.uk/files/approach_summaryreport_final.pdf

Charalambous, G., Demian, P., Yeomans, S., Thorpe, T., Peters, C., & Doughty, N. (2012). *BIM and Online Collaboration Platforms – An investigation into emerging requirements*.

Chartered Institute of Building. (2020). *Understanding the capability and capacity of the UK built environment to deliver and retain digital information*. Retrieved from https://www.goldenthread.co.uk/Golden-Thread-Review.pdf

Chen, H.-M., & Hou, C.-C. (2014). Asynchronous online collaboration in BIM generation using hybrid client-server and P2P network. *Automation in Construction*, *45*, 72–85. https://doi.org/10.1016/j.autcon.2014.05.007

Chong, H.-Y., Wong, J. S., & Wang, X. (2014). An explanatory case study on cloud computing applications in the built environment. *Automation in Construction*, *44*, 152–162. https://doi.org/10.1016/j.autcon.2014.04.010

Christian, C. (2020). *FDOT Data Governance Initiative: Managing Vital Data Assets*. Retrieved from https://rosap.ntl.bts.gov/view/dot/50671

Chuang, T.-H., Lee, B.-C., & Wu, I-Chen. (2011). Applying Cloud Computing Technology to BIM Visualization and Manipulation. *28th International Symposium on Automation and Robotics in Construction (ISARC 2011)*. https://doi.org/10.22260/isarc2011/0023

Cleven, A., Gubler, P., & Hüner, K. M. (2009). Design alternatives for the evaluation of design science research artifacts. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology - DESRIST '09*. https://doi.org/10.1145/1555619.1555645

Coates, P., Biscaya, S., & Rachid, A. (2018). The utilization of BIM to achieve prescribed undergraduate learning outcomes. *Core.ac.uk*. Retrieved from https://core.ac.uk/reader/199214740

Cockburn, A. (2009). *Agile software development: The cooperative game*. Upper Saddle River, Nj: Addison-Wesley.

Construction Innovation Hub. (2021). *Smart Standards An approach to implementing ISO 19650-2 using tasks in a digital process*. Retrieved from Centre for Digital Built Britain website: https://constructioninnovationhub.org.uk/wp-content/uploads/2021/06/SmartStandards_170621.pdf

Construction Management Association of America. (2012). *An Owner's Guide to Project Delivery Methods*. Retrieved from https://www.cmaanet.org/sites/default/files/inline-files/owners-guide-to-project-delivery-methods.pdf

CPNI. (2015). *Initiating a dialogue about the security of digital built assets: a guide for managers (with regard to PAS 1192-5, A Specification for security-minded building information modelling, digital built environments and smart asset management)*. Retrieved from https://www.cpni.gov.uk/system/files/documents/ae/78/BIM-A-Guide-For-Managers.pdf

CPNI. (2020). *Introduction to BS EN ISO 19650-5:2020 - Security-Minded Approach to Information Management*. CPNI.

Crotty, R. (2016). *Impact of building information modelling : transforming construction*. Oxfordshire: Routledge.

Cruz, I. F., Gjomemo, R., Lin, B., & Orsini, M. (2009). A Constraint and Attribute Based Security Framework for Dynamic Role Assignment in Collaborative Environments. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, 322–339. https://doi.org/10.1007/978-3-642-03354-4_24

Das, M., Cheng, J. C., & Kumar, S. S. (2015). Social BIMCloud: a distributed cloud-based BIM platform for object-based lifecycle information exchange. *Visualization in Engineering*, *3*(1). https://doi.org/10.1186/s40327-015-0022-6

Das, M., Tao, X., & Cheng, J. C. P. (2021). BIM security: A critical review and recommendations using encryption strategy and blockchain. *Automation in Construction*, *126*, 103682. https://doi.org/10.1016/j.autcon.2021.103682

Dave, B., Koskela, L. J., Kiviniemi, A., Tzortzopoulos, P., & Owen, R. L. (2013). *Implementing lean in construction : lean construction and BIM*.

Demian, P., Steven, Y., & Murguia-Sanchez, D. (2019). *Network FOuNTAIN A CDBB network: For ONTologies and information maNagement in digital built Britain: Final report*. Retrieved from https://www.repository.cam.ac.uk/bitstream/handle/1810/293302/Demian_Network_FOuNTAIN_Final_Report_v17-disclaimer-added.pdf?sequence=1&isAllowed=y

Dennis, A. R., Fuller, R. M., & Valacich, J. S. (2008). Media, Tasks, and Communication

Processes: A Theory of Media Synchronicity. *MIS Quarterly*, *32*(3), 575. https://doi.org/10.2307/25148857

Designing Buildings. (2021). Pre-qualification questionnaire PQQ for construction contracts. Retrieved from Designingbuildings.co.uk website: https://www.designingbuildings.co.uk/wiki/Pre-qualification_questionnaire_PQQ_for_construction_contracts

Durdyev, S., Hosseini, M. R., Martek, I., Ismail, S., & Arashpour, M. (2019). Barriers to the use of integrated project delivery (IPD): a quantified model for Malaysia. *Engineering, Construction and Architectural Management*. https://doi.org/10.1108/ecam-12-2018-0535

Eadie, R., McLernon, T., & Patton, A. (2015). *An Investigation Into the Legal Issues Relating to Building Information Modelling (Bim)*. Retrieved from https://www.academia.edu/22708067/An_Investigation_Into_the_Legal_Issues_Relating_to_Building_Information_Modelling_Bim_

Eastman, C. (1976). General purpose building description systems. *Computer-Aided Design*, *8*(1), 17–26. https://doi.org/10.1016/0010-4485(76)90005-1

Eastman, C. M., Teicholz, P. M., Sacks, R., & Lee, G. (2018). *BIM handbook : a guide to building information modeling for owners, managers, designers, engineers and contractors*. Hoboken, New Jersey: Wiley.

Egan, S. J. (1998). *Rethinking Construction*. Retrieved from https://constructingexcellence.org.uk/wp-content/uploads/2014/10/rethinking_construction_report.pdf

Elghaish, F., Abrishami, S., Hosseini, M. R., & Abu-Samra, S. (2020). Revolutionising cost structure for integrated project delivery: a BIM-based solution. *Engineering, Construction and Architectural Management*. https://doi.org/10.1108/ecam-04-2019-0222

Elghaish, F., Abrishami, S., Reza Hossein, M., & Abu-Samra, S. (2019). Revolutionising cost structure for integrated project delivery: a BIM-based solution | Emerald Insight. *Engineering, Construction and Architectural Management*. https://doi.org/10.1108\/ECAM

Emmitt, S., & Gorse, C. (2006). *Communication in Construction Teams*. https://doi.org/10.4324/9780203018798

Evans, M., Farrell, P., Elbeltagi, E., & Dion, H. (2021). Barriers to integrating lean construction and integrated project delivery (IPD) on construction megaprojects towards the global integrated delivery (GID) in multinational organisations: lean IPD&GID transformative initiatives. *Journal of Engineering, Design and Technology*. https://doi.org/10.1108/jedt-02-2021-0070

Fathi, M., Abedi, M., Rambat, S., Rawai, S., & Zakiyudin, M. (2012). Context-Aware Cloud Computing for Construction Collaboration. *Journal of Cloud Computing*, 1–11. https://doi.org/10.5171/2012.644927

Ford, J., & Shana'a, M. (2020a). *Information management according to BS EN ISO 19650 - Guidance Part C Facilitating the common data environment (workflow and technical solutions)*. UKBIMFRAMEWORK.

Ford, J., & Shana'a, M. (2020b). *Information management according to BS EN ISO 19650 Guidance Part F About information delivery planning*. Retrieved from UKBIMFRAMEWORK website: https://www.ukbimframework.org/wp-content/uploads/2020/09/Guidance-Part-F_About-information-delivery-planning_Edition-1.pdf

Gallaher, M., O'connor, A., Dettbarn, J., & Gilday, L. (2004). *Cost Analysis of Inadequate Interoperability in the U.S. Capital Facilities Industry*. Retrieved from https://nvlpubs.nist.gov/nistpubs/gcr/2004/NIST.GCR.04-867.pdf

Ganah, A., & John, G. A. (2015). An Overview of the Feasibility of Achieving Level 2 Building Information Modeling by 2016 in the UK. *Journal of Civil Engineering and Architecture*, *9*(8). https://doi.org/10.17265/1934-7359/2015.08.001

García de Soto, B., Georgescu, A., Mantha, B., Turk, Ž., & Maciel, A. (2020). *Construction Cybersecurity and Critical Infrastructure Protection: Significance, Overlaps, and Proposed Action Plan*. https://doi.org/10.20944/preprints202005.0213.v1

Ghadiminia, N., Mayouf, M., Cox, S., & Krasniewicz, J. (2021). BIM-enabled facilities management (FM): a scrutiny of risks resulting from cyber attacks. *Journal of Facilities Management*. https://doi.org/10.1108/jfm-01-2021-0001

Ghassan Aouad, & Yusuf Arayici. (2010). *Requirements engineering for computer integrated environments in construction*. Chichester, West Sussex, U.K. ; Ames, Iowa: Wiley-Blackwell.

Hartmann, T., van Meerveld, H., Vossebeld, N., & Adriaanse, A. (2012). Aligning building information model tools and construction management methods. *Automation in Construction*, *22*, 605–613. https://doi.org/10.1016/j.autcon.2011.12.011

Hatab, M. A., & Hamzeh, F. (2013). *Information Flow Comparison Between Traditional and BIM-Based Projects in the Design Phase*.

Henderson, J. C., & Venkatraman, H. (1993). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, *32*(1), 472–484.

https://doi.org/10.1147/sj.382.0472

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75. https://doi.org/10.2307/25148625

Hossain, Md. A., Yeoh, J. K. W., Abbott, E. L. S., & Chua, D. K. H. (2020). Domain-knowledge enriched BIM in Construction 4.0. In *Construction 4.0: An Innovation Platform for the Built Environment*. Routledge.

Howard, R., & Björk, B.-C. (2008). Building information modelling – Experts' views on standardisation and industry deployment. *Advanced Engineering Informatics*, *22*(2), 271–280. https://doi.org/10.1016/j.aei.2007.03.001

İLAL, M. (2007). *The Quest for Integrated Design System: A Brief Survey of Past and Current Efforts*. Retrieved from http://jfa.arch.metu.edu.tr/archive/0258-5316/2007/cilt24/sayi_2/149-158.pdf

Infrastructure and Projects Authority. (2016). *Government Construction Strategy (GCS)*.

Isikdag, U., & Underwood, J. (2010). Two design patterns for facilitating Building Information Model-based synchronous collaboration. *Automation in Construction*, *19*(5), 544–553. https://doi.org/10.1016/j.autcon.2009.11.006

ISO - International Organization for Standardization. (2018a). ISO 19650-1:2018 - Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 1: Concepts and principles. In *ISO*. Retrieved from https://www.iso.org/standard/68078.html

ISO - International Organization for Standardization. (2018b). ISO 19650-2:2018 - Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 2: Delivery phase of the assets. In *ISO*. Retrieved from https://www.iso.org/standard/68080.html

Jallow, A., Demian, P., Baldwin, A. N., & Anumba, C. (2010). An integrated requirements management system for construction projects. Retrieved from: **https://www.semanticscholar.org/paper/An-integrated-requirements-management-system-for-Jallow-Demian/4557fc4c866963ed4d9f05ba5eabd2bc10c1a6f3**

Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, Adoption Barriers and Myths of Open Data and Open Government. *Information Systems Management*, *29*(4), 258–268. https://doi.org/10.1080/10580530.2012.716740

Jiao, Y., Wang, Y., Zhang, S., Li, Y., Yang, B., & Yuan, L. (2013). A cloud approach to unified lifecycle data management in architecture, engineering, construction and facilities management: Integrating BIMs and SNS. *Advanced Engineering Informatics*, *27*(2), 173–188. https://doi.org/10.1016/j.aei.2012.11.006

Jonas, J. (2007). "Need to Know" vs. "Need to Share" – A Very Fine Line Indeed. Retrieved, from website: **https://jeffjonas.typepad.com/jeff_jonas/2007/04/need_to_know_vs.html**

Jones, D., & Gregor, S. (2007). The Anatomy of a Design Theory. *Journal of the Association for Information Systems*, *8*(5). https://doi.org/10.17705/1jais.00129

Jørgensen, K. A., Skauge, J., Christiansson, P., Svidt, K., Sørensen, K. B., & Mitchell, J. (2008). *Use of IFC Model Servers - Modelling Collaboration Possibilities in Practice*. Retrieved from https://vbn.aau.dk/en/publications/use-of-ifc-model-servers-modelling-collaboration-possibilities-in

Kähkönen, K., & Rannisto, J. (2015). Understanding fundamental and practical ingredients of construction project data management. *Construction Innovation*, *15*(1), 7–23. https://doi.org/10.1108/ci-04-2014-0026

Kamara, J. M., Augenbroe, G., Anumba, C. J., & Carrillo, P. M. (2002). Knowledge management in the architecture, engineering and construction industry. *Construction Innovation*, *2*(1), 53–67. https://doi.org/10.1108/14714170210814685

Kannengiesser, U., & Roxin, A. (2016). An agile process modelling approach for BIM projects. In *eWork and eBusiness in Architecture, Engineering and Construction*. Boca Raton, Florida: Crc Press.

Kaptelinin, V., & Nardi, B. (2007). Acting with technology: Activity theory and interaction design. *First Monday*, *12*(4). https://doi.org/10.5210/fm.v12i4.1772

Kassem, M., Iqbal, N., & Dawood, N. (2013). A Practice-Oriented BIM Framework and Workflows. *Computing in Civil Engineering*. https://doi.org/10.1061/9780784413029.066

Kayworth, T., & Whitten, D. (2010). Effective Information Security Requires a Balance of Social and Technology Factors. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2058035

Kehily, D., & Underwood, J. (2015, October 1). Design Science: Choosing an appropriate methodology for research in BIM. Retrieved from usir.salford.ac.uk website: http://usir.salford.ac.uk/id/eprint/38522

Kenny, J. (2016, April 3). BIM and cyber security: Defending the chain. Retrieved September 28, 2021, from ConstructionManagerMagazine website: https://constructionmanagermagazine.com/cyb5er-secu2rity-defend3ing-chain

Kerosuo, H. (2015). BIM-based Collaboration Across Organizational and Disciplinary Boundaries Through Knotworking. *Procedia Economics and Finance*, *21*, 201–208. https://doi.org/10.1016/s2212-5671(15)00168-9

Kerosuo, H., Miettinen, R., Paavola, S., Mäki, T., & Korpela, J. (2015). Challenges of the expansive use of Building Information Modeling (BIM) in construction projects. *Production*, *25*(2), 289–297. https://doi.org/10.1590/0103-6513.106512

Kiviniemi, A., Fischer, M., & Bazjanac, V. (2005). *Integration of Multiple Product Models: IFC Model Servers as a Potential Solution*.

Latiffi, A. A., Brahim, J., & Fathi, M. S. (2014). The Development of Building Information Modeling (BIM) Definition. *Applied Mechanics and Materials*, *567*, 625–630. https://doi.org/10.4028/www.scientific.net/amm.567.625

Lawson, H. (2015). Cyber threats to building automation and control systems. Retrieved September 22, 2021, from www.designingbuildings.co.uk website: https://www.designingbuildings.co.uk/wiki/Cyber_threats_to_building_automation_and_control_systems

LDAC. (2014). *Joint Workshop on Linked Data in Architecture and Construction (2nd LDAC worksh*.

Lee, W., Wong, A., & Tong, C. (2014). A Qualitative Study of the Software Adoption of Building Information Modelling Technology in the Hong Kong Construction Industry. *Business and Economic Research*, *4*(2), 222. https://doi.org/10.5296/ber.v4i2.6319

Leicht, R. M., Messner, J. I., & Anumba, C. J. (2009). A framework for using interactive workspaces for effective collaboration. *Journal of Information Technology in*

Construction (ITcon), *14*(15), 180–203. Retrieved from https://www.itcon.org/paper/2009/15

Lindsay, J. R. (2015). The Impact of China on Cybersecurity: Fiction and Friction. *International Security*, *39*(3), 7–47. https://doi.org/10.1162/isec_a_00189

Liu, Y., van Nederveen, S., & Hertogh, M. (2017). Understanding effects of BIM on collaborative design and construction: An empirical study in China. *International Journal of Project Management*, *35*(4), 686–698. https://doi.org/10.1016/j.ijproman.2016.06.007

Lou, E. C. W., Goulding, J. S., Alshawi, M., Khosrowshahi, F., & Underwood, J. (2012). Leveraging IT-Based Competitive Advantage: UK Industry Perspective. *Journal of Architecture, Planning and Construction Management*, 27–62.

Macdonald, J. A. (2011). *BIM - Adding Value by Assisting Collaboration*.

Mahamadu, A.-M., Mahdjoubi, L., & Booth, C. (2013). Challenges to BIM-Cloud Integration: Implication of Security Issues on Secure Collaboration. *2013 IEEE 5th International Conference on Cloud Computing Technology and Science*. https://doi.org/10.1109/cloudcom.2013.127

Mamun, M., Jenkinson, S., Hartwig, R., Davidson, S., Edahtally, J., & Jones, N. (2020). Project Security Provision – Baseline Security. In *Ukbimalliance.org*. Retrieved from UK BIM Alliance website: https://www.ukbimalliance.org/project-security-provision/

Mantha, B., García de Soto, B., & Karri, R. (2021a). Cyber security threat modeling in the AEC industry: An example for the commissioning of the built environment. *Sustainable Cities and Society*, *66*, 102682. https://doi.org/10.1016/j.scs.2020.102682

Mantha, B., García de Soto, B., & Karri, R. (2021b). Cybersecurity in Construction: Where

Do We Stand and How Do We Get Better Prepared. *Frontiers in Built Environment, 7*. https://doi.org/10.3389/fbuil.2021.612668

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251–266. https://doi.org/10.1016/0167-9236(94)00041-2

Martyn Denscombe. (2010). *The Good Research Guide for small-scale social research projects* (4th ed.). Open University Press.

McGraw Hill Construction. (2014). *SmartMarket Report - The Business Value of BIM for Construction in Major Global Markets: How Contractors Around the World Are Driving Innovation With Building Information Modeling*. Retrieved from https://www.icn-solutions.nl/pdf/bim_construction.pdf

McGraw, G. (2013). Cyber War is Inevitable (Unless We Build Security In). *Journal of Strategic Studies*, *36*(1), 109–119. https://doi.org/10.1080/01402390.2012.742013

Meadati, P., & Irizarry, J. (2014). *BIM – A Knowledge Repository*.

Meng, Q., Zhang, Y., Li, Z., Shi, W., Wang, J., Sun, Y., … Wang, X. (2020). A review of integrated applications of BIM and related technologies in whole building life cycle. *Engineering, Construction and Architectural Management*. https://doi.org/10.1108/ecam-09-2019-0511

Meth, H., Mueller, B., & Maedche, A. (2015). Designing a Requirement Mining System. *Journal of the Association for Information Systems*, *16*(9), 799–837. https://doi.org/10.17705/1jais.00408

Miceli Junior, G., Pellanda, P. C., & Reis, M. C. (2020). *Management Procedure for Sensitive Projects in the Context of a BIM Adoption in a Public Organization*.

https://doi.org/10.46421/2706-6568.37.2020.paper017

Miettinen, R., Kerosuo, H., Korpela, J., Mäki, T., & Paavola, S. (2012). An activity theoretical approach to BIM-research. *EWork and EBusiness in Architecture, Engineering and Construction*, 777–781. https://doi.org/10.1201/b12516-124

Miettinen, R., & Paavola, S. (2014). Beyond the BIM utopia: Approaches to the development and implementation of building information modeling. *Automation in Construction*, *43*, 84–91. https://doi.org/10.1016/j.autcon.2014.03.009

Mirahadi, F., McCabe, B., & Shahi, A. (2019). IFC-centric performance-based evaluation of building evacuations using fire dynamics simulation and agent-based modeling. *Automation in Construction*, *101*, 1–16. https://doi.org/10.1016/j.autcon.2019.01.007

National Cyber Security Centre. (2020a). *Cyber Essentials: Requirements for IT infrastructure*.

National Cyber Security Centre. (2020b). *Cyber Essentials: Requirements for IT infrastructure v2.1*. Retrieved from https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-2-1.pdf

National Infrastructure Commission. (2017). *Data for the public good*. Retrieved from https://nic.org.uk/app/uploads/Data-for-the-Public-Good-NIC-Report.pdf

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. https://doi.org/10.6028/nist.cswp.04162018

Navarrete, A. (2020). *User Requirements Elicitation: A Comparison between Generative Techniques and Semi-Structured Interviews*. Retrieved from http://essay.utwente.nl/85315/1/Garcia_Navarrete_MA_BMS.pdf

NBS. (2020). *NBS' 10th National BIM Report* (p. NBS).

Needham-Laing, M. (2016). Cybersecurity and BIM: what issues are being overlooked? Retrieved September 22, 2021, from Stevens & Bolton LLP website: https://www.stevens-bolton.com/site/insights/articles/cybersecurity-and-bim-what-issues-are-being-overlooked

Newman, C., Edwards, D., Martek, I., Lai, J., Thwala, W. D., & Rillie, I. (2020). Industry 4.0 deployment in the construction industry: a bibliometric literature review and UK-based case study | Emerald Insight. *Smart and Sustainable Built Environment*. https://doi.org/10.1108\/SASBE

Oates, B. J. (2006). *Researching information systems and computing*.

Office for Nuclear Regulation. (2014). FINDING A BALANCE - *GUIDANCE ON THE SENSITIVITY OF NUCLEAR AND RELATED INFORMATION AND ITS DISCLOSURE*.

Office for Nuclear Regulation. (2017). *Security Assessment Principles for the Civil Nuclear Industry*. Retrieved from https://www.onr.org.uk/syaps/security-assessment-principles-2017.pdf

Olatunji, O. A. (2011). A preliminary review on the legal implications of BIM and model ownership. *Journal of Information Technology in Construction (ITcon)*, *16*(40), 687–696. Retrieved from https://www.itcon.org/paper/2011/40

Oraee, M., Hosseini, M. R., Edwards, D. J., Li, H., Papadonikolaki, E., & Cao, D. (2019). Collaboration barriers in BIM-based construction networks: A conceptual model. *International Journal of Project Management*, *37*(6), 839–854. https://doi.org/10.1016/j.ijproman.2019.05.004

Oraee, M., Hosseini, M. R., Edwards, D., & Papadonikolaki, E. (2021). Collaboration in

BIM-based construction networks: a qualitative model of influential factors. *Engineering, Construction and Architectural Management*. https://doi.org/10.1108/ecam-10-2020-0865

Oraee, M., Hosseini, M. R., Papadonikolaki, E., Palliyaguru, R., & Arashpour, M. (2017). Collaboration in BIM-based construction networks: A bibliometric-qualitative literature review. *International Journal of Project Management*, *35*(7), 1288–1301. https://doi.org/10.1016/j.ijproman.2017.07.001

Orlikowski, W. J., & Barley, S. R. (2001). Technology and Institutions: What Can Research on Information Technology and Research on Organizations Learn from Each Other? *MIS Quarterly*, *25*(2), 145. https://doi.org/10.2307/3250927

Panas, A., & Pantouvakis, J. (2010). *Evaluating Research Methodology in Construction Productivity Studies*.

Papadonikolaki, E., van Oel, C., & Kagioglou, M. (2019). Organising and Managing boundaries: A structurational view of collaboration with Building Information Modelling (BIM). *International Journal of Project Management*, *37*(3), 378–394. https://doi.org/10.1016/j.ijproman.2019.01.010

Parn, E. A., & Edwards, D. (2019). Cyber threats confronting the digital built environment. *Engineering, Construction and Architectural Management*, *26*(2), 245–266. https://doi.org/10.1108/ecam-03-2018-0101

Pärn, E. A., & Soto, B. G. de. (2020). Cyber threats and actors confronting the Construction 4.0. In *Construction 4.0: An Innovation Platform for the Built Environment*.

Patel, H., Pettitt, M., & Wilson, J. R. (2012). Factors of collaborative working: A framework for a collaboration model. *Applied Ergonomics*, *43*(1), 1–26.

https://doi.org/10.1016/j.apergo.2011.04.009

Peffers, K., Rothenberger, M., Tuunanen, T., & Vaezi, R. (2012). Design Science Research Evaluation. *Lecture Notes in Computer Science*, 398–410. https://doi.org/10.1007/978-3-642-29863-9_29

Peffers, K., Tuunanen, T., & Niehaves, B. (2018). Design science research genres: introduction to the special issue on exemplars and criteria for applicable design science research. *European Journal of Information Systems*, *27*(2), 129–139. https://doi.org/10.1080/0960085x.2018.1458066

Petri, I., Rana, O. F., Beach, T., Rezgui, Y., & Sutton, A. (2015). Clouds4Coordination: managing project collaboration in federated clouds. https://doi.org/10.1109/UCC.2015.88

Petter, S., Khazanchi, D., & Murphy, J. D. (2010). A design science based evaluation framework for patterns. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *41*(3), 9–26. https://doi.org/10.1145/1851175.1851177

Pradeep, A. S., Yiu, T. W., Zou, Y., & Amor, R. (2021). Blockchain-aided information exchange records for design liability control and improved security. *Automation in Construction*, *126*, 103667. https://doi.org/10.1016/j.autcon.2021.103667

Prins, M., & Owen, R. (2010). Integrated Design and Delivery Solutions. *Architectural Engineering and Design Management*, *6*(4), 227–231. https://doi.org/10.3763/aedm.2010.idds0

PwC. (2020). *Assessment of the benefits of BIM in Asset Management Part 1 -Context and Methodology*. Retrieved from Centre for Digital Britain website: https://www.cdbb.cam.ac.uk/files/201117_uoc_req_2_value_of_bim_in_am_pt1_final

.pdf

Raziq, M. M., Ahmad, M., Iqbal, M. Z., Ikramullah, M., & David, M. (2020). Organisational Structure and Project Success: The Mediating Role of Knowledge Sharing. *Journal of Information & Knowledge Management*, *19*(02), 2050007. https://doi.org/10.1142/s0219649220500070

Redmond, A., Hore, A., Alshawi, M., & West, R. (2012). Exploring how information exchanges can be enhanced through Cloud BIM. *Automation in Construction*, *24*, 175–183. https://doi.org/10.1016/j.autcon.2012.02.003

Rezgui, Y., & Cooper, G. (2002). A Proposed Open Infrastructure for Construction Project Document Sharing. *Journal of Information Technology in Construction (ITcon)*, *3*(2), 11–25. Retrieved from https://www.itcon.org/paper/1998/2

Rezgui, Y., Wilson, I., Olphert, W., & Damodaran, L. (2005). Socio-Organizational Issues. *Virtual Organizations*, 187–198. https://doi.org/10.1007/0-387-23757-7_13

Rock, S. (2017). *Trant vs Mott MacDonald: BIM in court*.

Sackey, E., Tuuli, M., & Dainty, A. (2015). Sociotechnical Systems Approach to BIM Implementation in a Multidisciplinary Construction Context. *Journal of Management in Engineering*, *31*(1). https://doi.org/10.1061/(asce)me.1943-5479.0000303

Sanders, C. B. (2014). Need to know vs. need to share: information technology and the intersecting work of police, fire and paramedics. *Information, Communication & Society*, *17*(4), 463–475. https://doi.org/10.1080/1369118x.2014.891632

Saunders, M., Lewis, P., & Thornhill, A. (2019). Understanding research philosophy and approaches to theory development. In *Research Methods for Business Students*.

Sawhney, A., Riley, M., & Irizarry, J. (2020). Introduction and overview. In A. Sawhney, M.

Riley, & J. Irizarry (Eds.), *Construction 4.0: An Innovation Platform for the Built Environment*. Routledge.

Shafiq, M. T., Matthews, J., & Lockley, S. R. (2012). Requirements for Model Server Enabled Collaborating on Building Information Models. *International Journal of 3-D Information Modeling*, *1*(4), 8–17. https://doi.org/10.4018/ij3dim.2012100102

Shafiq, M. T., Matthews, J., & R, S. (2013). A study of BIM collaboration requirements and available features in existing model collaboration systems. *Journal of Information Technology in Construction (ITcon)*, *18*(8), 148–161. Retrieved from https://www.itcon.org/paper/2013/8

Sheen, R. (2015). The Problem with RACI. Retrieved March 30, 2021, from www.linkedin.com website: https://www.linkedin.com/pulse/problem-raci-ray-sheen/

Shelden, D. R., Pauwels, P., Pishdad-Bozorgi, P., & Tang, S. (2020). Data standards and data exchange for Construction 4.0. In *Construction 4.0: An Innovation Platform for the Built Environment* (pp. 222–239). https://doi.org/10.1201/9780429398100-12

Shen, W., Hao, Q., Mak, H., Neelamkavil, J., Xie, H., Dickinson, J., … Xue, H. (2010). Systems integration and collaboration in architecture, engineering, construction, and facilities management: A review. *Advanced Engineering Informatics*, *24*(2), 196–207. https://doi.org/10.1016/j.aei.2009.09.001

Shi, Q., Wang, Q., & Guo, Z. (2021). Knowledge sharing in the construction supply chain: collaborative innovation activities and BIM application on innovation performance. *Engineering, Construction and Architectural Management*. https://doi.org/10.1108/ecam-12-2020-1055

Silver, M. S., Markus, M. L., & Beath, C. M. (1995). The Information Technology

Interaction Model: A Foundation for the MBA Core Course. *MIS Quarterly*, *19*(3), 361. https://doi.org/10.2307/249600

Simon, H. A. (1996). *The sciences of the artificial* (3rd ed.). Cambridge, Mass.: M.I.T. Press.

Simpson, M., Underwood, J., Shelbourn, M., Carlton, D., Aksenova, G., & Mollasalehi, S. (2019). *Evolve or Die: Transforming the productivity of Built Environment Professionals and Organisations of Digital Built Britain through a new, digitally enabled ecosystem underpinned by the mediation between competence supply and demand*.

Singh, V., Gu, N., & Wang, X. (2011). A theoretical framework of a BIM-based multi-disciplinary collaboration platform. *Automation in Construction*, *20*(2), 134–144. https://doi.org/10.1016/j.autcon.2010.09.011

Smith, D. K., & Tardif, M. (2009). *Building information modeling : a strategic implementation guide for architects, engineers, constructors, and real estate asset managers*. Hoboken: Willey.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Steiner, I. D. (1972). Group process and productivity. In *Open WorldCat*. Retrieved from https://www.worldcat.org/title/group-process-and-productivity/oclc/445184

Stewart, P. (2015, October 16). An Overview of the BIM Process from an Irish Construction Project Management Perspective. Retrieved from www.bimireland.ie website: http://www.bimireland.ie/2015/10/16/an-overview-of-the-bim-process-from-an-irish-construction-project-management-perspective/

Succar, B. (2009). Building information modelling framework: A research and delivery foundation for industry stakeholders. *Automation in Construction*, *18*(3), 357–375. https://doi.org/10.1016/j.autcon.2008.10.003

Sun, C., Jiang, S., Skibniewski, M. J., Man, Q., & Shen, L. (2017). A literature review of the factors limiting the application of BIM in the construction industry. *Technological & Economic Development of Economy*, *23*(5), 764–779. https://doi.org/10.3846/20294913.2015.1087071

Taylor, R. (2013, May 28). Australian spy HQ plans stolen by Chinese hackers: report. *Reuters*. Retrieved from https://www.reuters.com/article/us-australia-hacking-idUSBRE94R02A20130528

Tse, T. K., Wong, K. A., & Wong, K. F. (2005). The utilisation of building information models in nD modelling: A study of data interfacing and adoption barriers. *Journal of Information Technology in Construction (ITcon)*, *10*(8), 85–110. Retrieved from https://www.itcon.org/paper/2005/8

Ulrich, P., Nilsson, A., & Smyser, J. (2015). *Improved Nuclear Security Through Effective Information Sharing*. Retrieved from https://stanleycenter.org/publications/pdb/SPCNSPDB315-19p.pdf

Underwood, J., & Isikdag, U. (2011). Emerging technologies for BIM 2.0. *Construction Innovation*, *11*(3), 252–258. https://doi.org/10.1108/14714171111148990

Underwood, J., & Khosrowshahi, F. (2012). ITC expenditure and trends in the UK construction industry in facing the challenges of the global economic crisis. *Journal of Information Technology in Construction (ITcon)*, *17*(2), 25–42. Retrieved from https://www.itcon.org/paper/2012/2

Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: a Framework for Evaluation in Design Science Research. *European Journal of Information Systems*, *25*(1), 77–89. https://doi.org/10.1057/ejis.2014.36

Volk, R., Stengel, J., & Schultmann, F. (2014). Building Information Modeling (BIM) for existing buildings — Literature review and future needs. *Automation in Construction*, *38*, 109–127. https://doi.org/10.1016/j.autcon.2013.10.023

Wilkinson, P. (2014, December 12). Behaviours4Collaboration. Retrieved April 1, 2021, from Extranet Evolution website: http://extranetevolution.com/2014/12/behaviours4collaboration/

Winfield, M. (2020). Construction 4.0 and ISO 19650: a panacea for the digital revolution? *Proceedings of the Institution of Civil Engineers - Management, Procurement and Law*, *173*(4), 175–181. https://doi.org/10.1680/jmapl.19.00051

Winfield, M., & Rock, S. (2018). *The Winfield Rock Report: Overcoming the legal and Contractual Barriers of BIM*.

Wilson, C. (2014). *Interview techniques for UX practitioners : a user-centered design method*. Amsterdam ; Waltham: Morgan Kaufmann.

Winter, R. (2008). Design science research in Europe. *European Journal of Information Systems*, *17*(5), 470–475. https://doi.org/10.1057/ejis.2008.44

Wix, J., & Karlshøj, J. (2010). *Information Delivery Manual Guide to Components and Development Methods*. Retrieved from https://standards.buildingsmart.org/documents/IDM/IDM_guide-CompsAndDevMethods-IDMC_004-v1_2.pdf

Wong, J., Wang, X., Li, H., Chan, G., & Li, H. (2014). A review of cloud-based BIM technology in the construction sector. *Journal of Information Technology in Construction (ITcon)*, *19*(16), 281–291. Retrieved from https://www.itcon.org/paper/2014/16

Yang, Q. Z., & Zhang, Y. (2006). Semantic interoperability in building design: Methods and tools. *Computer-Aided Design*, *38*(10), 1099–1112. https://doi.org/10.1016/j.cad.2006.06.003

Zhang, C., Beetz, J., & Weise, M. (2015). Interoperable validation for IFC building models using open standards. Retrieved March 30, 2021, from research.tue.nl website: http://www.persistent-identifier.nl/?identifier=URN:NBN:NL:UI:25-801767

Zhang, J. P., Liu, Q., Yu, F. Q., Hu, Z. Z., & Zhao, W. Z. (2014). A Framework of Cloud-Computing-Based BIM Service for Building Lifecycle. *Computing in Civil and Building Engineering (2014)*. https://doi.org/10.1061/9780784413616.188

Zomer, T., Neely, A., Sacks, R., & Parlikad, A. (2020). Exploring the influence of socio-historical constructs on BIM implementation: an activity theory perspective. *Construction Management and Economics*, 1–20. https://doi.org/10.1080/01446193.2020.1792522

10 Appendices

Appendix A – Research Interview Transcript Excerpts:

Appendix A.1 – Excerpts Table for Participant A1:

Excerpt	Excerpt Content
A.1.1	"I think to me the bit on that trust element because the collaboration needs trust from both sides you need the openness you need to have that trust that you could open yourself and the information up to these people and it will be used for… what it's intended for and it won't be used against you in effect but will be used… and I suppose I used that term against… - rather than in a confrontational way it's the fact that collaboration is that we're all aiming for the same end point."
A.1.2	"The trust aspect I'd just add to that it is there's two aspects of it – of course, there's getting things done efficiently but also certainly from security point of view, you need to trust people, that people in the end… that closer collaboration with them means you can have a much better understanding and rapport with the people - certainly you can get a much better chance to understand whether you do or don't trust them because of their behaviours".
A.1.3	"… in a way the principles of collaboration and security are pulling different ways - what's key for security is the 'Need to Know' principle - but part of the focus of BIM is actually perhaps because people have got information we thought that they didn't need to know, they've been able to make better decisions for the project - you really have to have huge amounts of foresight to understand what people 'actually' need to know. Some of the more 'subtleties' of what people need to know and share are

	actually more difficult to identify, and so that is something that needs to be looked at…”
A.1.4	“…One of the issues of the approaches of identifying the need to know is just being able to understand throughout a wider context of what information people in the BIM and design world actually require …”.
A.1.5	“I think that would be a positive step especially because we’re breaking it down into that task and element level, so - ‘you’ve got something to do’ - so there’s a need for you to know certain information – so, ‘what is the information that you need?’ and ‘what classification is that information?’” … “… my comment would be it needs that foresight, that planning - so once you start doing that in a more well defined manner, from a security point of view it’d be an improvement not a reduction, because you’ll have put more thought into what it is that *you know* into what other people need to know, which perhaps at the moment there’s room for improvement.”
A.1.6	“…and I think building IFC into that, there’s that potential to automate it and that puts you on a virtuous circle - so you’re not able make the exchanges unless you have thought about it whereas in the manual way, actually you can start sharing whilst not thinking about it which is a negative regarding security - but if you’ve automated it and therefore you possess control over it and say ‘look for this system to work we need to assess the information so that we can understand who can and should have it versus who can’t have it.’”

Appendix A.2 – Excerpts Table for Participant A2:

Excerpt	Excerpt Content
A.2.1	“I expect the explosion of data that we’re going to see in the next few years, I wouldn’t even like to put a number on it but it’s going be absolutely huge, so we need the right workflows – the right sorts of systems to manage that data”.
A.2.2	“Another project (rail) I know of is really struggling now that they’re at the commissioning phase because from what I understand, they’ve not implemented BIM and managed the information on their assets as well as they should have. Now that they want to bring that information back together to do various things with it, they’re finding it very difficult”.
A.2.3	“Yeah, we’ve got mechanisms that incentivise for the inclusion of the lowest level suppliers, encouraging the use of small and medium enterprises, they’re incentivised to take on apprentices, innovate all of that stuff - because it’s no good doing it at the top level and the primary contract arrangement if you’ve got a supply-chain that’s really long. You’ve got to get it to the lowest common denominator, don’t you?”.
A.2.4	“If I was to look at that scenario (A13’s example), I would look at whether some of those steps were unnecessary. It sounds to me that it was a hierarchal authorisation process rather than being made by people who are actually informed decision makers. In my previous role, if somebody said to me ‘Designer X needs access to the system – do they have permission?’ – I’d go ‘yeah okay.’ - I wouldn’t know whether to say yes or no. I think that’s where waste probably does occur when you get organisational authority levels as opposed to local authority levels. it’s a different type of decision it’s not (upper) hierarchal it’s technical.”

Appendix A.3 – Excerpts Table for Participant A3:

Excerpt	Excerpt Content
A.3.1	“One of the things I’ve seen here is saying things like it’s a ‘Secure Document’ so you can’t print it out and share it - but if it’s a drawing that someone needs to use for their bit of the design, how are they going to if they can’t even print it out. So, it’s a lack of common sense, the industry tends towards putting at a higher security then it possibly has to be, to cover their ***** (sic) - but actually it stops people working because it’s not a sensible security level. I mean we’ve seen here that during the design everything’s protected - and then they go ‘You’ve got to go build it’, ‘Oh **** (sic), we’ve got to go make it non-protectively marked to actually print it out’ and it’s like well if you had to make it non-sensitive in the end, why was it sensitive within the rest of the process, like was it a security risk? Or did you just not know, so you just went and defaulted to the highest security-level?”.
A.3.2	“I think it’s used as a bit of an excuse to not do anything. If you take the example we’ve just talked about where if not all the information is actually protectively marked, then why can’t people from two different companies who both have the same level of access and clearance share that information. It certainly shouldn’t stop people within the same organisation from talking and sharing with each other and it’s just identifying and applying more granular levels of what is and what isn’t a security-risk with a bit more common sense I suppose. Just saying I can’t share anything because we’re in this sort of environment I think is a big ‘Get Out’ and bit of an excuse for not doing anything and not change behaviours. I think nuclear thinks it’s a bit special when actually there’s probably technical ways around these things.”

A.3.3	"Collaboration to me in its simplest form is getting people to work together and be open and honest about what an issue is when it occurs. People working in construction, everyone's got their little job to do, and everyone sits in their office with their door closed and everyone's ready to blame someone else and make it somebody else's problem. So, it's not thinking that it's someone else's fault or problem, shutting your door and leaving everyone else to get on with it. It's about people being more willing to work together and share the information they've got to help the design as a whole - not just their little closed-door empire - but some people are naturally closed off, especially if they think that you're trying to pry at what they're doing, even if someone else ends up redoing that work because someone wouldn't share their work. It's that kind of behaviour that collaboration should address where people are comfortable to say – 'This is what I'm doing', and let others see it instead of everything being hidden away because often there's a lot of information out there that people on the project team don't know exists, or if they do, they wouldn't have a clue to where to go and find it."
A.3.4	"…so as soon someone logs in, they're like 'Well this is rubbish' and even if it does exactly what you want it to, the team-members are put off by the fact that it doesn't look and feel easy to use. If you talk to the software developers about it, they'll say 'Yeah but it doesn't need to look nice'. No for it to technically work, it does not need to look nice - but to get to people to want to use it and not have to do 20 clicks extra when they want to get there in 2. You're putting people off by making it more onerous for them then it would be to use an alternative like dropbox."
A.3.5	"Trying to get people to understand that you can't send critical design work through email is difficult because people seem to be like - 'Ah whatever, we use this all the time and nothing happened', and as a PM:

	‘Yeah but you know if someone really wanted you can go and get that out of dropbox - they would find a way’.
A.3.6	“I think you’d end up with the stages of design for different stages and then you’ve got you know estimating you need a relationship there between cost management and design, and then okay well what’s the next – so that’s well concept stage or brief stage and then you go to the next stage and it’s like ooh outline design – well that means designer 1 is going to have to talk to designer 2, and then okay what happens at the next stage well designer 1 and designer 2 are now going to have to talk to specialist (for) contractor 3 and then have to work out all those relationships funnel off and I imagine you’re going to start off with a small number of big stakeholders and at the kind of concept brief stage, by the time you’re going through design stages, you’re going to have all these smaller tasks all linking off and all these smaller groups of people doing things branching off of each other – visualising it would be quite fun, there’s a big tree that goes out.”
A.3.7	“That’s something we need to get in place that you can quite easily say ‘well actually, that bit there, if this person looks at it, they’ve got top clearance so they can see everything that’s in the building down to every pipe’. If that was the groundworks contractor, all they need to know is - ‘There is a building here, and you can’t work there because somebody else is there’ - They don’t need to know the inner workings of it. At the minute because you haven’t got that granularity within most BIM platforms, you either see the design or you don’t.”

Appendix A.4 – Excerpts Table for Participant A4:

Excerpt	Excerpt Content
A.4.1	"… they were talking about a leaked document to try to highlight some serious issues, but they showed the front cover of this leaked document, and the marking on that document was quite clear in that it was the lowest classicisation that you can have. It had been given a classification however - so they'd portrayed it to be this highly sensitive, highly critical information. The information itself was of no concern, but the attempt to use it to cause reputational damage - Very high – and that is the problem that we have. It's what people say it contains that causes reputational problems. So we protect all of our information to some degree because of that reputational damage that can be caused."
A.4.2	"… people will come back and say: '*Well I know it says it's sensitive, but it must be incorrectly marked, it's really benign*.' - That's not the point, the content could just be what I'm having tea for tonight, but it's the fact that it's been classified that it has to be protected in accordance with the classification group, regardless of the content to protect us from damage. So if somebody classifies information then it has to be treated and handled in a specific way. It's not up to the person who receives it or the person who is looking over it to say: "Oh, I know it says this, but I don't think it is, so I won't protect it as if it is a sensitive document". If the author has classified it in such a way, there's a reason for it, and that's how it must be handled."
A.4.3	Obviously with digital systems, GIS for instance as a graphical interface system, it's great in the application that you can click on a building and find out everything there is to know about it at a click of a button. But from a security point of view you might not want to make it quite that easy to find out exactly everything that goes on in a building in terms of

	quantity of materials. So you can sell the idea to our executive and say - *'Look we've got this bit of software that can pull all this information together, you can manage your dashboard and everything.'* Your exec will go *'We definitely need that.'* - but then when you put your security layer over it, we would step in say – *'Well hold on, do you really want to make it that easy to visualise everything?'* and they say - *'Well maybe not.'* - We never say they can't, and it might be that they do want it to happen in which case we would try to enable it in the appropriate environment so that they can do securely. But it may increase the cost of delivering that type of service. So the business need or desire may not be quite as strong once they realise how much the security cost will add to it."

Appendix A.5 – Excerpts Table for Participant A5:

Excerpt	Excerpt Content
A.5.1	"…well, it depends on what the client is saying and the requirements they should be putting forth. Ultimately, anyone on the delivery side such as the project manager will have a role on the job to do deliver the asset, and then they will walk away once it's done, so they or anyone else haven't got a liability if anything gets out. It's up to the client to really think and plan through: *'Right, I'm going to be in this building for the next 100 years, who do I want to know about it?*"*.*
A.5.2	"… as soon as you involve more people, more systems and there's more sharing, there's greater potential for the wrong person to get access to the information. So as the project scales and the information scales, so do the risks. You can only ever manage them, you can't make the risks zero. You'd not share anything with anyone…"
A.5.3	"**...** whilst professionals have a rough idea of the kind of information that's going to be shared by other people on the project, they don't know the nature of it specifically for that job and what it's actually going to look like. So we know that there's going to be some outline designs, some detailed design…some production design around security cabling. We put it into our matrixes, but there are things that we can't predict, things might change, and some of the plans might not be detailed enough for what information we actually need, so we will need to make an application to change someone's status either for our professionals or another party. Ideally, we want to have properly defined what information you're going to need in order to do what. And the people you're going to have on the job to undertake that work. And then you can start work out who needs access to what. The problem is the governance around all this. There's some governance there but it's poor, there's a lot of work to still do here."

Appendix A.6 – Excerpts Table for Participant A6:

Excerpt	Excerpt Content
A.6.1	“What we need to do is to get senior level people in organisations to recognise that it's not just flashy designed models - it's actually better asset information management procedures that give you an Information Model which will both be safer, more cost effective, it will have better assurances on delivery... but also it will give you better security and will create opportunities and assurances for the owner in the future. But trying to get that level of thinking in senior stakeholders is quite challenging especially when they've got a lot of day-to-day pressure.”
A.6.2	“You're fighting the marketing teams of big software vendors. One of the enterprise asset management vendors said recently: 'Buy our product and you can do ISO 55000' which is absolute rubbish, but they've got a marketing team - they've got lots of flashy collaterals putting out those messages. Trying from a good business governance perspective to get across that actually: ***'This is about better management of information, it's about avoidance of risk, it's about managing sensitive information and sensitive assets better'*** - but we don't have that level of clout yet to get that message across the same way.”
A.6.3	“If the project is starting to think about security but it isn't part of the procurement spec then they're going to be quoting something that there's no recognition of its value or sensitivity. If the procurement team haven't got any executive buy in, they're just going to come up with costs - if you think Grenfell Tower fire, people trying to save money on cladding costs - not thinking through the unintended consequences. What they ***are*** thinking about is: *'Are you sure we need to spend all this money on security models and all that? We'll do it for 50 Grand instead of a quarter of a million that you're saying it should be'*.

	They’re not thinking it through, so it has to flow down from the senior level - from the accountable people within the organisation.”
A.6.4	“One of the professional disciplines I am quite critical about is procurement - there’s too many cases where you have a procurement professional who is an itinerant individual - they spend a year or two with a client - run a big procurement project - at the end of it they get paid their bonus because they've made an ‘X percent saving’ on the overall purchase cost, and then they scarper. Meanwhile, the poor organisation is left with the consequences. Unfortunately, they are far too many of them in the procurement world - trying to educate them to think about that: *‘Actually you need to think about security within your requirements.’* - they aren’t going to get it - it's got to come from the clients, it's got to come from the exec of the client organisation saying: *'We understand we have got an infrastructure here that has sensitive assets with it. It has sensitive systems and we've actually got some IP that we don't want to lose. Therefore, we need to treat it appropriately...'*”
A.6.5	“If somebody gets fined for exposures - that will wake people up. One of the reasons why GDPR is starting to be taken a little bit more seriously than the data protection act for many organisations is the level of fines. Supposedly, there was a proposal that the ICOs office was self-funded from the revenue they've gained from fines, from the breaches they've discovered…” … “If the ICOs office were also considering security, the fact that not only have you let out some personal information, but also some sensitive enclosed information about CNI, therefore you are going to be fined X number of things. That will wake people up. It's got to be a mindset; it's got to be the executive board that has to recognise: *‘This is an accountability we have got. We cannot shirk it. If we get it wrong, that is potentially the company gone.’*”

A.6.6	“It's also about accountability as well as skillset - so if you have an organisation that has a chief information security officer (CISO) - even if that person doesn't know about everything about hardening SCADA (supervisory control and data acquisition) systems to make them properly resilient - at least by having somebody at sea level - talking about information security - you're heading within the right direction - and it's more about having that recognition and understanding - If you're an organisation who's got a chief information officer who just thinks about the technology, not about the data or the security then as an organisation, you run the risk of creating decisions or setting projects up which are probably not appropriate for what you really need.”
A.6.7	“…there's a health-care project, one of the challenges they’ve got is that its way off being a normal ‘Building’, yet the employers have no AIRs, it had an EIR based off of nothing and nobody knows how to deliver what they're after. So, it stems from the client not having enough information about what they should have in place to make sure the job is done right. I think client / asset-owner awareness is probably more important than contractor or supplier awareness - if they’re are fully aware of the security and BIM angles and the rest of it, and they put everything into their bid - but somebody else doesn’t, then they're going to lose out on the cost-basis - that will happen if the asset-owner doesn't recognise and put what they need in their requirements - so it's got to be down to asset-owners actually need to understand what do we need to do.”
A.6.8	“There’s a trend of usability of CDE security-models that I’m a bit concerned about - If you take the scenario of a painter who only needs about 40% or so of the model, but there's a lot of the model he / she doesn't need to have access to – how much admin overheard to actually get the security permissions set correctly, and how intuitive is the setting? My concern is whether the functionality is user-friendly enough

	way to make that happen in the way it's needed. So, a change of role is a classic one, somebody doing a particular role, they get changed from being a project admin on one bit of the project, move on to somewhere else, they get given permissions for the new bits of the model and then nobody actually goes back and closes down access to the old bits of the model that they should no longer have access to. There's a wakeup call to vendors that they need to think more carefully about how they implement their security models and how easy they can make it for somebody to get that clearance to different parts of the model and also to change that permission".
A.6.9	"So putting everything in one place gives you that better view of the overall coordination, however it then creates a security risk. Now, you can within some CDEs define strict security models that prevents people browsing and looking at models they shouldn't have access to. One of the areas I've not yet seen properly demonstrated is: if you've identified there's some sensitive assets in that shared design model, and you want to indicate there is something that is there - but it is not something you (i.e. actors) should need to know about - how do you do that without it being almost like an ancient medieval-map where it says, 'here be dragons'."

Appendix A.7 – Excerpts Table for Participant A7:

Excerpt	Excerpt Content
A.7.1	"…the people who were getting the background data - they didn't check it - they just copied whatever was available - and said: *'Model that in 3D for us.'*" … "so, another group started going through all of these sheets, and individually, some of the things didn't make any sense. There were lines on paper with nothing else around them, which didn't seem to connect to anything. Then they got the CAD files and all you did was reference them all together and all of a sudden you got this great big model of the asset that indicated quite a lot of information that you probably shouldn't know about".
A.7.2	"…for the CAD management process we had to produce the core fire safety plans - a very well detailed drawing that even an idiot could read it and understand where the doors are, where the fire escapes are, basically where all the choke-points in the [asset] are - you don't have to be clever to understand where these things are…" "… but those files - they showed the rooms and entrances you wouldn't publicly see - that information, nothing classified about that - anyone could take that data".
A.7.3	"It's their choice but we don't tend to encourage suppliers to use their own systems - because if we are the coordination body, then suppliers should have no issues with collaboration from information points of view. If they manage their own systems, it's at their whim who they share data with, who they integrate with, or work closer or lesser so. It *can* work - not saying it doesn't - projects around the world have all worked that away, but there is always a known issue around the collaboration aspect, there is always a cost impact and the programme delay from the actual delivery of the project, just because these companies whatever reason at any time they might go *'you know what, I'm not giving you access.'* and that has happened recently …(the injunction)"

Appendix A.8 – Excerpt for Participant A8:

“Half the problem is that you might have all the technical stuff to apply various types of access control but if you've not figured out the policy to say: ‘what parts of the BIM model you want exposed to what roles?’ Then even if you've got the ability to set those controls it may not mean that you will have set them up appropriately - and another problem I think with BIM is that it's not straightforward to map individual roles of work to specific parts of the building that people should see and parts that they shouldn’t- so the default in many cases will be for everybody to see everything - which obviously increases the risk.”

Appendix A.9 – Excerpts Table for Participant A9:

Excerpt	Excerpt Content
A.9.1	“I think the difficulties are people understanding why they need to work in this way so - so that you know when you go on to a secure site that you have to behave in a certain way but because people are working remotely in their offices they don’t take that same - they don't understand that behaviour concept, it's not just related to physical presence on site but it's there throughout the project no matter what it is you're doing in respect of the project and that's difficult and making sure that people manage their systems properly and their hardware properly. All of those things are quite challenging, and I don’t think - you can't guarantee it, you can just do what you can to understand where the risks are and try and manage them.”
A.9.2	“I align it to this idea you would never give a contractor a piece of paper that says build me a house and expect to get it, so why do we give people very scant information about how we expect them to work and how information should be managed. I think we definitely need to be more concise and meaningful when it comes to our information-requirements”.
A.9.3	“…so, you have to think what is more important - is it that you can generate and share all of this buildable data from a model or is it that you can protect some of the information, but you've still got just enough there to enable you to start coordinating? That's the pragmatic approach we've had to take - so we can look at models and some elements of them are highly detailed and some elements aren't - but we know that the

	geometry is correct, and we know that we can co-ordinate with other people on the project.”
A.9.4	“It's difficult because you're trying to figure out what information ‘you’ believe they need to know. Then at the same time you're also doing that in mind of their security clearance, not everybody will be security check cleared and there's a lot of reasons for that, but you have to work with that in mind when you’re making these decisions.”
A.9.5	“…so it identifies what are the project activities that you need to complete and then it says ‘well have you thought about this particular aspect of the information requirements...’ things like ‘have you established who will be contractually committed to the model data and information requirements’, ‘are the model data and information requirements agreed to the party to be appointed’, ‘have you included your PLQs and your information exchange program, your model production, your delivery table…’, it's all of these things so it's intended to capture quite a detailed process.”

Appendix A.10 – Excerpts Table for Participant A10:

Excerpt	Excerpt Content
A.10.1	"…there is a supply-chain that has built and manages that (specific sensitive-asset), but I think because BIM is forcing people down the route of collaboration, there's this kneejerk reaction from the rest of the industry, that 'oh my god, we're sharing sensitive information, we're going to cease to function, we can't do this.' - now frankly… we have been doing this for some considerable time but it's because the supply-chain that does that is very, very small and we are now forcing the rest of the industry down a route they've never been down before, and the people that know how to do it are few and far between…"
A.10.2	"It's what checks, balances and measures - whether they're procedural or technical you put in place to add these layers of security. So, think of it as an onion, and your sensitive information, assets or IP as the core of the onion. Then you put layers that wrap around each other in encapsulating whatever the sensitive asset is - and the more layers you add, the more difficult it is to get to the core - thus the more difficult it is to get through to the sensitive assets. Putting in those layers means you have to think about everything from policies and procedures to do with training and people, to technical solutions - whether that's the various procedures you can adopt to have good cyber-health - or the policies for physical protection that you have around that data. From a programme point of view, it's making sure the programme team is set up correctly, through to what contractual arrangements are in place that hold the supply-chain to the owner should they lose data. It's thinking about how you can set up those layers so that it has the right IT infrastructure, technical solutions and systems that enable them to work collaboratively but also mitigate the risk of data loss or data-theft, that could be anything from knowing where your data is stored to your anti-virus and firewall solutions, to your network connectivity, your password policy etc. Getting all that in place means working with business resilience, its working with the operational team, IT, HR, it's working with all these different people so that the project is set up so the myriad of consultants and suppliers are brought into a project environment which has been defined with the right layers of security and collaboration wrapping around it, so that people can then work collaboratively on that asset. That's the key thing, it's being able to function, to work collaboratively, being able to discuss, to share etc but in an environment with the right layers of security to mitigate data loss and breaches - so the way of working securely, collaboratively is already set-up, so we're not introducing change and tension as the programme grows."

Appendix B – Validation Transcription Extracts:

Appendix B.1 – Excerpts Table for Participant B1:

Excerpt	Excerpt Content
B.1.1	“So, when you think about the harm that could be caused to children, schools are arguably the need for the most protection in the world, the school to me is one the most insecure environments and one that we should be really protecting. But the ease within which they can be accessed via a school… and that relates to a note I made on: ‘Have you thought about the impact of Social Media?’. So that’s also things like 'We're all very happy to sell our houses online’, but if you go and look at a really high value property online and look at the plans, you can work out a lot about that property, and I think we have this issue... it's this... environment within which we operate our lives, where we'll more or less share everything - we're unable to distinguish what's going to cause problems…”
B.1.2	“We're also having to get up to speed with digital working, with modelling, with working within CDEs, with lots and lots of things, and so there's a lot for industry to deal with - So it's not like we're all skilled modellers, skilled sharers of information, that we know the correct file-naming off by heart - we are having to get to grips with all of that - and at the same time think about, ‘well how do we do this in a security-minded way?’”.
B.1.3	“… and it comes back to the burden of administration, one of the things the PAS said was that the information-management ‘activity’ was intended to be just a part of somebody's job as an architect, or as a surveyor or as an engineer - and that presented a message it was relatively straightforward and easy to do, but actually - it's Not.”
B.1.4	“… having a security-minded approach is extremely burdensome in terms of administration. When you're getting into the depths of the supply-chain and the commitment you call of them. When you start getting individual people, not even organisations - but individual people to commit to psy-ops forms, or non-disclosure agreements - then that

	becomes an administrative overhead. Also, particularly within the current environment we've been in now for 10 years, it's the commercial impact of that administration. So, all of a sudden, projects become more difficult and less commercially attractive...”.
B.1.5	“So we try to have very clearly defined information-requirements to develop cost-plans - but if I say ‘Right I'm going to produce my first cost-plan and that means I'm going to need that from you, and that from you and that from you.’ - when that doesn't materialise - I'm going to accept that it doesn't materialise, because there's not very much I can do to influence that situation - other than probably shout a bit louder - and so we make cost or time allowances for everyone else's shortcomings…”.
B.1.6	“…I think that it is intended that we now get into it at a more granular-level, but even as a task-team - you determine that these are your information-deliverables - that doesn't really equal – ‘So that means we understand what our information-demands are now - does it?’”.
B.1.7	“I think the big thing for me is what point in time does information get context attached to it, and I think it's that, that determines - what its vulnerability is really - because in some ways I always think of it - as, it's trying to find a very specific needle in a haystack - sometimes, there's so much stuff there... that it's...”.
B.1.8	“You do need more granular responses to a PLQ, - but there are multiple activities going on to answer a PLQ aren’t they - so if your PLQ is: 'What's the forecast life-cycle cost or whole life cost of this project at the end of stage 3?’ - then you've got to have - there's lots of different information-requirements feeding into inform that - there's a certain level of design (information on the design) that you've got to understand...”.
B.1.9	“You might send off some information at concept stage to a task for a given purpose - and the same information might be needed later on for another purpose - but it's actually changed because it's been refined. So, I think you would want to know where that data has gone to if you've now changed it - so you could then work out if you will need to push it again to where it went to in the first place or if it's just historic now and doesn't matter… I'm thinking going from concept into a more detailed design phase...” … “So, I think you need to be able to look at it from different directions - so as an originator of this piece of data - where did it go off to

	- what was the status of that data - you know how how reliable was that data? - and then if it becomes more reliable, or if it changes slightly - then being aware of 'do you have to push it off in exactly the same directions, or does it not matter?. So, there's that forward look and also there's also that if something down the line changes in other stages - what does that impact... so you need to have that directionality going against data from those perspectives."
B.1.10	“My thoughts on that side of things are it would work best in either a pure design and build situation - or a purely traditional situation - where roles and responsibilities are very clearly defined. So, the scenario a lot of us work under at the moment is some sort of quasi design-and-build, two-stage - or traditional, with design… - I think you start to get a blurring of responsibilities… – so you either need that very clearly defined (responsibility-structure) - or you have the ‘Collaborative Insurance’ backed way of working… - because with the Collaborative Insurance and Integrated Project Insurance - you can afford for the lines to be blurred, can’t you - because it's the project that's insured, and you work together as a team to resolve the issues...”

Appendix B.2 - Excerpts Table for Participant B2:

Excerpt	Excerpt Content
B.2.1	"So these aspects of information exchange - how we deal with... data as an asset or data as something that people will look at as things that they must be aware of and know how to contribute towards - in a proactive way - well, it comes down to culture as well as the competence to implement that effectively in an organisation - that say perhaps is earlier within its lifecycle then more mature organisations. So, I think that might be an area - you might want to assess as to, whether the maturity of an organisation affects the way these blockers evolve or if they function differently across it".
B.2.2	"… I created templates for my discipline with known-inputs factored in from other disciplines - but for every other discipline, although they had a sense of what's required to and from them, and it's in everybody's minds as what to expect… - it wasn't articulated…" "… so, there's all sorts of things that people intrinsically know when they're approaching design activities, but no one is properly articulating it and saying: *'I will need this information at this point in time - for this purpose.'* - it's more like: *'Well I know I need it... and it might be coming...'* but then they might have a conversation and go : *'Oh, it's not going to come so we can't do it anymore…'*".
B.2.3	"I guess it would work if the development of that matrix is done with everyone's buy-in, it's almost like a business requirements gathering - to say that: *'Well because you asked for this... - this is what that means - and therefore this is what you will get from this person, so that you can deliver what you need to deliver."*
B.2.4	"I suppose it would be beneficial for this network to look at this also in terms of what the assets are, and their interdependencies - and then relate the flow of information for the particular aspects of the asset - right from the first ever transaction, - so it creates an audit-trail - and then effective version-management and configuration would help the **flow** of said information at that level from organisation to organisation - but it would also help to look at what **happened historically** - because - you have: (1) the nomenclature of the final task, it's almost like categorising animal-species - you've got a taxonomy, you've got different variables, or different

	grades of gradation of the same sort of one species - but then: (2) you would be able to trace how that came to be of the evolution of the species - so it's almost like that... I know, biology is a bit of a weird example but it’s to say you could track how tasks would evolve…”.

Appendix B.3 - Excerpts Table for Participant B3:

Excerpt	Excerpt Content
B.3.1	“The information that’s shared is based on what’s sat in the standards (e.g. BSRIA) - so the client, i.e. the ‘receiver' in this case is being told what information they should be getting. That is also what’s likely leading to some of these strange (push and pull) hybrids because the suppliers read the guidance and say 'Ok, well, this is what I need to push over then.' and the client is then saying, 'Ok well, this is what is being given to me' - what they are not saying however is ‘This is the specific information I need.’”.
B.3.2	“A big issue we've got at the moment is the 'Design-Stop' where someone says, 'That's it - I'm at the end of Stage C - we're not doing anything else.' - so the changes they’re making in certain areas of the building they don't want us to see won’t come through …” “…the conversation always stops at 'No'. People feel because they’ve got their standard contractual obligations - they can just turn around to say: 'Well, at this stage and level, this is all we need to provide.' - irrespective of what is actually needed.”
B.3.3	“I mean, you would need to have an absolute understanding of, and it's as much as anything, it's ‘what people need to know?’, so it's understanding just simple things at a very granular level - so somebody needs to know that the plasterer is going in, and he's using that higher grade plaster - so that's going to add thickness to the walls, or it's going to draw in more paint because then the decorators going in and needs to use more paint to get a full coverage of that wall - that's such a big, big kind of piece that when it spans out” [B4: “And it evolves as well”.] “B3: Yeah, it evolves, all the time - yeah.”

Appendix B.4 - Excerpt for Participant B4:

“… right across industry - BIM became something for people to make a name for themselves on, rather than make a business and an industry efficient - **and a lot of people came in and made a lot of promises - a lot of them weren't delivered upon**, and some of the problems in terms of knowledge on BIM and security is the whole **'Once bitten, twice shy.**' - because people have been damaged by these early interactions with things that were wrong. So, when the BIM consultant has ‘up and left’ - it's up to the rest of the team to try and bring in later, not these one’s specifically, but these kind of security protocols and initiatives you’re talking about. I think the issue and question at the moment is, ‘Could we have got it down 10 years ago?’ - and it just would have solved so many problems - but obviously it doesn't make any of this work any less needed.”

Appendix B.6 – Excerpts Table for Participant B6:

Excerpt	Excerpt Content
B.6.1	“So the fact that the **pull** comes from the **need-to-know** part and therefore I’d say, the fact that the **need to share** keyly **comes from** the need to know – maybe it’s just showing that one has the primacy - and almost the chronology in effect isn’t it, in that the need to know comes first….” “…So, I'm thinking the concept diagram is related to the design-process flow of say - ‘This is what happens when architects go and they'll pass to the structural.’ - but I suppose the concept you're talking about is that ‘Well that's fine for the design-process but actually, what’s key for information-security is that requirements should start with the need-to-know principle, the pulling-side first. It does put the entire approach on its head a bit doesn't it…”
B.6.2	“My thoughts are that yeah I support it – it sounds like a great idea, just need to work through some of the practicalities of how it would work on a live project – but certainly the network of requirements - that's a really - I'm really supportive of that - and I think - that it goes wider than just security - I suppose because you know in the construction industry... our processes aren’t mapped properly, so yeah - that would be a big huge step - and especially when we're talking about moving technology into it - you need to... the sector needs a standardised approach so we know that we're talking about the same processes in the same way - so yeah - I think that's opening up a big door of lots of things to do, probably outside your research - but I think it's good - the other side is that yeah that's fine for all the other things to do but I think for security it's definitely the way forward.”

Appendix B.7 – Excerpts Table for Participant B7:

Excerpt	Excerpt Content
B.7.1	"…a supplier had demonstrated that this is how we can visualise all of the viewing angles - and so they rang up the group concerned and said, 'Were you aware that your CCTV camera viewing angles are visible on the internet?' and they said 'Well we knew that PR were doing some publicity, but it was all anonymised - we didn't know that it was us (specifically)' … - 'So how come I'm ringing you then?' - And so, the issue is that there's all these different things that people need to think about - and it goes back to your point on your security-incognisance - it's about people that are digitally competent - but maybe they're not security-minded."
B.7.2	"I think the other thing to think about, is in terms of the network, you talked about shared, and published - I think there is a risk that... - making information available too early, it might mean it is still... not fully signed off - and there is a risk that it will change... - however, giving an early sight of something may mean that somebody can start doing some indicative planning ready for their task - and I think there is a bit of a tension there, that needs to be reflected that... making information available early can enable some opportunities but may also present commercial risks if not properly managed."

Appendix B.8 – Excerpts Table for Participant B8:

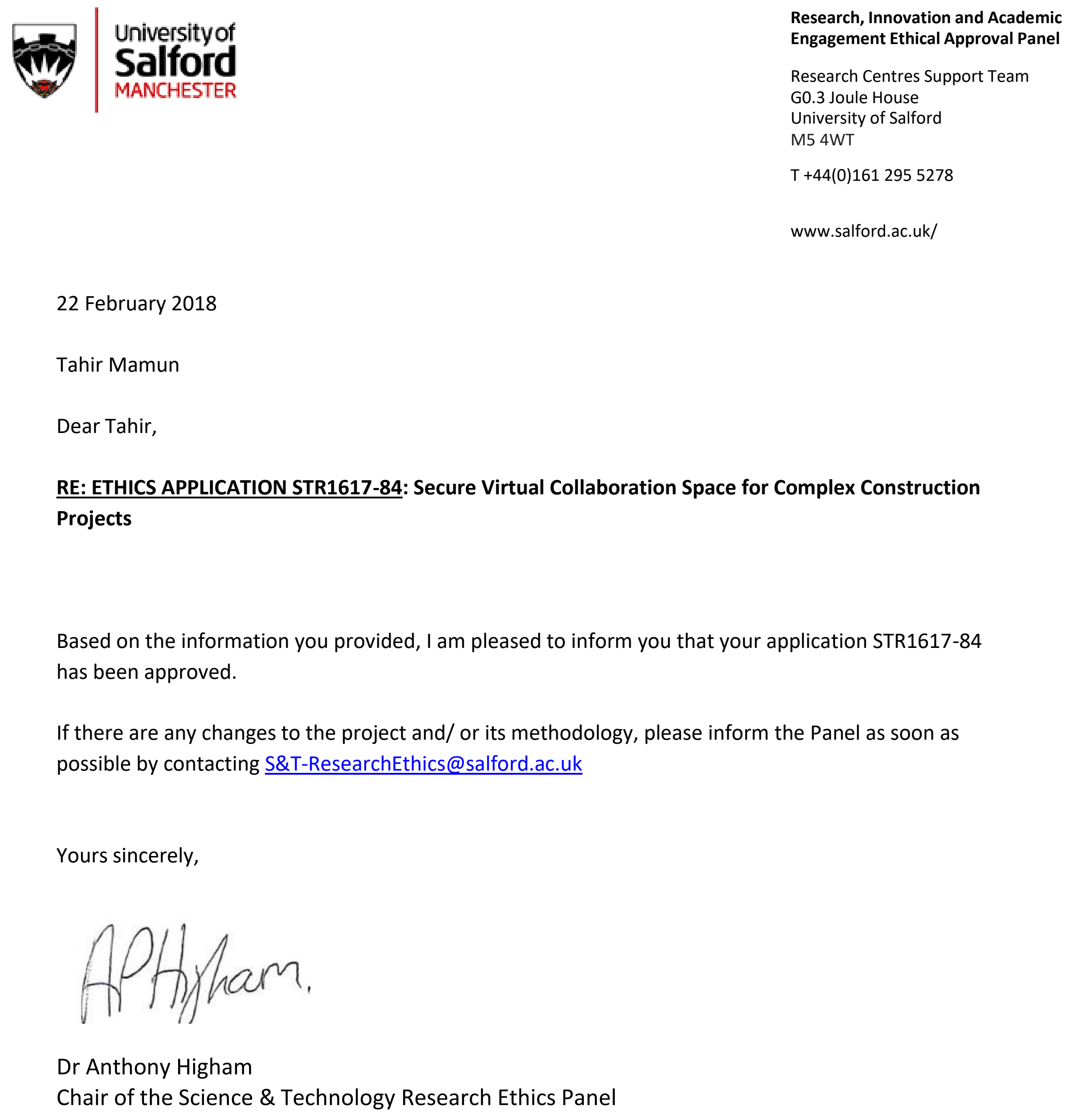
Excerpt	Excerpt Content
B.8.1	"…they simply refer to a CISO or equivalent and he or she says 'right, everything has to be on this secret level system' - and that means that only ten percent of your potential contractors can even bid for the job anymore, therefore the price will triple or quadruple - they tend to tackle the info-sec stuff as though it's just outside their span of control - but that's completely wrong - it's simply another risk like running out of money on the project is a risk, having it stop it in its track for some purely political reason is a risk - there's all sorts of risks, but information security risk often tends to get treated as though it's just utterly different.
B.8.2	"…there is an aspect which is important for BIM management which is knowledge-management and you have touched on it here - but to be effective on a construction programme - you need to be able to easily find out who is doing what and who knows what - and who's in charge of what and who to ask about what - so there is definitely a need for effective mapping of, in a single word – 'knowledge' if you like... in other words you need to know, that which is only accessible, which is only available from human beings - but you need some kind of mapping as to who's doing what."

Appendix B.9 – Excerpts of Discussion between B1 and B2:

Excerpt	Excerpt Content
B.9.1	**B2**: “Yeah a very detailed review of the process is something that is rarely undertaken - like you said**...** 'the rain caused the overrun' - that's one of the most obvious excuses”**.** **B1**: “Well that’s a consequence of poor information and process planning**.**” **B2**: “Yeah, not identifying the process-gaps – so – 'We'll follow the same processes because that process got us to the planning application' – But it wasn’t done in the best-way… so we’ll still use the same clunky processes but just start earlier**.**” **B1**: “Exactly, we didn't get the planning application in time because we didn't have critical information from critical people - at the right time, so we'll just give ourselves 10 weeks instead of 6 but we don't actually identify that we still won't get the critical information from the right people**.**”
B.9.2	**B1**: “If you were drilling into a plant room or a lab - but you didn't actually know what was happening in that room, it wouldn't make it sensitive - you could still have access to information, but only up to a certain degree of detail**.** So, if you were to run this approach enough times with these templates, you create the potential to define at **what point** a **space** or a **task** - **or information** becomes sensitive to who**.**” **B2:** “You're right, the more **you iterate it** - the **more you realise** there **are aspects** that **will become sensitive** as the **project progresses** - so for example - if it's a provision for rooms - you don't know what the risk is, but the room is going to be built - you kit them out with walls of certain kinds, the loading has to be calculated, everyone is going to have access to it**.** - But then you get to the point to when the client comes in to say that – here’s this sensitive information that needs **to go here** so for e.g. a core set of communication equipment… - But until you get to the stage where you're kitting out the room, you know that the information could be accessible to everyone**...** up until the point the specifics of what's in a specific room become needed**...** - but as what ***B1*** is saying - with the iterative way of going through your templates, you would be able to predict - and that would inform the levels of security required - and

	planning ahead of - it's not to imply everyone will get to know things are going to get secret, it's more the GR governing the template will know when things are going to become sensitive…”. **B1**: “I'm looking at it as a real positive you can start to have a strategy around your clearance, you can start to model when and what point, for what reason and for what people you need to put through clearance – because you know… that can take 16 weeks…”.

Appendix C – Ethics Approval Confirmation:



University of Salford MANCHESTER

Research, Innovation and Academic Engagement Ethical Approval Panel

Research Centres Support Team
G0.3 Joule House
University of Salford
M5 4WT

T +44(0)161 295 5278

www.salford.ac.uk/

22 February 2018

Tahir Mamun

Dear Tahir,

RE: ETHICS APPLICATION STR1617-84: Secure Virtual Collaboration Space for Complex Construction Projects

Based on the information you provided, I am pleased to inform you that your application STR1617-84 has been approved.

If there are any changes to the project and/ or its methodology, please inform the Panel as soon as possible by contacting S&T-ResearchEthics@salford.ac.uk

Yours sincerely,

APHigham.

Dr Anthony Higham
Chair of the Science & Technology Research Ethics Panel

Appendix D – Semi-structured Interview Questionnaire:

1. Start of the Interview

My name is Mohammed Tahir Mamun. I am a student of the University of Salford undertaking a doctoral project based around enabling secure collaboration within security-conscious BIM projects. The interview should take about 60 – 90 minutes depending on how quickly we go through the topics. Are you available to respond to some questions for this time?

I also require your consent for the interview to take place. This is as part of the ethics process required and governed by the University of Salford's academic ethics committee. I have provided you a copy of the consent form to complete if you choose to continue with the interview. You can read this at your own pace and ask any questions in regard to the ethical aspects of the research process. I have developed an information sheet that you can read at your own pace. It will detail all relevant aspects of the research but please feel free to ask any questions at any time.

Transition: I would like to ask you some questions about your experience in relation to security-conscious projects in order to gain your insight on issues or shortcomings that need to be addressed. This also includes your perspectives on future directions / approaches that you feel are necessary to address issues or shortcomings. Please feel free to expand on concerns common throughout such sectors and industry as a whole. I hope to use this information to help guide my research and to develop my research artefacts.

Let me begin the interview in full by asking you some questions about yourself and your previous competencies on security-conscious projects.

2. Questions to understand Interviewee Experience & Competencies

A. Could I first please ask what experience you've had with security-conscious BIM projects?

B. (If participant has no first-hand experience) Alternatively, could you please tell me your knowledge or background in relation to security conscious BIM projects or of security topics relevant to the AEC industry?

Transition: So now that I have understood your background your experience with security-minded issues, I'd like to give you a brief overview of the research and my proposed idea to enabling secure collaboration.

Detailed explanation of research:

The focus of my work is on enabling and improving secure collaboration within high security-risk BIM projects. From my literature search, I have identified a potential of a 'clash' existing between collaboration & security in sharing enough to remain effective but not so much that it poses risks. A number of issues may inhibit secure collaboration within practice that I wish to explore. I have identified potential issues related to *security* and *collaboration* respectively, and the overlap between the two factors, that appear to link to BIM processes, technologies, stakeholders, and the socio-technical aspects. The questions I ask will focus on these factors. Additionally, this research is focused on how new research artefacts can be derived from my interview analysis to attempt to resolve any issues I may identify. I will explore any ideas or requirements you may have as we progress through the discussion.

I hope you have understood the research. Do you have any questions? Thank you for listening to the idea, I'd like to now move on to some question that will help me to gain an understanding of how collaboration takes places on your project and how BIM fits into this.

A. Current collaboration practices:

1) What do you believe are the key principles, values and mind-sets in enabling collaboration and collaborative working on your projects?
   a) [Prompt] Are there any particular approaches taken to achieve collaboration and collaborative working?

2) In what capacity are standards such as the PAS 1192-2 applied within your projects in order to support collaborative working?

3) Would you be able to give me an overview of how you apply BIM as part of your collaborative workflows?
   a) [Prompt] Would you be able to walk-through how information is managed and shared with (a) internal and (b) external stakeholders throughout the project life cycle?
   b) [Prompt] How are CDEs applied to support collaborative workflows via management and sharing of BIM information with (a) internal and (b) external stakeholders?

4) What improvements do you believe need to be made to enhance collaboration within your practices?
   a) [Prompt] Are there any issues / limitations from (a) stakeholder, (b) workflow, (c) technical, (d) cultural and behavioural perspectives?

I'd like to now move on to questions to help me gain an understanding your view of security-minded principles and actual project practices employed on your project.

B. Current security practices:

1) What do you believe are the key principles, values & mind-sets that should be employed in order to ensure effective security?
   a) How are these applied within project practices?
   b) For example, how is the 'need to know' principle applied?

2) In what capacity are standards such as the PAS 1192-5 applied to promote security and support security-risk management?

3) What do you believe are the most significant security concerns / threats that affect you?
   a) For your particular project/s?
   b) For the rest of the industry?
   c) What concerns have arisen from application of digital workflows?
   d) How do you address issues of data-aggregation raised within the PAS 1192-5 (Explain concept if necessary).

4) Would you be able to give me an overview how you manage security-risk on your projects?
   a) How effective and granular do you believe security-risk assessment procedures are when classifying information that may be sensitive?
   b) Do your procedures result in precise and accurate security-classifications?
   c) Overall, how effective do you believe your security-risk mitigation approaches are?

5) Which roles would be involved in managing security-risk and what are their responsibilities?
   a) For example, which roles identify sensitive aspects of the BIM project?

6) Are current CDEs capable of securely managing sensitive information within BIM models effectively?
   a) Are they able manage concerns to ensure only those who 'need to know' about sensitive aspects are aware of them?

7) What improvements do you believe need to be made in order to enhance security within your practices?
   a) Are there any issues or limitations from a (a) stakeholder, (b) workflow, (c) technical, (d) cultural and behavioural perspective?

Thank you for helping me understand the principles and practices of security-minded approaches. I would now like to ask some key questions on how collaboration and security 'overlaps' in your practices.

C. Security and collaboration overlap:

1) Do you believe a clash exists between collaborative & security-minded approaches within (your) project practices and if so, how?
   a) For example, collaboration and information-sharing is underpinned by principles of openness, but security is based upon principles of 'least privilege' which may restrict sharing and access.
   b) How do you share with stakeholders based on the 'need to know'?

2) Do you believe the application of overly rigorous security presents collaboration difficulties?
   a) What difficulties are present when managing and sharing information:
      i) Internally within project teams?
      ii) Externally with other collaborating stakeholders? (For example, this could include your supply-chains or collaborators of the client.)

   b) For example, maybe due to not identifying how security-related measures may conflict or present tension with information-sharing require with stakeholders.
      i) Could this lead to difficulty sharing information? E.g. under-sharing.

   c) Could presence of sensitive information present additional sharing difficulties?
      i) What occurs when stakeholders cannot access information which is required for their work?

   d) Can other security related factors lead to other difficulties within project workflows? If so, how would you mitigate these issues?

3) Can you propose any scenarios where shortcomings in the collaboration aspect of BIM processes has led to adverse security-risk scenarios?
   a) What security-risks are present when collaborating and sharing information:
      i) Internally within your own team/s.
      ii) Externally with other collaborating stakeholders?

   b) What security-risks do you believe have arisen through ineffective application of BIM and digital workflows (throughout your project/s?)

c) Do you possess concerns of oversharing information during exchanges?

i) How would you manage or remediate these concerns?

4) What limitations are present with the systems currently used to facilitate secure & collaborative BIM information-flows?

a) What limitations are present in facilitating collaboration and effective exchange?

b) What limitations are present in ensuring & maintaining security?

5) What then do you think are the key barriers and approaches necessary to enable *secure collaboration*?

a) What factors do you think are relevant across the U.K Industry?

Thank you. The questions I have asked were to understand how security & collaboration motives overlap on projects. I would now like to discuss BIM governance & management. I.e. how you manage information across the project-lifecycle but also 'how' you govern how different participants are given appropriate rights to information based upon roles & responsibilities and what they need to know. Also, the 'how' aspect includes the process behind decisions, the roles, methods, and technologies involved, and policies / procedures. By discussing these factors with you, I hope to gain a better understanding how an ideal governance approach could help to facilitate secure collaboration.

D. Current vs future BIM Governance and Management:

1) Are BIM standards relevant in governing the management and sharing of BIM information?

a) If so, how are these standards relevant and how are they applied?

2) [Process Overview] Could you provide me an overview of how BIM information is managed & governed / controlled on your project?

a) How effective and precise are the current:

i. BIM information-management and information-sharing processes?

ii. Governance procedures for controlling those processes?

3) [Roles] What roles / stakeholders are currently involved in the governance & management of information?

a) Are any security-specific roles involved in making such decisions?

b) What issues do these roles have in making information-governance decisions?

i. How can they effectively identify what stakeholders need to access?

    c) What should responsibilities of roles be within future BIM governance approaches?

4) [Process - Policy] What governance or information-management policies are applied within your project practices?
    a) For example, what project-specific policies are applied for management or sharing?
    b) Are there any organisational policies related to the management & sharing?

5) [Technology] How effectively are you able to leverage CDE access-control based upon:
    a) The user's role & sensitivity of information in question?
    b) The 'file-level' or at a 'object and attribute' level (i.e. BIM data within files).
    c) Can access-rights be set in line with granular responsibilities?

6) Is there a need to move beyond current BIM processes & technologies of model-file level management and sharing? (Internal and external).

7) How could future BIM processes and technologies enable more precise and granular governance and management of information-flows?
    a) Would defining precise and granular responsibilities allow us to better govern, manage and share BIM information?

8) What are limitations of current BIM workflows and CDEs in achieving this?
    a) What would the role of future BIM workflows and CDEs be here?

9) How could future BIM processes *and* technologies account for precise / granular governance.

Finish off Interview: *Thank you for your time in answering my questions. It has been extremely helpful for my research, and I appreciate that you have made time for the interview. If you would like to ask any other questions in regard to the research, then please feel free to do so.*