Enhancing Security Architecture Framework Practice using the CyBOK Knowledge Areas for Practitioners

Author: Duncan Greaves, PhD, CISSP. duncan.greaves@warwick.ac.uk

Keywords: Cybersecurity, Digital Transformation, CyBOK

Abstract

Digital business transformation has security implications. These arise from organisational, business processes and technology changes that produce both risk and opportunity. Transformation requires business systems planning to take account of these altered security profiles and system architects should consider the cyber risks of such changes in advance of implementation.

Analysis of the academic literature relating to Digital Transformation was undertaken and mapped to the Cybersecurity Body of Knowledge (CyBOK) using keywords from the selected papers. The published content of two curricular frameworks relating to Enterprise Architecture (TOGAF and SABSA) were also mapped to the CyBOK. This produced a keyword mapping of the cybersecurity risk analysed at framework and Job Role levels.

The results reveal several key areas where architects can improve cybersecurity guidance and assurance. It was found that architects most greatly influence the area of Risk Management and Governance, but their influence contributes across many of the CyBOK knowledge areas to improve cybersecurity systems engineering. This work identified the need for further training of architects to include management security knowledge and new technology areas, and that architecture practice should support the development of security by assigning cybersecurity responsibility areas to different roles, enabling all architects to make an integrated contribution to security.

Introduction

In business terms Digital Transformation is a change process enabled by digital technologies that aims to bring radical improvement and innovation to an organization. Digital Transformation is carried out to create value for stakeholders by strategically leveraging key resources and capabilities (Gong and Ribiere, 2021), and leads to the evolution of, or creation of new business models (Henriette et al., 2016). However, in digital transformation, business strategy focuses on the transformation of products, processes, and the organization (Matt et. al, 2015) and it is these changes that increase exposure to risk, including cybersecurity risk by affecting the confidentiality, integrity, and availability of informational capital (Sallos et al., 2019). In addition, the Covid-19 crisis has led to an unprecedent reliance on digital solutions, ranging from teleworking to virus-tracking systems.

This has resulted in an increase in the number of cybersecurity incidents and types of attacks including Covid-19 related cybercrime, critical information infrastructure attacks and dissemination of pandemic disinformation (Carrapico and Farrand, 2020).

Thus, there is a growing need to explain and understand how enterprise professionals can be equipped with the multi-level, multi-disciplinary knowledge required to help decrease cyberattacks and increase the information quality of cybersecure systems. Digital transformation has changed the landscape of who does security, from a central security function towards a guiding function that allows opportunities for those closer to the development of components to implement controls (Berki et al., 2016). This brings with it an increased requirement for organisations to recognise cyber risk in business transformation programmes, and to connect this knowledge to the roles of the experts that architect, design and implement these changes. Digital Transformation is changing the requirement for cyber knowledge throughout the workforce and the way it is communicated and embedded in the training of personnel.

The CyBOK is a comprehensive Body of Knowledge developed to inform and underpin education and professional training for the cyber security sector (CyBOK,2019). By mapping digital transformation skill categories to architecture training curricula categories via the common language of the CyBOK knowledge areas, it is possible to gain insights into the common skills and training gaps which digitalisation and business transformation are bringing to management and planning in an environment of change. As part of business transformation transition planning, enterprise architects map business activities like organizational goals, products and services, markets, business processes, and performance indicators (Braun and Winter, 2005). It is only when these 'purely' business related artifacts are covered by architecture that important management activities like business continuity planning, change impact analysis, risk analysis and compliance can be fully supported (Winter and Fischer, 2006). The business risks, capabilities and processes only emerge when business principles and the information systems architecture are combined.

This paper explores new questions that seem to be fundamental to how to identify, manage, and introduce risk into business information systems against a cybersecurity background. There is a lack of academic publications that relate to the relationship between digital transformation and cybersecurity risk (Moşteanu, 2020), the use of cybersecurity controls in the enterprise architecture profession (Ekstedt and Sommerstad, 2009), and a lack of agreement on what the effect of changes brought by digital transformation exert on business principles, IT systems and architecture, especially in the cybersecurity domain (Fischer, Winter and Aier, 2010; Stelzer, 2009).

Despite the many studies conducted on the effects of digitalisation on organisations, there has been little documented evidence highlighting the overall big picture of the impact and effects. Guo et al., (2017) recommended studies need to focus on digitalisation vision by linking it to organisational learning, digital innovations, organisational agility, business ecosystems and organisational structures. By identifying the connections between business change and cybersecurity risk it is possible to identify and map the knowledge requirements to the CyBOK. This gives an outline of how to develop and enhance the training, capabilities,

practice and knowledge of architects in cyber-architectural approaches to business and systems development that can close these gaps.

The approach taken in this paper to analysing the need for cyber-architectural security is set out as follows:

- A literature review of Digital Transformation as it relates to the experiences of enterprise organisations and cybersecurity.
- Identification of relevant academic papers that explore the risks of cybersecurity in Digital Transformation and Business Change programmes and using these to extract keywords and keyword clusters.
- Mapping the keywords obtained from the academic literature along with keywords obtained from analysis of the curricula of two leading architectural frameworks (TOGAF and SABSA) to the CyBOK knowledge areas.
- Analysing the keyword mapping fit to demonstrate where the frameworks and the CyBOK correspond to identify synergies, and where gaps are identified to highlight where enhancements can be made to improve the training and knowledge of practitioners.

Literature Review

Digital Transformation and Risk

The intersection of digital transformation, Covid, and cyber security have made business continuity, pandemic issues, and cybersecurity incidents the three largest risk issues for companies across the world in 2021 (Alliancz, 2021). These risks, and many others, are interlinked and affect the whole business ecosystem. The integration of business with digitalisation is producing a growing vulnerability and uncertainty in a globalized and connected world.

The drivers for business transformation and change programmes are being fuelled by changes in the adoption of digital technologies. The technological drivers for change - Mobile computing, Social media, Big Data analytics, Cloud computing (Châlons and Dufft, 2017) and the IoT (Radanliev et al., 2019) are fundamentally altering business processes, products, services, and relationships (Karimi and Walter, 2015). This has required organizations to fundamentally change not only the way they do business with different organisational practices, but also affects the employee mindset and role in enabling these changes to happen. Opportunity wise, IT is a critical organisational resource with the potential to deploy digital innovation activities effectively so that greater opportunity in the transition to digital can be realised when IT strategy is aligned with innovation strategy (Cui *et al.* ,2015). The transition towards IT flexibility and integration have long been the cornerstones of IT strategies but aligning organisational and dynamic IT capabilities also enables organisations to adapt applications to digitalisation rapidly and economically.

For those tasked with protecting enterprises these drivers have introduced three main changes to the management of security (Nominet, 2020). Firstly, as digital transformation is

predominantly an IT-led initiative more education is needed for board and high-level decision makers to support transformation initiatives. Secondly, to realise secure outcomes cyber security should be considered at the earliest possible stages of digital transformation initiatives and, where this has not happened, remedial action needs be taken. Thirdly, to ensure comprehensive solutions security teams need to seek advice from a broader range of vendors and analysts, mainly outside their home organisation. It has long been known that successful IT-based business transformation programmes are founded upon changing thinking, changing behaviour, and changing perceptions of key personnel (Morgan and Page, 2008). Managing systemic risks successfully, therefore, requires management to become educated about cyber technology risks, to act on security early and to build in greater resilience in supply chains and business models so that the organisation can manage future exposures.

Regardless of whether cybersecurity issues are directly linked to digital transformation change has business leaders thinking again about risk and solutions that minimize risk, but Chief Information Security Officers (CISOs) are still grappling with visibility into the breadth of projects in their ecosystems (CSOonline, 2021). Although the knowledge of practitioners has increased, the number and heterogeneity of risk vectors introduced by digital technology makes the task of understanding the whole landscape harder (Almeida, Santos, and Monteiro, 2020). This task is made more complex with the existence of scenarios where old technologies cohabit with emerging technologies and a perceived lack of time and resources to invest in cybersecurity (Martins, 2019). To combat this, mature organisations link organizational objectives and cybersecurity risk, and senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. In these companies, cybersecurity risk is integrated into the organizational culture and evolves from an awareness of previous activities and continuous monitoring (NASA, 2019). It is also recognised that no practical cybersecurity strategy can prevent all attacks, and this requires other resilience strategies to sustain business during a cyberattack and to recover quickly (Rothrock et al., 2018). Digital resilience is a business issue, balancing data accessibility with the necessity of protecting customer data and intellectual property.

This involves a trade-off between security and interactivity (real-time interaction) that affects the way the customer experiences the service and how the business approaches providing those services. When balancing resilience against security, business priority must be given to resilience (Rothrock et al, 2018) and the protection of those business attributes that are important to customers. A balanced approach to security and resilience requires building an argument around risks, involving senior managers asking the correct questions and developing a common language between the business and IT (AttributiveSecurity, 2021). The US Dept of Energy guidelines (DoE, 2020) are one example of how business value can be anchored to the measurement of risk, with senior management questions like who has access to most important information? which assets are most likely to be attacked? which systems would cause most disruption? and which data cause financial, competitive, reputational, or other losses? Uncertainty considerations always involve an element of risk weightings and trade-offs between systems, human, organisational, and regulatory security measures. Risk serves as an explicit interface between the business and IT (Chmielecki et al., 2014), and

should be managed to accommodate the realisation of opportunity alongside the threat of loss.

Risk Management

Producing an enterprise-wide cybersecurity architecture practice that protects the organisation and its assets whilst preserving the capability to grasp opportunities is not an easy task to achieve. This is where risk management techniques, which span both business and technology uncertainty can help. Risk management is a discipline that is concerned with predicting and managing risks that could hinder the organization from reliably achieving its objectives under uncertainty, for example, cybersecurity. Cybersecurity includes information security but also comprises of the protection of information resources, assets, and people (von Solms and van Niekerk, 2013). All security is relative to value and risk propositions and risk analysis and management helps to protect that which stakeholder's value (Boehm, 2006).

The objective of risk analysis is to quantify and remediate the business impact and reputational damage caused to the business by the activities of information systems attackers or system failures. The complexity of such systems mean that they remain significant vectors of risk through which unauthorised users can access poorly guarded systems. There are many different risk management frameworks in use with which to quantify assess the impact of risks. For example, the FAIR assessment is widely used in visualising and quantifying risk (CyBOK, 2019), an important part of selecting and designing the controls with which to stop attacks (ISO27001, 2013). The business and systems risk assessment informs the choice of security level, which, in turn, allows choice of the appropriate security controls that are implemented (NIST800-37R2, 2017). In large organisations a cycle of continual improvement, baselining, diagnosis, evaluation, and prioritisation is required for the treatment of systemic risks which arise from the people and processes that such systems rely on (NIST 800-160, 2016).

However, many business systems are characterised by intermediation (Cherdantseva and Hilton, 2013) often without a central authority, which makes evaluating risk and the securing the IT estate more complex, for example, in cloud systems. As systems and structures become decentralised and agents are increasingly used to deliver functionality it becomes essential to invest in trustworthy component systems and the security of such systems is generally promoted by enforcing security objectives. These include the confidentiality, integrity, and availability (CIA) of information (ISO/IEC 27000:2018, 2018). Systems management, encryption and key management schemes underpin information distribution among the participating entities who may not know or trust each other. Enterprise security deals with the protection of this information and helps to avoid the economic, reputational, and legal risks of compromise. What social and technical systems have in common is that a secure network to pass messages is necessary but not sufficient for trust (Weckert, 2005). Therefore, it is the role of the enterprise security architect to evaluate the risk in systems that protect messages between trustworthy systems to create a sense of security.

The focus on technical safety and security measures helps to protect customers and business reputation. This is because cybersecurity fosters confidence that the expected actions will be predictable and undertaken in line with the principles of the enterprise that is

carrying them out. Poorly implemented cybersecurity in systems runs counter to effective organisational value due to the cost and maintenance of cyber-insecure systems and inhibits the development of further capabilities that produce value. Securing risks and opportunities before they are realised is one reason why architects produce implementation plans and roadmaps for with the business and communicate these roadmaps to the organisation (TOGAF, 2019).

Planning the Implementation of Risk

Enterprise architecture is concerned with managing the totality of business and information systems and has its roots in information systems management (Gøtze, 2013; Zachmann, 1987). When overseeing systems design, the architect is not wholly concerned with the resolution of single point issues. Enterprise security is concerned with the holistic functioning of collaborating systems and the emergent properties of interactions. This requires that both component and system engineering perspectives must be applied (CyBOK, 2019; Rasmussen, 1985) to the management and specification of risky capabilities by treating systems not only as the sum of its' parts (Nightingale and Rhodes, 2004) but also upon the behaviour of its interactions.

Architects use modelling techniques to communicate structures, processes and designs to stakeholders, and architectural models represent attempts to produce estimates of behaviour prior to implementation. Architectural principles act as a consistent set of principles and standards that guide design (Hoogervorst, 2004). They are general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which the organisation addresses the goals and concerns of key stakeholders (Van Bommel et al., 2007). By reasoning about risk, architects visualise the solutions, patterns of interaction and planning with which to realise the requirements of the supporting business systems. System designs are arrived at by rational processes, but design also requires prediction regarding possible future aims, processes, and results (Gonzalez Perez and Henderson Sellars, 2008; Simon, 1969). When designing future-focused business systems it is not just the intended use of the system that is important, it is in reducing the potential hazards of attack by those with differing aims, processes, and results that is also required (Huang et al., 2018). The emergence of values-based engineering design techniques (Spiekermann and Winkler, 2020) allows the use of architectural principles as normative guidelines to model and incorporate cybersecurity concerns into the formal specifications for the resultant business systems.

To remove some of this risk complexity several different enterprise architecture frameworks have been developed. An architecture framework defines the products an architect must deliver and how those products must be constructed without constraining the product content (Nightingale and Rhodes, 2004). Frameworks use views to simplify the overall architecture into a set of useful perspectives and models that describe certain aspects of the whole system. The TOGAF framework is an approach that models the structure of the enterprise and emphasises requirements management and a business system planning approach. Risk assessment in TOGAF is based on a qualitative approach combining effect and frequency labels to produce an overall impact assessment. Risk assessment and mitigation worksheets are then maintained as governance artefacts (CyBOK, 2019). The SABSA

enterprise security framework takes a 'layered' approach to decomposing risk and the method is enacted by decomposing business processes and attributes at different architectural layers from high-level capabilities and concepts down to logical and physical aspects, technology components and activities. Risk is addressed at every layer in a top-down approach through activities in all layers, and filtering security requirements from top to bottom to ensure cyber risk is considered throughout.

As the scope of overview expands, the level of detail known to the architect decreases. In exchange for a wider field of vision the enterprise architect sacrifices the depth of detail of the component systems at the lower level, favouring generality over granularity (Aier, Gleichauf and Winter, 2011) and concentrating on critical details (Maier, 1998). Conversely, applications and solution architects generally do not see the full enterprise, they deal with parts of the component stack but in greater detail (Figure 1). Emergent characteristics like security arise because of the unique constraints existing at each level (Cacioppo et al., 1999), but this can lead to vulnerabilities that cannot be fully appreciated at the lowest level of detail. These require the architect to explore gaps and architectural weaknesses in the overall security landscape *at the level of interest* by documenting the aspects that can and cannot be changed without compromising system integrity (Nightingale and Rhodes, 2004). The scope of different levels allows the implementation of the minimum of architectural decisions concerning the maintenance of system integrity across a single, unified overall design, form, or structure (Malan and Bredemeyer, 2002).

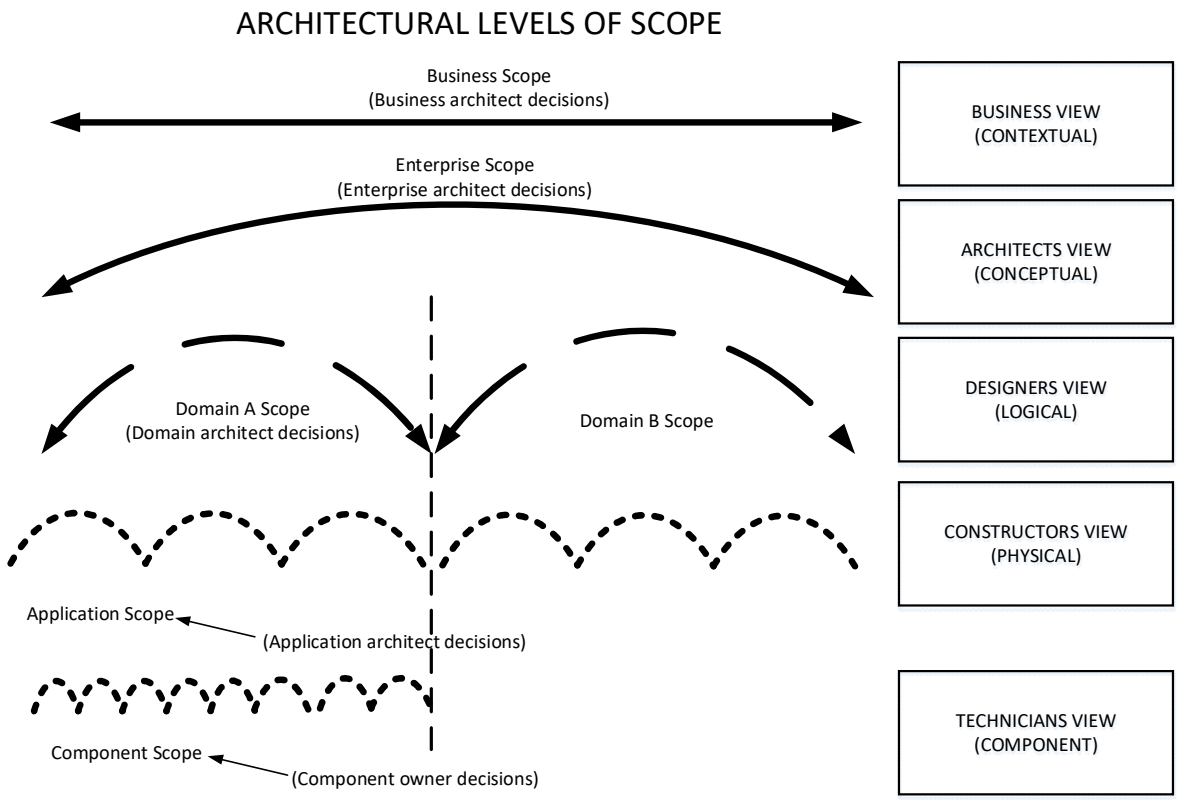

Figure 1 Architectural Levels of Scope (after Malan and BredeMeyer, 2002 with SABSA layers shown)

System analysis is dependent on theories of how to achieve security and security objectives, so models are produced with which to assess and predict the risk behaviour and effects of changes to a system or sub-system (Ekstedt and Sommestad, 2009). This approach

allows architects to reason before implementation about the emergent properties of systems and their interdependencies. It provides key actions towards implementing principles and controls that are generally accompanied by verification or assurance that they have been implemented correctly (Fischer, Winter, and Aier,2010).

The survival of businesses relates to the adoption of innovation, and embracing digital changes, to improve the efficiency and performance within the organization (Scardovi, 2017). Introducing correctly balanced risk into organisations is a necessity to realise these gains and grasp opportunities, but also implies change for people, processes and the technologies employed to release value. Architects manage the introduction of change and risk into the enterprise by taking a balanced overview of the utility and security of systems and by following business principles that shape the enterprise they produce requirements that shape systems (Josey et al., 2016). The decomposition and reconstruction of organizations and technology implies new educational specializations and developing new skills and competences (Moşteanu, 2020) to fulfil the challenges of different and new job requirements.

Methodology

The methodology undertaken to link the study of Digital Transformation to the analysis of risk and implementation of security measures in architecture is detailed in Figure 2. This approach was taken to ensure that the keywords extracted for analysis were relevant, but also at the required level of granularity to provide a meaningful comparison with the CyBOK lexicon.

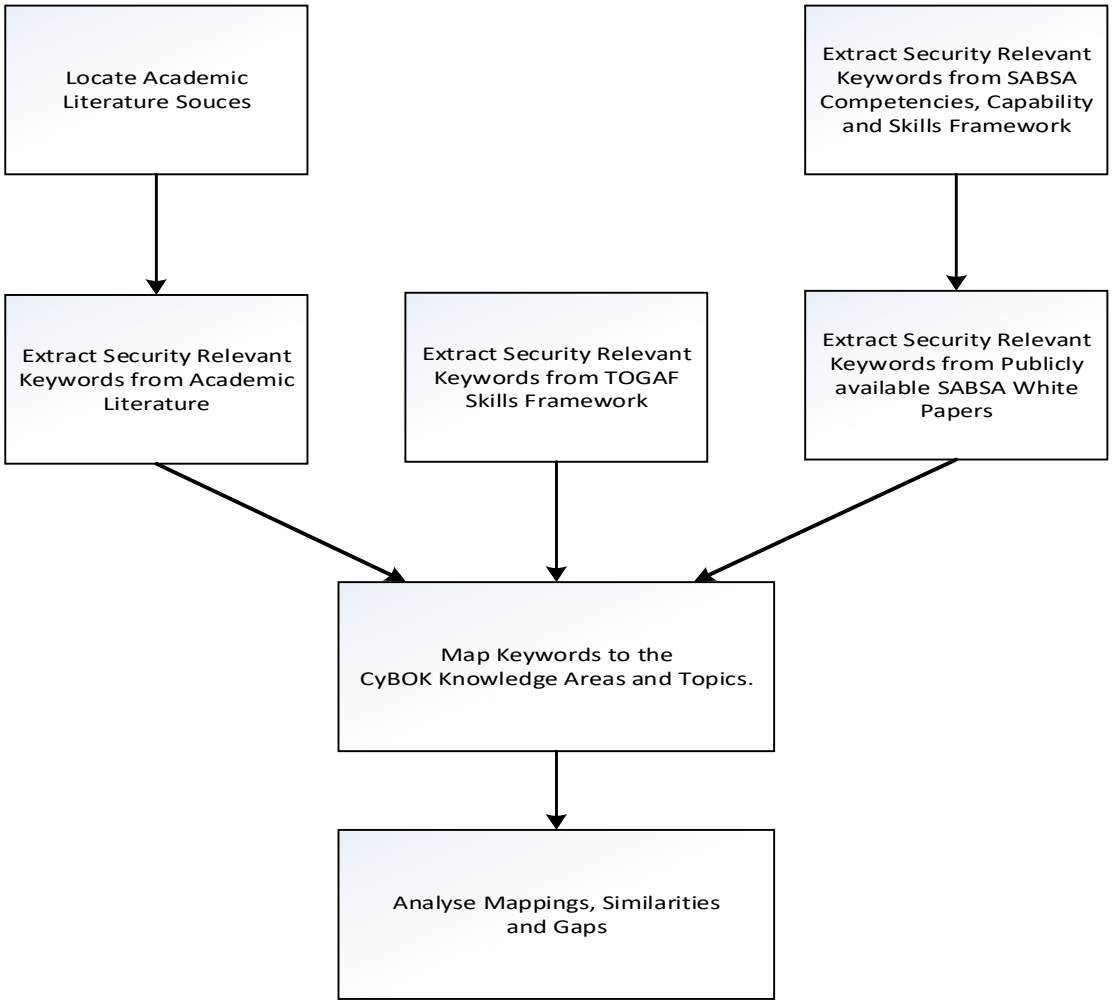

Figure 2 Methodology Approach

To locate relevant academic literature and obtain keywords for the mapping exercise an adapted four-phase literature analysis approach as employed (Table 1) to obtain concepts that were grouped for analysis (Morakanyane et al, 2017).

Phase	**How Used**
Phase 1: Searching Process. Search for academic journals & conference papers using Google Scholar	"business change" and "Cybersecurity" "Implementation of large projects" and "Cybersecurity" "business digitalisation" and "Cybersecurity" "digital transformation" and "Cybersecurity" "digital transformation" and "risk management" "business transformation" and "Risk management" "digital transformation" and "systematic review" "business change" and "review" and "cybersecurity"
Phase 2: Screening Process. Screening conditions were developed and used to focus results obtained from the searching process	The results were screened to include only those papers published in English since 2010. Preference was given to those papers that had been cited multiple times and those that had undertaken systematic review, large scale questionnaires or outlined taxonomies.
Phase 3: Clustering Process. Keyword clusters were developed based on thematic areas.	10 papers meeting the search criteria were selected for keyword identification and clustering. The emphasis was placed on interdisciplinary research

Phase	How Used
	and different business contexts. These papers are identified in the Appendix. These terms were added to those obtained from the TOGAF and SABSA Frameworks to identify the thematic areas of consideration.
Phase 4: Mapping Process. The keywords were mapped to the CyBOK Knowledge Areas and topics. Analysing the results.	The keywords were matched to the CyBOK Knowledge Areas and Topics using the methodology outlined in CyBOK, 2021.

Table 1 Literature Search and Mapping Methodology

It is the nature of enterprise frameworks to give a comprehensive coverage of the skills required to fully document the structure and processes of large organisations. The personal competencies of architects have been developed over many years and are based on skills and experience gained in different domains. As such any skills mapping would cover most or all the CyBOK knowledge areas, therefore a minimalist architecture approach (Malan and Bredemeyer, 2002) was taken to assessing which skills were most directly relevant to the work of the enterprise level architects.

Each enterprise framework was examined to find its smallest unit. Each unit was mapped, where appropriate, to a single CyBOK knowledge area. Where the unit size of the required skills was too coarse additional keywords and groups of keywords were sourced from the supporting literature for that framework (e.g., White Papers, Case Studies) to effectively define the skills in use. The subject mappings to the CyBOK knowledge areas aimed for consistency and rigour, but it was necessary to use judgement to map the topics in areas where the published frameworks did not have the full curriculum details. In these areas, contextual keywords were used to elaborate on the meaning. Where there were emerging issues identified from the literature, for example, the assessment of digitalisation, these were also added to the mappings. Where skills or competencies were present in all frameworks the keyword was extracted and mapped so that some keywords have multiple sources.

Results

Overall, 104 different sets of keywords relating to architectural skills were identified relating to the three sources (TOGAF, SABSA, and Literature Review) that were within the CyBOK scope. Of these 84 were mapped to knowledge areas, topics, and indicative content of the CyBOK, a match rate of 81%. The high-level mapping results are shown in Figure 3.

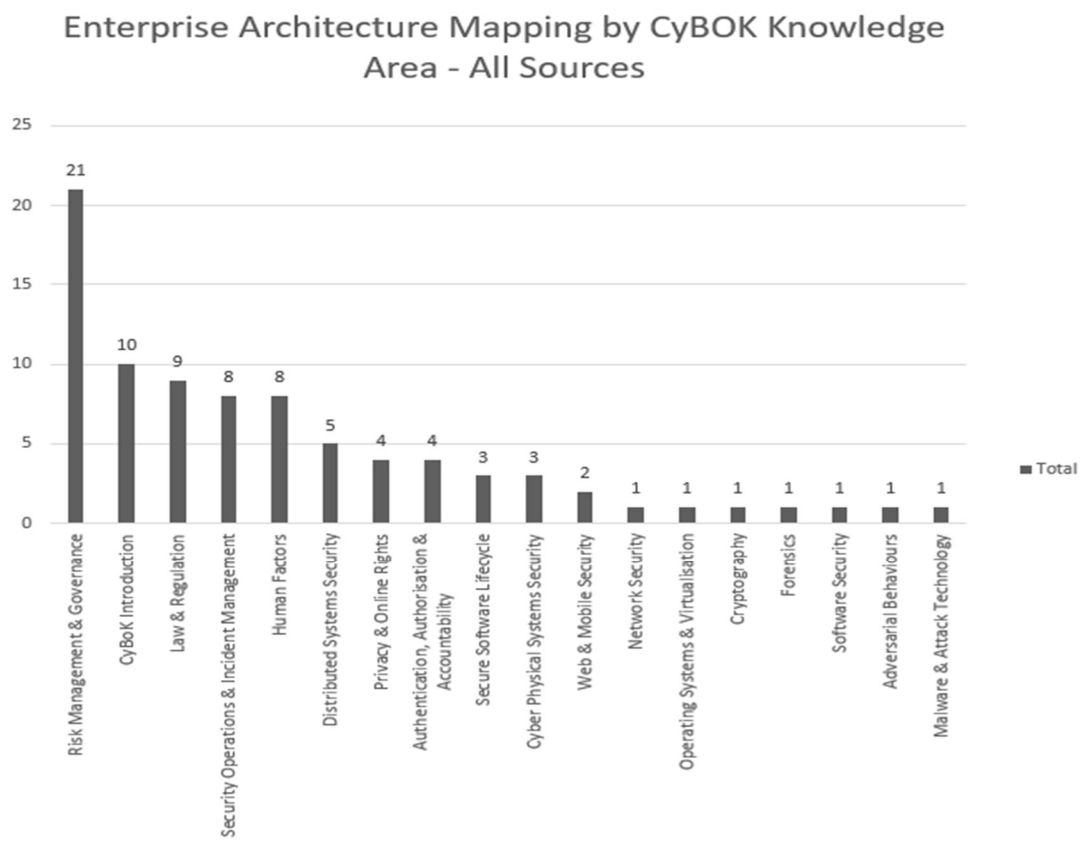

Figure 3 Keyword Mapping to Cybok Knowledge Areas - All Sources

The production of keyword clusters from the literature search mapped to the CyBOK provided insight into the cybersecurity concerns that lie behind business change and digital transformation. These topics represent the potential cybersecurity challenges faced by the leaders of businesses that are planning a large change or digital business programme of work. The high-level mapping results for the topics highlighted by the literature are shown in Figure 4.

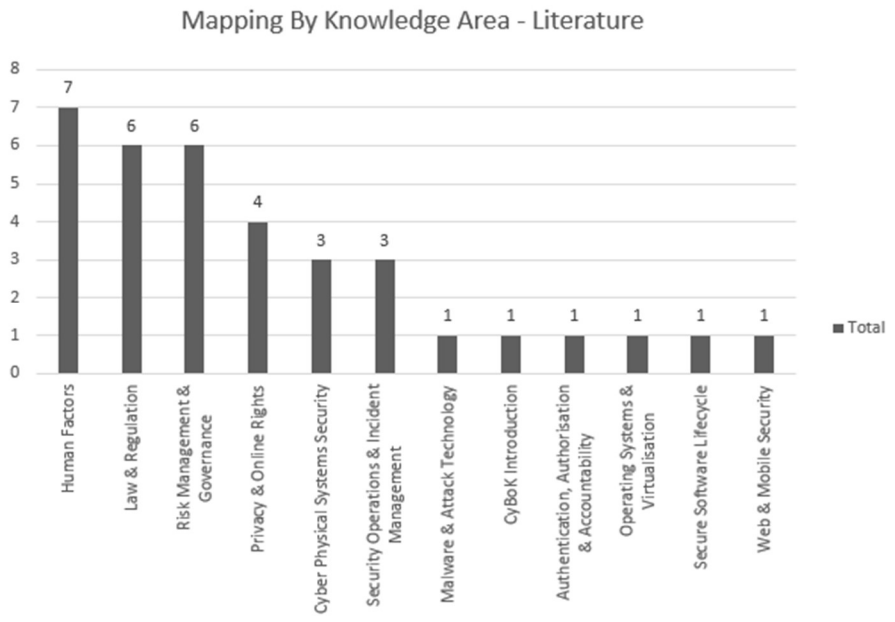

Figure 4 Keyword Mappings to CyBOK - Literature

The task of business and systems planning and implementation the based on the value and risk assessment of implementing digital initiatives is the work of the enterprise architects and management. By mapping architecture curriculum skills to the CyBOK it is possible to gain an overview of where the emphasis is placed in architecture frameworks. These are shown in Figure 5. Keywords that match to multiple frameworks are included in the knowledge area count once for each individual knowledge area.

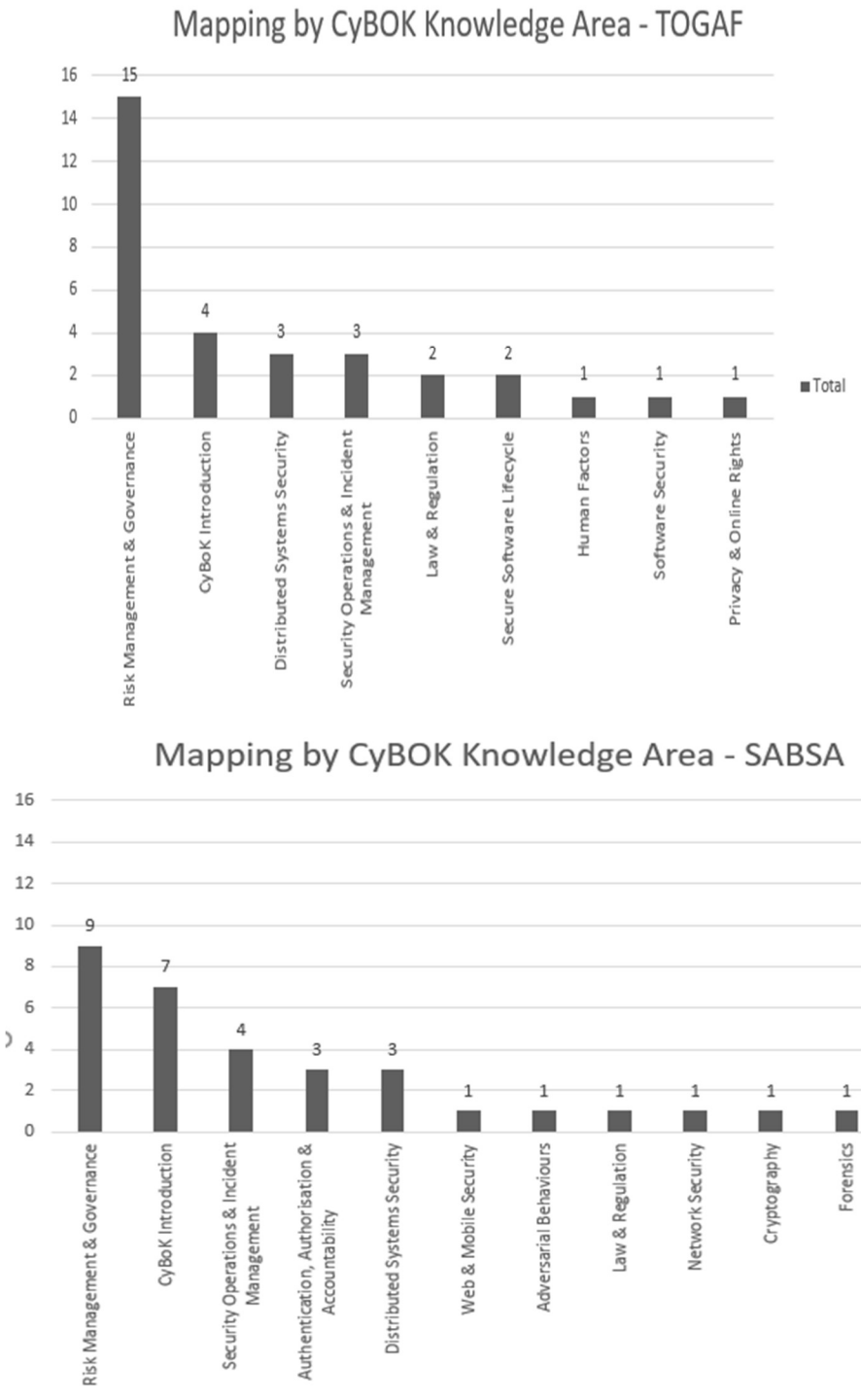

Figure 5 CyBOK Mappings by Framework

The keywords that could not be mapped to the CyBOK (Table 2) related to three main areas, those that were specific to business strategy; those that related to architecture processes; and those that relate to formal methods. These areas do not directly fall within the scope of the CyBOK version 1.0 (Rashid et al., 2018).

Keyword or keyword group	**Suggested Area**
Business Models, Business Strategies, Business Value Chain. Business modelling, SWOT, PESTLE, opportunity modelling. Wardley Mapping, assigning utility vs bespoke value.	Business Strategy
Allowable System States, Systems modelling and meta modelling.	Formal Methods
Holistic, Systems Thinking, Architectural Continuum, System coupling, System dependencies	Architecture Processes

Table 2 Keyword Groups Not Mapped to the CyBOK Knowledge Areas

The CyBOK was mapped to the architecture job roles using the suggested areas of expertise areas (job roles) for architects were selected from the TOGAF skills competency framework. These include the following: Enterprise Architecture Manager (EA); Business Architect (BA); Data Architect (DA); Application Architect (AA); Technology Architect (TA) and Solution Architect (SA). The Enterprise Security Architect (ESA) mapping is made to the SABSA framework capabilities where roles are not designated.

The specific nature of some architect roles requires that professionals have prior knowledge in certain domains related to their work and the primary base skills areas for these architects broadly map to the CyBOK broad subject areas shown in Table 2. Senior architect roles (Enterprise Architectuire Managers, Business Architects, Solution Architects and Enterprise Security Architects) will generally have developed expertise across multiple technical and business areas.

Architecture Role	**Primary CyBOK knowledge areas**
Data Architect (DA)	Distributed System Security (DSS) Law & Regulation (LR) Privacy and Online rights (POR)
Application Architect (AA)	Software Security (SS) Distributed System Security (DSS) Secure Software Lifecycle (SSL)
Technology Architect (TA)	Security Operations and Incident Management (SOIM) Network Security (NS) Web and Mobile Security (WAM)

Table 3 Mapping of architecture roles to core knowledge areas.

Architect roles were mapped to the CyBOK at role level (Table 4) using keywords taken from the relevant skills frameworks. The duties of each role were mapped to the CyBOK keywords based on the architectural skills frameworks for the role. Some keywords are mapped to more than a single role so are included in as many job descriptions as they have relevance to, accounting for the higher number of keyword counts observed.

	Risk Management & Governance	CyBOK Introduction	Authentication, Authorisation & Accountability	Security Operations & Incident Management	Human Factors	Distributed Systems Security	Law and Regulation	Software Security	Forensics	Adversarial Behaviours	Malware & Attack Technology	Cryptography	Network Security	Web & Mobile Security	Operating Systems and Virtualisation	Privacy & Online Rights	Secure Software Lifecycle	Cyber Physical Systems Security	Count of Keywords Mapped
Enterprise Architect	16	7	1	2	1	2	3	1	0	0	0	0	1	2	0	2	3	0	**41**
Enterprise Security Architect	13	8	4	4	4	4	2	1	1	1	1	1	1	1	1	1	0	0	**46**
Business Architect	5	2	1	1	1	1	1	0	0	0	0	0	0	1	0	0	0	0	**13**
Solution Architect	2	2	0	0	2	3	0	1	0	0	0	0	1	0	0	1	2	0	**14**
Application Architect	1	3	0	3	0	2	1	1	0	0	0	0	1	1	0	1	3	1	**18**
Technical Architect	1	2	1	3	0	3	1	1	1	1	1	0	1	0	1	0	1	0	**18**
Data Architect	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	1	0	0	**3**

Table 4 Keyword Mappings by Job Role

Analysis and Discussion

Business change programmes are initiated in response to the risks and opportunities that confront organisations. Large digital transformation programmes involve managing change throughout all levels of an organisation from the business model to the processes that realise business value, including human resource management and the introduction of technology. Mapping the keywords associated with digital transformation to literature sources, architectural frameworks, and role levels ensures coverage of potential cybersecurity concerns at Business, Management, and Individual levels to build a picture of the forces in play at each organisational level due to large project and programme activity.

This study showed that the combined Human, Organisational, and Regulatory Aspects of cybersecurity accounted for 50% of the mapped keyword attributes, and Attack and Defence aspects of cybersecurity comprised 38% of mapped attributes. The remaining 12% of the mappings related to the knowledge contained in the CyBOK introductory chapter which gives an overview of the body of cybersecurity knowledge.

Keywords derived from literature sources attribute more cyber risk to Human Factors (HF) knowledge (20%) than the enterprise framework level of analysis. This reflects the fact that the reasons that Board members cite for initiating change programmes are led by themes such as improving self-service, ease of use, building value, scale, resilience, and replacing personnel with technology, all of which are driven by the business context in which the changes are being undertaken. The organisational response to these contextual pressures and business drivers at architecture framework level is to assess the risks to organisational design, service processes and the implementation of change. The management of RMG processes is considered essential to synchronize information and activity across governance, risk, and compliance to operate more efficiently, enable effective information sharing, more effectively report activities, and avoid wasteful overlaps (OCEG, 2021). Therefore, to ensure that an organization reliably achieves new objectives, addresses uncertainty and acts with integrity management processes must be applied to recording actions. Examples of management processes to aid business objectives include accountability; the ability to trace the actions of individuals (Mulligan and Schneider, 2011), auditing (including threat auditing), assessment auditing, validation assessments, and assurance; to demonstrate that security measures have been implemented correctly (Sabillon et al., 2017). These measures use risk management and governance processes to identify and quantify cybersecurity threats and vulnerabilities in the business. Elements of architectural support that capture the needs found in the literature to address the Human Factors requirements of business change at role level are included in the job skills of the Solutions Architect and the Business Architect. Drilling into the results reveals that stakeholder engagement and system security are key skills for solutions architects, whilst business architects are focused on exploring the perceptions, thresholds and appetite for risk, and the continuity and policy aspects of business resilience.

The prominence of the CyBOK introduction in the mappings to frameworks (12%) and to the work of enterprise architects (17%) but with no mention in the literature sources reflects the positioning of the architecture frameworks as the key observers of crosscutting cybersecurity concerns. Some components or applications will be relevant to more than one business line or affect more than a single system., and this involves mapping data or system interdependencies, and monitoring or reducing lateral movement within and between systems (NCSC, 2021). In addition, overview functions involve resilience and system engineering and design skills, especially where the safety and security of remote devices or workers is at risk. This observation can also explain why authentication, authorisation, and accountability (AAA) and Distributed Systems Security (DSS) knowledge is also prominent in the skill set required of enterprise architects. The importance of boundaries, human-computer, computer-computer interfaces, and physical or logical barriers require information barriers and interfaces to enforce policy. These interfaces and their specifications guide

policies that play an important role in restricting lateral movement and data exfiltration that architects should be aware of.

The Enterprise Security Architect has most categories that map to the Authentication, Authorisation, and Accountability (AAA) knowledge area, reflecting the prominence of this role in providing security and assurance at management level, with the responsibilities of the roles of Solutions Architect and Technical Architect mapping to the knowledge area of Distributed Systems Security (DSS). Software Security (SS), an assessment of the vulnerability of applications is shared across all job roles, implying that the security of all platforms is a common concern.

The identification of distributed systems vulnerabilities and security was prominent in the matched keywords for all architect job roles and frameworks (6%) as was the identification of Security Operations and Incident Management (SOIM) (10%). Vulnerabilities are often described as component level difficulties to be patched. However, local vulnerabilities at component level require observation and control measures to be applied at different levels. Enterprise models can be used to detect the exposure to weaknesses at different levels by mapping the correspondence of vulnerabilities, especially where latent design conditions may arise because of the use or repurposing of legacy systems (Reason, 2008). This finding suggests that enterprise frameworks do not fully take account of the potential impacts of end to end or layered attacks completing their own business processes through the cyberattack chain. To combat this risk cyber-aware enterprise practice should emphasise the responsibility of modelling the presentation of layered defences and secure interfaces to challenge the capabilities of an attacker.

Systems development requires contextualisation, where constraints operate upon the local implementations. The need for systems to be aligned to their context is mapped to architecture frameworks in several CyBOK topic areas, including Web and Mobile Security, Human Factors, Distributed and Cyber-Physical systems, and Privacy and Online Rights (27% combined). The appearance of new technologies and the organisational response to these challenges are contextualised by the architects who assess the risks to advance decisions needed in adopting business changes. Organisations seek to balance the desired business outcomes with cybersecurity controls and considerations that these technology changes bring. As security relies upon the contextual authorisation of participants and systems to regulate the execution of code architects need ensure that project decisions have associated controls in place that do not undermine the management of the enterprise and other projects. The knowledge in areas of new technology is generally held by those architects that are involved in implementation (Application, Solutions and Data Architects), and it is essential that enterprise level architects are also involved in risk assessing developments due to the need for controls to be put in place.

In addition to considering the cybersecurity protective effects of the CyBOK knowledge areas, business strategy, modelling and architectural considerations also play a part in securing enterprises and represent the keyword attributes that were out of scope or that could not be mapped. The importance of leadership, planning and systems modelling to the security landscape should not be underestimated. Enterprise strategy can be viewed as a

set of selective ecosystem interventions that fulfil the goals of the organisation whilst adhering to the principles of development. In so doing, an enterprise architecture capability becomes a strategic differentiator (Ross, Weill, and Robertson, 2006). To exercise this control over strategy managers must evaluate the overall effectiveness and risks in introducing systems or processes to the business prior to systems development. These assessments help to define the forward-looking vision for the organisation towards realising value and describe how the resources and capabilities are mobilised towards this objective.

Conclusion

It is estimated that 56% of boards prioritise cybersecurity (KPMG, 2019), yet 27% of organisations have no cyber policy (NCSC, 2020). Given that cybersecurity issues exist and are a growing concern of enterprises, architectural and systems principles relating to socio-technical issues are required to reason about risk and cybersecurity. Transformation, change, or digitalisation initiatives are proposed from a business perspective, but the opportunities sometimes appear with cyber risks attached. Business challenges include innovation, new technologies, agility, digital transformation, and sustainability. Architecture practice needs to balance competing priorities including profit, legislation, regulation, and business risks with cybersecurity. Thus, a balanced approach to risk is needed and security concerns must be weighed against the need for resilience measures to maintain business continuity in the event of digital disruptions. Reputational risk in business should be an effective motivator for businesses to create a cyber policy, as are legislation and compliance. By anchoring the goals of business transformation to enterprise risk, organisational and technical cybersecurity principles applied to the introduction of risk aid the formation and protection of trust in business systems to add organisational value.

To illustrate this, an analysis of business change literature and two widely used enterprise architecture frameworks were mapped to the CyBOK. SABSA is a taxonomy-based meta-analysis, a layer cake of systems abstraction. TOGAF uses a different taxonomy of layering, through the analysis of the business, data, applications, and technical domains. Frameworks add structure to cybersecurity capabilities but need to be used in an integrated fashion. Although SABSA is important in defining the context within which security takes place, an important part of the TOGAF framework includes ensuring that the architecture practice can apportion responsibility for security across different job roles. This helps to include cybersecurity as a whole organisation endeavour. Analysis of these mappings to the CyBOK knowledge areas has shown that the contribution of enterprise frameworks allows all classes of architects to actively contribute to cybersecurity.

The largest area of correspondence with the CyBOK for all sources was that of Risk Management and Governance (RMG). The academic business literature contained a large element of this knowledge but was weighted towards Human Factors (HF) cybersecurity, echoing the concerns that board level decision makers have about service improvement and business opportunity. The architectural frameworks that were mapped address these issues through the initiation and production of risk management processes to embed cybersecurity thinking through the involvement of Business Architects and Solutions Architects in particular.

The provision of systems security is primarily the responsibility of the Enterprise Security Architect, with Solutions Architects and Technical Architects helping to ensure that software and distributed systems are secured appropriately. It was noted that the greater involvement of Data Architects in security can assist in ensuring that legal compliance and privacy goals are met. The use of Security Operations and Incident Management (SOIM) was concentrated in the Technical (TA) and Application Architect (AA) job roles. As SOIM plays a pivotal role in identifying real-time threats and vulnerabilities, and in maintaining the stability of ongoing systems and operations this knowledge is used by the security teams to build awareness and responses to attacks. This improves risk profiling and assists in the understanding of complex attack patterns that management can use to protect the organisation. Understanding the risks in the introduction of technology were mapped to the Applications, Solutions and Data architect job roles (AA/SA/DA), but the impact of new implementation was not reflected in the knowledge mappings seen in enterprise level architect roles. This suggests that there may be significant risk introduced by new technology that is not being fully considered at management level.

The application of the CyBOK knowledge areas to developing architect training and continuing professional development programmes allows practitioners to recognise the fundamental systemic, human factors and technical risks that can result in business impacts and reputational damage. The overall effect of security education in digital transformation scenarios is to improve risk awareness and security involvement in early stages of the architecture and design process. This allows standards, dealing with interoperability, availability, and reliability to be developed that build business resilience (Bhuyan et al, 2020). Education advances the identification of potential cybersecurity issues during the planning and development stages of projects. However, many issues do not manifest until production run time and the burden of identification of such issues falls to operational staff. Adding cybersecurity concepts into the training and design of architects helps to change security thinking by modelling secure processes before adding controls to existing systems. This permits organisations wishing to develop cyber policy to anticipate cybersecurity issues and design problems out beforehand rather than dealing with them once operational.

Further Research Directions

Using enterprise architecture frameworks allow the development of enterprise structure, which is crucial to properly address risk, but differ in the extent to which they guide through the cybersecurity aspects (Chmielecki et al., 2014). The integration of cybersecurity into enterprise frameworks to remain relevant and to provide clear advice and reference guidance is an ongoing task. As part of the CyBOK development project the SABSA and TOGAF frameworks were mapped separately but integrating the two is also possible. Comparative assessments with other development and management frameworks in the Software Development Lifecycle (SDLC) and business space can help to build a fuller picture of the contribution of the CyBOK to cybersecurity awareness at senior levels of organisations.

Appendix

The following academic papers were used in creating the keywords list for the mapping:

Author(s)	Year	Title
Morakanyane et al.	2017	Conceptualising Digital Transformation in Business Organisations: A Systematic Review of Literature
Smirnova et al.	2019	Formation of requirements for human resources in the conditions of digital transformation of business
Brown et al.	2011	Are you ready for the era of 'big data'
Dilmegani et al.	2014	Public-sector digitization: The trillion-dollar challenge.
Maglaras et al	2020	Cybersecurity in the Era of Digital Transformation: The case of Greece.
Safrudin et al.	2014	A typology of business transformations.
Moşteanu	2020	Challenges for Organizational Structure and design as a result of digitalization and cybersecurity
Parsoya	2021	Significance of Technology and Digital Transformation in Shaping the Future of Oil and Gas Industry.
Bhuyan S.S. et al.	2020	Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations
Matt et al.	2015	Matt, C., Hess, T. and Benlian, A., 2015. Digital transformation strategies. *Business & information systems engineering*, *57*(5), pp.339-343.

Table 5 References used in academic literature to CyBOK mapping

Attributions

References

Aier, S., Gleichauf, B. and Winter, R., 2011. Understanding enterprise architecture management design-an empirical analysis.

Alliancz, 2020. Alliancz Global Risk Barometer, 2020. https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html Accessed 11th July 2021.

Almeida, F., Santos, J.D. and Monteiro, J.A., 2020. The challenges and opportunities in the digitalization of companies in a post-COVID-19 World. *IEEE Engineering Management Review*, *48*(3), pp.97-103.

AttributiveSecuirty.com, 2021. The SABSA podcast https://www.attributivesecurity.com/episode/11-balanced-risk Accessed 11th July 2021.

Berki, E., Valtanen, J., Chaudhary, S. and Li, L., 2018. The need for multi-disciplinary approaches and multi-level knowledge for cybersecurity professionals. In *Multidisciplinary Perspectives on Human Capital and Information Technology Professionals* (pp. 72-94). IGI Global.

Bhuyan, S.S., Kabir, U.Y., Escareno, J.M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D. and Dobalian, A., 2020. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of medical systems*, *44*(5), pp.1-9.

Boehm, B.W., 2006. Value-based software engineering: Overview and agenda. *Value-based software engineering*, pp.3-14.

Bommel, P.V., Buitenhuis, P., Hoppenbrouwers, S. and Proper, E., 2007. Architecture principles–A regulative perspective on enterprise architecture. *Enterprise modelling and information systems architectures–concepts and applications*.

Braun, C. and Winter, R., 2005. A comprehensive enterprise architecture metamodel and its implementation using a metamodeling platform.

Brown, B., Chui, M. and Manyika, J., 2011. Are you ready for the era of 'big data'. *McKinsey Quarterly*, *4*(1), pp.24-35.

Cacioppo, J.T., Gardner, W.L. and Berntson, G.G., 1999. The affect system has parallel and integrative processing components: Form follows function. *Journal of personality and Social Psychology*, *76*(5), p.839.

Carrapico, H. and Farrand, B., 2020. Discursive continuity and change in the time of Covid-19: the case of EU cybersecurity policy. *Journal of European Integration*, *42*(8), pp.1111-1126.

Châlons, C. and Dufft, N., 2017. The role of IT as an enabler of digital transformation. In *The drivers of digital transformation* (pp. 13-22). Springer, Cham.

Chatham, 2016 https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf Accessed 11 July 2021.

Cherdantseva, Y. and Hilton, J., 2013, September. A reference model of information assurance & security. In *2013 International Conference on Availability, Reliability and Security* (pp. 546-555). IEEE.

Chmielecki, T., Cholda, P., Pacyna, P., Potrawka, P., Rapacz, N., Stankiewicz, R. and Wydrych, P., 2014, September. Enterprise-oriented cybersecurity management. In *2014 Federated Conference on Computer Science and Information Systems* (pp. 863-870). IEEE.

CSO Online , 2020 https://www.csoonline.com/article/3512578/what-is-securitys-role-in-digital-transformation.html Accessed 11 July 2021.

Cui, T., Ye, H.J., Teo, H.H. and Li, J., 2015. Information technology and open innovation: A strategic alignment perspective. *Information & Management*, *52*(3), pp.348-358.

CyBOK, 2019. https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf

CyBOK, 2021. https://www.cybok.org/media/downloads/CyBOK_Mapping_Framework_academic_professional_progs_Feb21.pdf , Accessed 06 November 2021

Dilmegani, C., Korkmaz, B. and Lundqvist, M., 2014. Public-sector digitization: The trillion-dollar challenge. *McKinsey. com, December*.

DoE, 2020. US Dept of Energy Guidelines https://www.energy.gov/ceser/cybersecurity Accessed 11 July 2021.

Ekstedt, M. and Sommestad, T., 2009, March. Enterprise architecture models for cyber security analysis. In *2009 IEEE/PES Power Systems Conference and Exposition* (pp. 1-6). IEEE.

Fischer, C., Winter, R. and Aier, S., 2010. What is an enterprise architecture principle? In *Computer and Information Science 2010* (pp. 193-205). Springer, Berlin, Heidelberg.

Gong, C. and Ribiere, V., 2021. Developing a unified definition of digital transformation. *Technovation*, *102*, p.102217.

Gonzalez Perez, C. and Henderson-Sellers, B., 2008. *Metamodelling for software engineering*. John Wiley and Sons.

Gøtze, J., 2013, September. The changing role of the enterprise architect. In *2013 17th IEEE International Enterprise Distributed Object Computing Conference Workshops* (pp. 319-326). IEEE.

Guo, J., Pan, J., Guo, J., Gu, F. and Kuusisto, J., 2019. Measurement framework for assessing disruptive innovations. *Technological Forecasting and Social Change*, *139*, pp.250-265.

Hallett, J., Larson, R. and Rashid, A., 2018. Mirror, mirror, on the wall: What are we teaching them all? Characterising the focus of cybersecurity curricular frameworks. In *2018 {USENIX} Workshop on Advances in Security Education ({ASE} 18)*.

Henriette, E., Feki, M. and Boughzala, I., 2016, September. Digital Transformation Challenges. In *MCIS* (p. 33).

Hoogervorst, J.: Enterprise Architecture: Enabling Integration, Agility and Change. IJCIS 13(3), 213–233 (2004)

Huang, K., Siegel, M. and Madnick, S., 2018. Systematically understanding the cyberattack business: A survey. *ACM Computing Surveys (CSUR)*, *51*(4), pp.1-36.

ISO/IEC 27001:2013, https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Josey, A., Lankhorst, M., Band, I., Jonkers, H. and Quartel, D., 2016. An introduction to the ArchiMate® 3.0 specification. *White Paper from The Open Group*.

Karimi, J. and Walter, Z., 2015. The role of dynamic capabilities in responding to digital disruption: A factor-based study of the newspaper industry. *Journal of Management Information Systems*, *32*(1), pp.39-81.

KPMG, 2019 *"A changing Perspective 2019 CIO Survey"* https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/07/harvey-nash-kpmg-cio-survey-2019.PDF

Maglaras, L., Drivas, G., Chouliaras, N., Boiten, E., Lambrinoudakis, C. and Ioannidis, S., 2020, November. Cybersecurity in the Era of Digital Transformation: The case of Greece. In *2020 International Conference on Internet of Things and Intelligent Applications (ITIA)* (pp. 1-5). IEEE.

Maier, Mark W. "Architecting principles for systems-of-systems." *Systems Engineering: The Journal of the International Council on Systems Engineering* 1, no. 4 (1998): 267-284.

Malan, R. and Bredemeyer, D., 2002. Less is more with minimalist architecture. *IT professional*, *4*(5), pp.48-47.

Martins A., Cyberthreats named the most concerning issue for businesses, Accessed: May 12, 2020. [Online]. Available: https://www.businessnewsdaily. com/15295-cyberthreats-biggest-business-concern.html

Matt, C., Hess, T. and Benlian, A., 2015. Digital transformation strategies. *Business & information systems engineering*, *57*(5), pp.339-343.

Morakanyane, R., Grace, A.A. and O'Reilly, P., 2017. Conceptualizing Digital Transformation in Business Organizations: A Systematic Review of Literature. *Bled eConference*, *21*.

Morgan, R.E. and Page, K., 2008. Managing business transformation to deliver strategic agility. *Strategic Change*, *17*(5-6), pp.155-168.

Moşteanu, N.R., 2020. Challenges for Organizational Structure and design as a result of digitalization and cybersecurity. *The Business & Management Review*, *11*(1), pp.278-286.

Mulligan, D.K. and Schneider, F.B., 2011. Doctrine for cybersecurity. Daedalus, 140(4), pp.70-92.

NASA, 2019. NASA's Security Readiness https://oig.nasa.gov/docs/IG-21-019.pdf Accessed 11th July 2021

NCSC, 2016. How Cyber Attacks Work. https://www.ncsc.gov.uk/information/how-cyber-attacks-work

NCSC, 2020. NCSC Board Toolkit Introduction.https://www.ncsc.gov.uk/collection/board-toolkit/introduction-cyber-security-board-members

NCSC, 2021. Preventing Lateral Movement. https://www.ncsc.gov.uk/guidance/preventing-lateral-movement

Nightingale, D.J. and Rhodes, D.H., 2004, March. Enterprise systems architecting: Emerging art and science within engineering systems. In *Proceedings of the ESD External Symposium* (pp. 1-13).

NIST, 2016. NIST 800-160 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final

Nominet, 2020 https://media.nominet.uk/wp-content/uploads/2019/07/Cyber-Security-in-the-Age-of-Digital-Transformation.pdf Accessed 11 July 2021

OCEG, 2021. https://www.oceg.org/about/what-is-grc/

Parsoya, S., 2021. Significance of Technology and Digital Transformation in Shaping the Future of Oil and Gas Industry. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(3), pp.3345-3352.

Radanliev, Petar, David Charles De Roure, Jason RC Nurse, Pete Burnap, Eirini Anthi, Uchenna Ani, Omar Santos, and Rafael Mantilla Montalvo. "Definition of cyber strategy transformation roadmap for standardisation of IoT risk impact assessment with a goal-oriented approach and the internet of things micro Mart." *University of Oxford* (2019).

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M. and Peersman, C., 2018. Scoping the cyber security body of knowledge. *IEEE Security & Privacy*, *16*(3), pp.96-102.

Rasmussen, J., 1985. The role of hierarchical knowledge representation in decisionmaking and system management. *IEEE Transactions on systems, man, and cybernetics*, (2), pp.234-243.

Reason, J., 2008, The human contribution: unsafe acts, accidents, and heroic recoveries. CRC Press.

Ross, J.W., Weill, P. and Robertson, D., 2006. *Enterprise architecture as strategy: Creating a foundation for business execution*. Harvard business press.

Rothrock, R.A., Kaplan, J. and Van Der Oord, F., 2018. The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, *59*(2), pp.12-15.

Sabillon, R., Serra-Ruiz, J., Cavaller, V. and Cano, J., 2017, November. A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In *2017 International Conference on Information Systems and Computer Science (INCISCOS)* (pp. 253-259). IEEE.

SABSA, 2020. The SABSA institute https://sabsa.org/the-sabsa-institute/

Safrudin, N., Rosemann, M., Recker, J. and Genrich, M., 2014. A typology of business transformations. Available online: https://eprints.qut.edu.au/73857/1/360_Journal___11th_edition_Typology.pdf

Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. *Journal of Intellectual Capital*.

Scardovi, C., 2017. *Digital transformation in financial services* (Vol. 236). Cham: Springer International Publishing.

Simon, H.A., 2019. *The sciences of the artificial*. MIT press.

Smirnova, A., Zaychenko, I. and Bagaeva, I., 2019, September. Formation of requirements for human resources in the conditions of digital transformation of business. In *Proceedings of the International Conference on Digital Technologies in Logistics and Infrastructure (ICDTLI 2019). Available online: https://www. atlantis-press. com/proceedings/icdtli-19/125918521*.

Sommestad, T., Ekstedt, M. and Johnson, P., 2009, January. Cyber security risks assessment with bayesian defense graphs and architectural models. In *2009 42nd Hawaii International Conference on System Sciences* (pp. 1-10). IEEE.2009).

Spiekermann, S. and Winkler, T., 2020. Value-based engineering for ethics by design. *arXiv preprint arXiv:2004.13676*.

Stelzer, D., 2009, November. Enterprise architecture principles: literature review and research directions. In *Service-oriented computing. ICSOC/ServiceWave 2009 workshops* (pp. 12-21). Springer, Berlin, Heidelberg.

TOGAF, 2019. TOGAF Architecture Skills Framework https://pubs.opengroup.org/architecture/togaf8-doc/arch/chap30.html

Von Solms, R. and Van Niekerk, J., 2013. From information security to cyber security. *computers & security*, *38*, pp.97-102.

Weckert, J., 2005. Trust in cyberspace. *The impact of the internet on our moral lives*, pp.95-120.

Winter, R. and Fischer, R., 2006, October. Essential layers, artifacts, and dependencies of enterprise architecture. In *2006 10th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW'06)* (pp. 30-30). IEEE.

Zachman, J. A. (1987) A Framework for Information Systems Architecture. IBM Systems Journal 26 (3), pp 276-292.