ENTERPRISE SECURITY ARCHITECTURE – MYTHOLOGY OR METHODOLOGY?

MICHELLE GRAHAM

SCHOOL OF COMPUTER SCIENCE

UNIVERSITY OF ADELAIDE

Table of Contents

List of Tables

TABLE PAGE

List of Figures

Abstract

Security is a complex issue for organisations, with its management now a fiduciary responsibility as well as a moral one. Organisational security, such as computer security, human security, access control, risk management etc.; is conducted in separate business units creating a silo effect. A cohesive and holistic approach is required to mitigate the risk of security breaches and parts of the business not monitored by any silo. Without a holistic robust structure, the assets of an organisation are at critical risk. Enterprise architecture (EA) is a strong and reliable structure that has been tested and used effectively for designing, building, and managing organisations globally for at least 30 years. Grouping security with EA promises to leverage the benefits of EA in the security domain.

Through a review of existing security frameworks this work evaluates the extent to which they employ EA and determines there is a need for developing a comprehensive solution. This research designs, develops, evaluates and demonstrates a security EA framework for organisations regardless of their industry, budgetary constraints or size. The framework is developed from the Zachman framework 2013 Version 3.0 because it is the most complete, most referenced in our frameworks review, and historically the methodology that is chosen by others to base their frameworks on. The results support the need for a holistic security structure and indicate benefits including reduction of security gaps, improved security investment decisions, clear functional responsibilities and a complete security nomenclature and international security standard compliance among others. This research bridges the gap and changes the way we fundamentally view security in an organisation, from individual silo capabilities to a holistic security eco-system with highly interdependent primitive security models.

Declaration of Originality

I certify that this work contains no material which has been accepted for the award of any other degree or diploma in my name in any university or other tertiary institution and, to the best of my knowledge and belief, contains no material previously published or written by another person, except where due reference has been made in the text. In addition, I certify that no part of this work will, in the future, be used in a submission in my name for any other degree or diploma in any university or other tertiary institution without the prior approval of the University of Adelaide and where applicable, any partner institution responsible for the joint award of this degree. I give permission for the digital version of my thesis to be made available on the web, via the University's digital research repository, the Library Search and also through web search engines, unless permission has been granted by the University to restrict access for a period of time. I acknowledge the support I have received for my research through the provision of an Australian Government Research Training Program Scholarship.

6 March 2021

Michelle Rey Graham — Date

Acknowledgements

"At times, our own light goes out and is rekindled by a spark from another person. Each of us has cause to think with deep gratitude of those who have lighted the flame within us."

Albert Schweitzer

I wish to express the deepest appreciation to my supervisors Dr Katrina Falkner, Dr Claudia Szabo and Dr Yuval Yarom, who without their kindness and long suffering support to me, this would not have been completed.

To my husband and best friend Franklyn Graham who has never known me not studying. Somehow you should get an award as well for always encouraging me and consistently taking care of the other things so I could concentrate. Love you always. You are my heart.

My fan club and parents, Sharon Pederick and Peter Deacon, thank you for the steak dinners, the belief in my ability and the love you always show. I pray I've made you proud.

Gabriel Maicas Suso, my PhD partner in crime and the one who always makes me laugh! Started our study on the same day and have laughed ever since. What an unlikely friendship we have but I will always be grateful.

And finally to my mentors and friends, John Sheridan and Peter Kalkman who have given me the creative space at work and personally to produce this amazing concept and run with it. And for seeing more in me than I see in myself at times including the kick up the pants to keep going. Thank you!

Publications

The following publications were derived from this dissertation:

"Enterprise Security Architecture: Mythology or Methodology?" M. McClintock, K. Falkner, C. Szabo and Y. Yarom, in International Conference on Enterprise Information Systems (ICEIS) 2020. Prague, Czech Republic.

I was awarded the ICEIS Best Student Paper Award Certificate for this publication.

"Security Architecture Framework for Enterprise (SAFE)" M. Graham, K. Falkner, C. Szabo and Y. Yarom, to appear in a book in the "Lecture Notes in Business Information Processing" (LNBIP) 2020 published by Springer.

N.B. Note author's change of name from Michelle McClintock to Michelle Graham.

1 Introduction

"It always seems impossible until it is done."
Nelson Mandela

In less than one year, between April 2018 and March 2019, there were 964 data breach notifications made under the Australian Notifiable Data Breaches (NDB) scheme by business, 60 per cent of which were malicious or criminal attacks. This is a 712 per cent increase in business notifications since the introduction of the NDB scheme and a change in reporting obligations, compared with the previous 12 months under a voluntary scheme (OAIC 2019). These startling statistics highlight that effective security has never been more important to Australian business and therefore individuals (Patterson 2003). However, very few companies have adopted a cohesive security strategy that encompasses the protection of all assets whether they be physical, digital or cognitive (Roeleven and Broer 2010). Basic online security behaviours are not being practiced by Australians and small to medium businesses. The Australian Cyber Security Centre had more than 13,672 reports of cybercrime from July to September 2019 and of those 11,461 were of sufficient merit to be referred to Australian law enforcement agencies (ASD 2020). High profile American security breaches such as the Verizon breach releasing more than 14 million customer records[1], the WannaCry ransomware computer hack giving access to NSA files[2] and the iCloud accounts extortion[3] highlight the global need for increased security resilience. Most information security programs manage each security instance departmentally, e.g. the finance department is responsible for risk management, the human resources department is responsible for security checks such as clearances, the ICT department is responsible for computer security and the facilities department is responsible for physical security. This approach is a complicated silo approach and uses many different security models, leading to duplication of resources, responsibility confusion and parts of the organisation being overlooked entirely (Roberti 2001; Shariati et al. 2011). Table 1 provides the common departmental approach to security management. An organisational security framework that includes all aspects of security – information, physical, technical process, people, cycles and risk; and has the flexibility of implementation to work with an organisation's budget, size and security mechanisms, could be used to mitigate these risks (Angelo 2001; Copeland 2017).

[1] http://www.zdnet.com/article/millions-verizon-customer-records-israeli-data/

[2] http://www.wired.co.uk/article/wannacry-ransomware-virus-patch

[3] https://www.theregister.co.uk/2017/04/07/icloud_wipe_threat/

Security Implementation	Managing Department
Computer security (application, network, data, information, e-commerce, cryptography)	IT
Physical security (security guards, locks, fences, gates)	Facilities
Human security (hiring process, security clearance)	Human Resources
Infrastructure security	Facilities
Operational security	Project Managers
Security architecture and design	IT
Access control	Facilities
Business continuity / disaster recover planning	Facilities
Information security governance and risk management	IT
Legal / regulations / compliance	Finance or Board of Directors

Table 1. Organisational Security Management Sample

This work conducted an extensive review of existing security frameworks – 27 in total – and the results indicate a comprehensive solution, with all aspects of security equally considered, does not exist. The analysis indicates a lack of research process in the development, a disjoint focus in either technical or policy, and a department or project focus for the implementation. Of those frameworks reviewed with a holistic approach, the most common framework methodology referenced is Enterprise Architecture (EA)(Fatolahi and Shams 2006; Gokhale 2010).

EA is a holistic method to guide the enterprise's people, information, processes and technologies, to achieve the most effective execution of the corporate vision and strategy (Gorazo 2014). An EA structure can reduce unnecessary costs, ad-hoc projects, unintentional reinvention, and provide corporate direction and relevance (Bente et al. 2012). The use of EA has a number of significant benefits, which include a reduction of IT expenditure, improved process innovation, standardised business processes, increase in risk management effectiveness, better strategic planning and improved business / IT alignment (Boucharas 2010; Haren 2011; Kreizman and Robertson 2006; Meyer et al. 2011). EA provides a methodology that reaches all parts of an organisation, addressing and breaking down the silo approach indicated in Table 1. If we are to test the theory of a complete holistic security model effecting every aspect of business, EA provides such a mechanism. The EA benefits also directly address the concerns of a lack of strategic security and could be harnessed when employing EA for the design of a security framework.

Notwithstanding the popularity and recent adoption of EA, the majority of EA frameworks do not have a security component (Agarwal et al. 2017; Saint-Louis and Lapalme 2016). The Zachman ontological framework (Zachman 1987) is one of the most widely accepted and implemented EA frameworks, however, despite Zachman's success, it does not include security in any form (Zachman 2001). This lack of security has been identified by others (Copeland 2017) who have used Zachman to create an enterprise security architecture (ESA). However, the results have been limited and none of the ESA's to date have utilised the Zachman concept of an ontology or ensured a strict adherence to the original definitions of Zachman (Zachman 1987). Zachman is the ontological language of EA and building on this concept, a security implementation of Zachman would be the first security ontology available – a defined organisational security language. Furthermore, most existing ESA's are from business white papers, and thus lack in-depth case study analysis, experimental replicability and research exploration (Tamm et al. 2011). The use of EA in security will also provide a single capture of all the organisation's security – a holistic security structure that is not yet available in a mature form.

The resulting research question for this work therefore is:

Will a holistic security model, using Enterprise Architecture, provide security benefits to an organisation more effectively than a piecemeal approach?

The contributions to practice and knowledge of this research are three fold. Firstly, the extension of the Enterprise Architecture Domain – the development of a standardised, comprehensive enterprise security architecture. There are some examples of similar research in the literature (Ertaul and Sudarsanam 2005; Ho 2002; Sherwood et al. 1995) however, they have a smaller scope and their purpose is not to cover the entire spectrum of an organisation. For example EA security governance frameworks tend to be very top heavy – ensuring the highest levels of the organisation are fulfilling their legal responsibilities but do not include implementation or technology (Anderson and Choobineh 2008). Also, most of the writings about enterprise security architecture are from business white papers and not from academia (Tamm et al. 2011) thus lacking research rigour. Secondly, the Security Domain – the development of the first fully researched security ontology and ESA based on security industry standards and security regulatory compliance and practices. The work is compliant with both NIST 800-53 (NIST 2013) and ISO/IEC 27002 (ISO 2013) and will provide an assurance that all aspects or the organisation have been considered for security. Finally, the design of a security dimension to the original EA framework - Zachman. Previous research which have created a security construct for the Zachman framework, have restricted their scope to a specific organisational focus, such as technical, instead of considering the organisation as a whole (Kreizman and Robertson 2006). Adherence of an ESA to the EA principles from Zachman extends the utility of the Zachman and provides a security dimension which has otherwise been lacking (Copeland 2017).

The opportunity for a reduction of security breaches, increased economic security and cyber resilience in organisations through a holistic approach to an organisational security framework with methodological supporting documentation, the importance and benefits of which have been mentioned in research, needed to be tested (Anderson 2008; Moulton and Coles 2003). This work developed a novel, fully researched enterprise security architecture (ESA) framework for organisations. The framework, analysed by industry professionals to determine if a holistic security model can address the much needed solution to the identified organisational security gaps and provide security benefits. The framework, the *Security Architecture Framework for Enterprises* (*SAFE*), is a comprehensive security solution based on the enterprise architecture methodology. The evaluation and analysis, backed by feedback from industry professionals, supports our hypothesis that a holistic security design using EA will provide security benefits to an organisation more effectively than a piecemeal approach. This research is a complete security solution and provides organisational defence in depth and in the current world climate, what could be more necessary to business (Copeland 2017).

This dissertation, a precis of which was published at ICEIS 2020 (McClintock et al. 2020), is organised as follows:

Background and Literature Review (Chapter 2)

A literature review, including search parameters, of the relevant domains – security, enterprise architecture and enterprise security architecture, is provided including general background relevant to the research, the significance of the research, prior knowledge and an analysis of related work. The justificatory knowledge (kernel theory) is included to inform the construction of the ESA artifact, as is the design principles developed from the literature review analysis.

Method (Chapter 3)

The chapter will discuss the methods used and the sources consulted to meet the research goals. This research used the Design Science Research (DSR) methodology to drive the research project and is explained in detail including rationale. Other methods selected and discussed include Grounded Theory Method for qualitative analysis, an Oppenheim questionnaire for the survey of the experts analysing the artifact, and the philosophy and approach of the research which were constructivist and inductive. To aid future research, a description of why these choices were made and other options were not selected, will also be provided.

Artifact Description (Chapter 4)

To describe the ESA artifact, a description of the design search (development) process and procedures that led to the artifact design is provided as well as a detailed description of the artifact itself. For the ESA, three levels of abstraction were developed and each will be provided in detail including how they were developed, the real world application and notable features. The ESA was also compliance mapped against security standards and this will be explained.

Evaluation (Chapter 5)

The evaluation chapter will include a description of the evaluation tool – an Oppenheim Survey, including how the survey questions were developed, written and mapped to the research motivation; the qualitative analysis process which used Grounded Theory Methodology coding and how this provided cyclical results through each coding phase, iterating to a richer data set after each phase. The explanation will also demonstrate the chosen evaluations' utility, validity, quality and efficacy (Gregor and Hevner 2013).

Discussion (Chapter 6)

The research discussion focuses on the significance and real world applications that have been identified from the design evaluation outcomes. The discussion links together the research question and design goals to the artifact and show how the novelty of the artifact design has bridged the research gap.

Conclusions (Chapter 7)

The artifact is an important step forward in finding a comprehensive solution to disparate organisational security solutions and demonstrates that the whole is clearly greater than the sum of its parts. This chapter concludes the research with the key findings, noting the artifact demonstrates the success of the design and describes future work options to expand and develop the research further.

2 Background and Literature Review

"Words are sacred. They deserve respect. If you get the right ones, in the right order, you can nudge the world a little."

Tom Stoppard

Enterprise security architecture (ESA) draws from two fields of research – security and enterprise architecture. This chapter gives an overview and the background of both the security and the enterprise architecture fields and then provides an overview of the work done to date to combine these two fields using a semi-systematic literature review. Key design principles were captured from the review to inform the development of the artifact and will be discussed in detail.

2.1 Enterprise Architecture

The enterprise architecture (EA) domain began with Zachman's 1987 seminal work (Zachman 1987). The paper notates the construction process done by all industries that design, engineer, and build large scale objects, e.g., airplanes and buildings. The notation, or architecture, is then applied to the engineering of organisations. The theory states that an organisation is at least as complex as a large construction project and should be engineered using a similar process, namely, one that defines the *context*, the *concept*, the *design*, the *build*, the *implementation* and the *use* of the organisation. EA provides a link between organisational goals and mission statements, through the organisational layers, down to the project level, and, similar to an initial engineering concept document, it is traceable to a final built product. The organisation's assets are defined in the EA as 1) people, 2) information, 3) process and 4) technology, and these are used to implement the vision of the organisation.

Academic rigour and growing research interest in developing EA theory is demonstrated from the last three decades with more than 4,000 journal articles and conference papers focusing on EA (Gampfer et al. 2018).

Figure 1 demonstrates how EA interacts with an organisation. The organisation is constructed through the language of EA and then the vision is implemented throughout the organisation using its assets, i.e. the people, information, process and technology. The people of an organisation represent any person who interacts with the organisation in any manner e.g., employees, customers, contractors, vendors, suppliers. Information or data refers to all data that has been generated by or given to the organisation in any form whether it be electronic or paper. Process is the way a company "does business" and includes processes, policy and procedures. Technology refers to the tools that facilitate the business process and store the business data; it is used by the people. EA provides a mechanism to link the vision to the rest of the organisation and its assets.

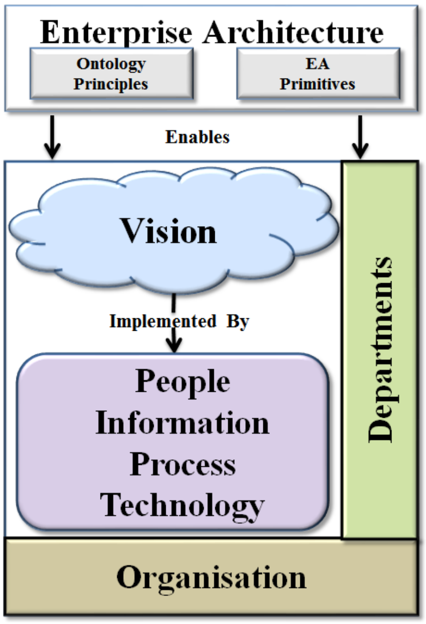
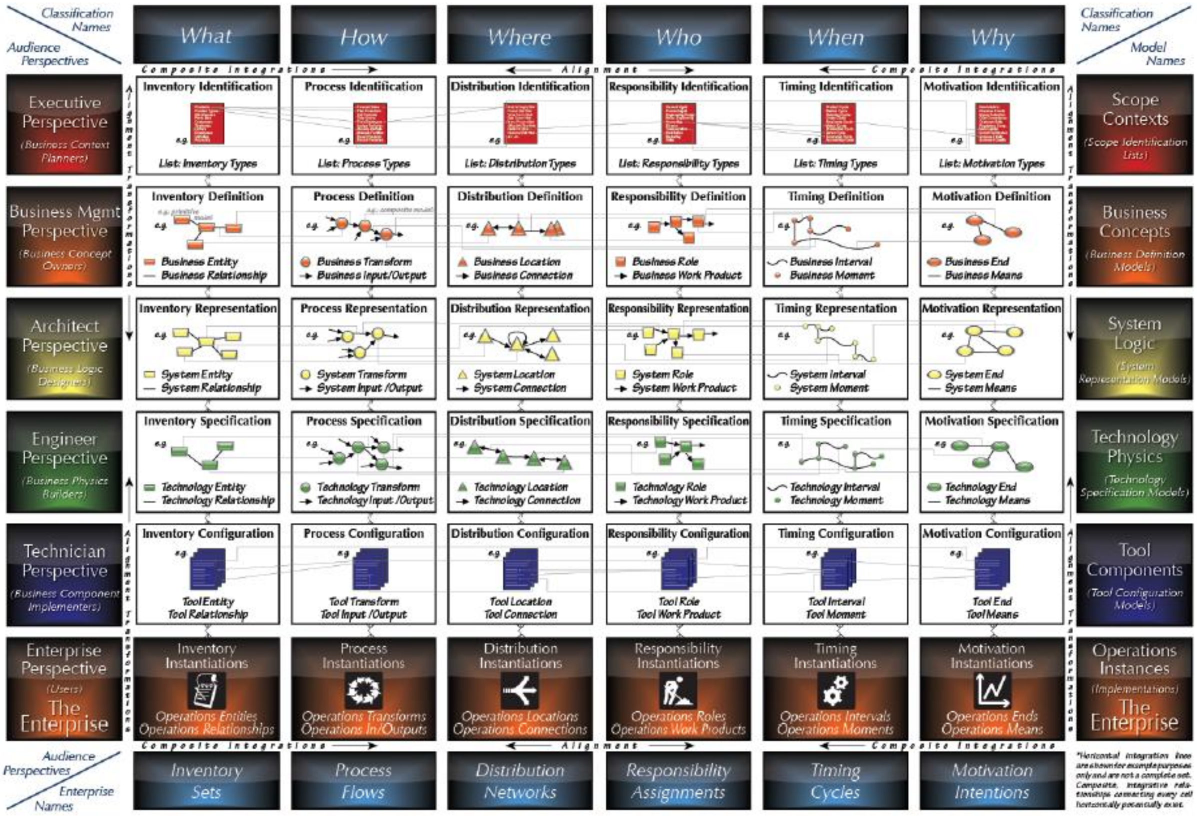


Figure 1: Enterprise Architecture Role in an Organisation

There are many EA frameworks in use by various organisations. The frameworks fall into two categories, *ontologies* and *prescriptive methodologies* (Gerber et al. 2020; Zachman 2016). An ontology or classification structure is a recognised vocabulary used to describe objects in a particular domain (Guarino et al. 2009). A prescriptive methodology is explicit in its requirements. Examples include describing how to create the artifact, describing what tools should be used, or what artifact should be purchased to be in compliance with the framework. The Zachman framework (see Figure 2) is an example of an ontology and is the adopted vocabulary for EA. The Zachman framework is also a structure independent of the tools and methods used in any particular business. This is useful because it can be adopted by any organisation without the need for specific, proprietary tools.



Classification Names / Audience Perspectives	What	How	Where	Who	When	Why	Classification Names / Model Names
Executive Perspective (Business Context Planners)	Inventory Identification e.g. List: Inventory Types	Process Identification e.g. List: Process Types	Distribution Identification e.g. List: Distribution Types	Responsibility Identification e.g. List: Responsibility Types	Timing Identification e.g. List: Timing Types	Motivation Identification e.g. List: Motivation Types	Scope Contexts (Scope Identification Lists)
Business Mgmt Perspective (Business Concept Owners)	Inventory Definition e.g. primitive model Business Entity Business Relationship	Process Definition e.g. composite model Business Transform Business Input/Output	Distribution Definition e.g. Business Location Business Connection	Responsibility Definition e.g. Business Role Business Work Product	Timing Definition e.g. Business Interval Business Moment	Motivation Definition e.g. Business End Business Means	Business Concepts (Business Definition Models)
Architect Perspective (Business Logic Designers)	Inventory Representation e.g. System Entity System Relationship	Process Representation e.g. System Transform System Input /Output	Distribution Representation e.g. System Location System Connection	Responsibility Representation e.g. System Role System Work Product	Timing Representation e.g. System Interval System Moment	Motivation Representation e.g. System End System Means	System Logic (System Representation Models)
Engineer Perspective (Business Physics Builders)	Inventory Specification e.g. Technology Entity Technology Relationship	Process Specification e.g. Technology Transform Technology Input /Output	Distribution Specification e.g. Technology Location Technology Connection	Responsibility Specification e.g. Technology Role Technology Work Product	Timing Specification e.g. Technology Interval Technology Moment	Motivation Specification e.g. Technology End Technology Means	Technology Physics (Technology Specification Models)
Technician Perspective (Business Component Implementers)	Inventory Configuration e.g. Tool Entity Tool Relationship	Process Configuration e.g. Tool Transform Tool Input /Output	Distribution Configuration e.g. Tool Location Tool Connection	Responsibility Configuration e.g. Tool Role Tool Work Product	Timing Configuration e.g. Tool Interval Tool Moment	Motivation Configuration e.g. Tool End Tool Means	Tool Components (Tool Configuration Models)
Enterprise Perspective (Users) The Enterprise	Inventory Instantiations Operations Entities Operations Relationships	Process Instantiations Operations Transforms Operations In/Outputs	Distribution Instantiations Operations Locations Operations Connections	Responsibility Instantiations Operations Roles Operations Work Products	Timing Instantiations Operations Intervals Operations Moments	Motivation Instantiations Operations Ends Operations Means	Operations Instances (Implementations) The Enterprise
Audience Perspectives / Enterprise Names	Inventory Sets	Process Flows	Distribution Networks	Responsibility Assignments	Timing Cycles	Motivation Intentions	*Horizontal integration lines are shown for example purposes only and are not a complete set. Composite, integrative relationships connecting every cell horizontally potentially exist.

Figure 2: Zachman Enterprise Architecture Framework (Zachman 2008)

The implementation of the Zachman 6 x 6 framework grid (Figure 2) would require an enterprise architect to use all 36 cells of the framework as a guide to describe a complex item like an organisation. The cells are called *primitive models*. Primitive models are the classification name of a required element in an EA framework. For example, a primitive model for an organisation's security could be "access control", and an organisation might decide on specific artifacts to fulfil it, e.g., security guard, firewall, door locks etc., depending on organisational needs and budget constraints. The rows of the framework are the *views* of an organisation, for example the executive view would be the management of the organisation. The columns are English interrogatives that describe the details of each view e.g., the what, how, where, who, when and why of the management perspective. The result is a complete explanation of the particular view of the organisation. A key principle for the Zachman framework is that a framework row is not an abstraction but a transformation, meaning each row is an entirely new view, not a decomposition of an earlier view. The ontology is used to organise and categorise the architectural artifacts, which are notated in the framework's grid. The architect works methodically through each row and identifies or develops the required architectural artifact(s) (an instance of the cell) for the organisation they have chosen to architect. Completion of the artifacts can be executed using existing instances of the artifact or created using various methods including a technical writer, or brainstorming or conceptualisation techniques.

In contrast to the Zachman framework, the majority of other frameworks are prescriptive and describe how to create the artifacts and the specific tools to use; or they name the instances specifically, for example a firewall as compared to a network security component. In this case a firewall is a specific instance of an implementation, but a network security component allows the implementation decision to be made by the organisation. Because these types of frameworks do not use ontological conventions, they are often used very effectively in conjunction with the Zachman framework. Some examples described below, include the TOGAF (Josey 2009), the GEAF (Bittler and Kreizman 2005), the FEAF - described later in this chapter (U.S.Government 2013) and the DoDAF (DoD 2010).

The Open Group Architecture Framework (TOGAF) (Josey 2009) is a process driven enterprise architecture framework that includes a method and a set of tools. The TOGAF methodology divides the organisation into four different architectural areas:

- Business architecture – a description of the business processes
- Data architecture – describes how data repositories are stored and used
- Application architecture - application design descriptions and how they interact with each other
- Technology architecture – describes the supporting software and hardware

The TOGAF recommends that it can be built in conjunction with such artifact driven frameworks like the Zachman. The combination of the process and the artifacts make a strong organisational EA. Chapter 21 of the TOGAF describes the security architecture and the approach is to apply policy to the enterprise architecture not have a specifically designed security architecture.

The Gartner Enterprise Architecture Framework (GEAF) (Bittler and Kreizman 2005) is described as an architecture process model that interacts with architectural frameworks. The Gartner view is that architecture is about environmental trends and strategy not engineering and the process driven GEAF reflects this belief. The model describes architecting and documenting requirements, principles and models to move an organisation from the present to their desired future state. This model does not include security however Gartner have created the Gartner Enterprise Information Security Architecture.

The Department of Defense Architecture Framework (DoDAF) (DoD 2010) is an overarching supporting framework to support decision making for all managers in the United States Department of Defense through sharing of information – organised data. The second version of the DoDAF moved the framework away from its original focus of architectural artifacts and products to architecture data and its collection, store and structures. Data is visualised through models and when completed become views and collectively viewpoints. The framework continues to work effectively with NIST 800-53 (NIST 2010) – the U.S.A. Federal Government's security framework.

Perhaps indicative of its historical importance, most frameworks, including the TOGAF, GEAF, FEAF and DoDAF, actually have their origins in the Zachman framework, which is why they complement and are used effectively with the Zachman framework. The following discussion provides a detailed explanation of the rows and columns in the Zachman framework (Figure 2).

Audience Perspectives / Stages of Reification

The perspectives or rows of the Zachman framework constitute a complete way to view an organisation from the people who would initially identify the business concept (the first row) to the final instantiation of the running organisation (the final row). Each stage or row of the reification process, moving down the framework, is a transformation rather than a more detailed view of the previous perspective – that is, it is a completely separate view that is not reliant or evolved from the previous view.

Executive Perspective / Identification (Row 1)

The executive perspective is defined at the inception of a company, generally at the Board of Directors level. It is the identification of the concept for the business and is externally focused. The definition indicates the boundaries of where the enterprise will sit in the market or operating domain. The interrogatives in this row provide detailed lists of these boundaries including responsibilities, processes, motivation and timings. Row 6 is the business implementation of this perspective.

Business Management Perspective / Definition (Row 2)

The business management perspective is internally focused in that it defines the executive, external concept for the enterprise, into a business model of enterprise design and operational reality. This is used by the enterprise to implement the logical depiction into the building blocks of the enterprise.

Architect Perspective / Representation (Row 3)

The architect perspective represents the business model as the required pieces or building blocks of the enterprise and indicates how they will interact with each other. At this point, such considerations as high level technology categories e.g. database; and the alignment to business of that technology, are identified for the purpose of turning the ideas from the business management perspective into an organisational reality. The concepts from Row 2 are now more formalized.

Engineer Perspective / Specification (Row 4)

The requirements and specifications of the systems of the organisation are designed at the engineering perspective. It is the creation of the detailed designs, which will transform and implement the conceptual building blocks – the physical depiction of the earlier logical descriptions. The designs can include such detail as nodes and edges, operating systems and middleware.

Technician Perspective / Configuration (Row 5)

The technician perspective is the business component level. The detailed designs of the organisation from Row 4 are implemented using specific tooling configurations.

Enterprise Perspective / Instantiation (Row 6)

The enterprise perspective is the instantiation of the reification process from Row 1 to 5, outworked and demonstrated in the functioning organisation. At this stage of the framework, the artifacts are the actual organisation not the architectural abstractions like the previous five rows.

Classification Names

What – Things (Column 1)

The "what" is the inventory sets of the organisation, that is, the sets of things that are tracked and managed for the organisation to function. This can be in the form of people or information and governs how these inventory items are defined, represented, specified and configured. The inventory models are explained pictorially in terms of the entity itself and the relationships between the entities (the enterprise inventories of assets).

How – Process (Column 2)

The "how" refers to the processing of the organisation through various process types. At this point the definition, representation, specification and configuration of the processes are created enterprise transformations. The processes provide the transformation models of the assets from the inputs and outputs of the organisation and are depicted using process flows.

Where – Location (Column 3)

Distribution networks depicted using network models are the "where". The distribution type for the inventories, including business location, system location, technology location or tool location, provide the network with the operations locations and connections. It is particularly important for Column 3 to map its relationship with the other columns as it provides the network maps that the other columns feed into – including data, processing and logic or enterprise storage, transportation or transmission capacities.

Who – People (Column 4)

The responsibility assignments are allocated to the organisational stakeholders in Column 4 – the "who". Those who are responsible are identified (note this can be both internal and external e.g. staff and clients), their roles are defined, represented, specified and configured. The overall view of this is an enterprise work performance model. The roles and the work products of those roles are present in the functioning organisation and the defined responsibilities are often used for managing performance. Because of the nature of the "who" – that is people; there is no standard notation for representing the information from Column 4, with the exception of organisational charts and workflow models. Also, some modern organisations tend to have globalisation issues due to the new nature of an international workforce.

When – Events (Column 5)

The "when" is about timing cycles, the intervals and moments of the organisation and how those are identified as types, defined, represented, specified and configured within the architecture and the organisation. The timing instantiations of Column 5 are the operations intervals and moments and are often represented as distance (due to globalisation effects), relative time or operating hours. These dynamic models are the enterprise cycle times.

Why – Ends (Column 6)

The motivations of the organisation can be found in Column 6 – "why". The objectives and strategies explain why the organisation is in business, how those motivations and intentions are outworked through ends and means. The thoughtful values or enterprise objectives from this column will drive the organisation through issues and decision making cycles. The motivation models are described using definitions, representations, specifications and configurations.

Model Names

The model names, indicated in the right hand edge column of Figure 2, describe how the views are modelled (pictorially) for explanation purposes. Each of the columns in the framework (indicated in Column 1 of Table 2) is represented by a particular type. Like data types in programming, enterprise architecture has six types to describe content. The types and the corresponding column are described in Table 2.

Column Name	Enterprise Architecture Type	Example Data for Executive Perspective
What	Inventory	Product types
How	Process	Forecast sales
Where	Distribution	Parts distribution network
Who	Responsibility	General management
When	Timing	Market cycle
Why	Motivation	Revenue growth

Table 2: Enterprise architecture types by column (Zachman 2008)

The models are created for the audience perspective (see Table 3). For example, an executive would want to identify the scope contexts during the execution of their role because this will give them the most strategic level of knowledge for the executive to make decisions for the organisation. An architect would identify all types for each audience as indicated in the Example Data from Table 2. The outcome is a complete set of data for all 36 cells of Figure 2.

Row (Audience)	**Model Name**	**Perspective**
Executive Perspective	Scope Contexts	Identification
Business Perspective	Business Concepts	Definition
Architect Perspective	System Logic	Representation
Engineer Perspective	Technology Physics	Specification
Technician Perspective	Tool Components	Configuration
Enterprise Perspective	Operation Instances	Instantiations

Table 3: Enterprise architecture models by row perspectives (Zachman 2008)

Enterprise Names

The final row in Figure 2 is the Enterprise Names. These are the aggregated names for all six data sets of each interrogative column. For example, the six rows of the How column are organisational processes for all six perspectives and the group name for the six is Process Flows. Therefore, this column indicates the process flows of the organisation. The other aggregated enterprise names are Inventory Sets, Distribution Networks, Responsibility Assignments, Timing Cycles and Motivation Intentions.

Zachman and Security

In 2001, John Zachman wrote a paper about the intersection of security and EA (Zachman 2001). His key perspective is that his framework already supports security and does not need any additions. He is purporting role-based security and focuses on the technical implementation of security, particularly recommending the combination of EA and positive identification of individuals accessing the enterprise as the essence of organisational security. The paper also provides a discussion directing the external interfaces of the enterprise to encrypt files and provides two technical security architectures; “Systems Centric Approach” or “User Centric Approach”. Both related to the placement of the security technologies within the system that is consistent with his recommendation for physical access control and encryption of files leaving the organisation. Finally, Zachman states: "I probably don't have to make this observation, but Security is only one benefit (and only one rather incidental benefit at that) to having Enterprise Architecture."

Since the publication of this paper, Zachman has remained quiet on the topic of security and left it to security professionals who agree that organisational security is infinitely complex (Juntunen and Virta 2019) and requires all aspects of an organisation to begin with security in mind to achieve organisational security in depth and security resilience (Crossler et al. 2017).

2.2 Security

Since the first virus named "Brain", in 1986 (Highland 1988), and the Morris Worm in 1988 (Orman 2003), information security has become essential for organisations everywhere. Through the 1990s the security approaches were ad hoc and reactionary (Chaisiri and Ko 2016) however, it is now clear that more thoughtful methodologies are required to maintain a secure defence (Shariati et al. 2011). At the same time, the societal uptake of computing has enabled cyber-corporate espionage, providing companies with tangible reasons for the security of their organisations, namely the protection of the assets.

The need for organisational security initially began with the protection of information stored on computers and the physical security of organisations however, this has broadened to include all departments within an organisation. As the organisation has evolved, most departments have retained individual control over the security matters they have put in place. This implies that each security solution is managed separately, which results in a lack of a cohesive strategy (Eloff and Eloff 2005). Some of the most common yet individually managed security implementations today are:

- Computer security (application, network, data, information, e-commerce, cryptography)
- Physical security (security guards, locks, fences, gates)

- Human security (hiring process, security clearance)
- Infrastructure security
- Operational security
- Security architecture and design
- Access control
- Business continuity / disaster recover planning
- Information security governance and risk management
- Legal / regulations / compliance

Holistic frameworks for organisational security, which is those that view the organisation's security holistically rather than each security instance separately, are limited. One example is governance frameworks that are defined by the IT Governance Institute (ITGI 2001) as the "set of responsibilities and practices exercised by the board and executive management". However, governance frameworks focus on management fulfilling their legal requirements, which does include security. But they do not address security any lower in the organisation than management.

The other most common response to organisational security has a technical focus such as computer and information security (Anderson 2001). Unfortunately, it is still very common for a company to believe that organisational security is solely about virus defence and firewalls. When asked, most do not include broader security mechanisms in their definitions of security, other than computer security, and the effect is a lack of awareness for the need of a broader security strategy until a security incident occurs (ISACA 2009). As Anderson (2008) states, "Security engineering requires cross-disciplinary expertise, ranging from cryptography and computer security through hardware tamper-resistance and formal methods to a knowledge of economics, applied psychology, organizations and the law." The solutions are not just technical and require a broader response.

Organisational Security Principles and Standards

Security standards are used as a benchmark by organisations to provide a level of assurance for their security programs. As Siponen and Wilson (2009) state, "By adopting an authoritative guideline, organizations can demonstrate their commitment to secure business practices; organisations may then apply for certification, accreditation, or a security-maturity classification attesting to their compliance to a set of rules and practices." The choice of the standard or standards is based on the requirements of the organisation's security needs. Following is a discussion of the most commonly identified standards, summarised in Table 4.

International Information Systems Security Certification Consortium — Common Body of Knowledge ([ISC]^2 CBK) (Contesti et al. 2007)

ISC^2 is an internationally recognised organisation that holds a continually developing body of knowledge for information security. The CBK serves as a common framework of terms and principles, which are used to define global industry information security standards (Theoharidou and Gritzalis 2007).

National Institute of Standards and Technology (NIST) (NIST 2013)

NIST is the federal technology agency for the United States that "works with industry to develop and apply technology, measurements, and standards" through research and development of current and emerging technologies (NIST 2013). The information technology branch specialises in areas such as:

- Biometrics
- Computer Forensics
- Computer Security
- Conformance Testing
- Cybersecurity
- Data Mining
- Data and Informatics
- Health IT
- Imaging
- Information Delivery Systems

- Networking
- Scientific Computing
- Software Testing Metrics
- Telecommunications/Wireless

NIST has two frameworks for adoption in security. The first is the NIST Cyber Security Framework (NIST CSF) which is a framework that can be used but any organisation to develop a security program. The second is the NIST 800-53 which is specifically developed to keep the U.S. Federal Government secure and is more than 10 times longer than the NIST CSF, demonstrating its complexity and prescriptiveness.

International Organisation for Standardization / International Electro-technical Commission (ISO/IEC) 27000 and 17799 (ISO 2013)

The ISO provides "specifications for products, services and systems, to ensure quality, safety and efficiency" specifically for the benefit of international trade (ISO 2013). The development of a standard is done through a consensus of international industry experts on the particular subject as requested or required. ISO 27000 is the family of standards (includes 27001, 27002, 27003, 27004) for an information security management system and ISO 17799 is the code of practice for information security management (ISO 2013).

Control Objectives for Information and Related Technology (COBIT) Security (De Haes et al. 2013)

COBIT is a management and governance framework for information technology created by the Information Systems Audit and Control Association (ISACA). Initially COBIT was created by auditors for their use in organisations but the framework, now in its 5th iteration, is used more broadly as a practical solution to guide and implement governance principles (De Haes et al. 2013). The framework has identified 316 objectives for an organisation to achieve in order to be in compliance with COBIT, however, only 21 are directly security related indicating that security is not the focus of this framework (von Solms 2005).

Information Technology Infrastructure Library (ITIL) Security (Clinch 2009)

ITIL provides guidance on how to use information technology as a tool to "facilitate business change, transformation and growth"(ITIL 2015). Similar to COBIT Security, ITIL has security as a part of its framework however, it is not the focus. Of note is that the information security management content in ITIL is directly mapped to the ISO/IEC 27001 and 27002 standards and therefore a more accurate reference would be ISO/IEC (Clinch 2009; ISO 2013).

Author	Title	Geographical Remit	Purpose and Features
(Contesti et al. 2007)	International Information Systems Security Certification Consortium — Common Body of Knowledge ([ISC]² CBK)	International	Common framework of terms and principles that defines global security standards.
(NIST 2013)	National Institute of Standards and Technology 800-53	U.S.A. (referenced internationally)	Provides recommended security controls in federal information systems and for organisations and industry that work with federal agencies.
(ISO 2013)	International Organisation for Standardization / International Electrotechnical Commission (ISO/IEC) 27000 and 17799	International	International standards that ensure quality, safety and efficiency. Used particularly in international transactions or trade.
(De Haes et al. 2013)	Control Objectives for Information and Related Technology (COBIT) Security	International	Created by Information Systems Audit and Control Association (ISACA) as a set of governance principles and processes for the management of information technology.
(Clinch 2009)	Information Technology Infrastructure Library (ITIL) Security	U.K. (referenced internationally)	Codifies best practices in information technology gathered from many sources including industry.

Table 4: Commonly Referenced Security Standards

2.3 Enterprise Security Architecture

The earliest enterprise security architecture (ESA) frameworks were developed in 1995 (Sherwood et al. 1995) and the few approaches available all agree that "the problem is that no standardised, comprehensive information security architecture currently exists" (Copeland 2017; Eloff and Eloff 2005). Our analysis of existing work identified five surveys of ESA frameworks (Table 5), which give a broad domain overview of the status of Enterprise Security Architecture as a discipline. The surveys are discussed below.

Year	Author	Notable Features and Focus
2011	Shariati, Bahmani & Shams	The interoperability of organisational architectures and the direct conflict with security principles
2009	Oda, Fu & Zhu	The effectiveness of ESA frameworks on certain criteria including business architecture, information architecture and technology architecture
2007	Da Veiga & Eloff	Information security governance frameworks
2006	Claycomb & Shin	Enterprise security management architectures for mobile devices – particularly criteria authentication, access control and audit
2005	Eloff and Eloff	ESA frameworks from various fields including risk management and international standards.

Table 5: Existing ESA Surveys Reviewed

Existing Surveys of Enterprise Security Architecture Frameworks

The Shariati, Bahmani and Shams (Shariati et al. 2011) survey of five frameworks focuses on the importance of interoperability for organisational architectures, perceiving an organisation as a holistic seamless flow of information rather than compartments, which is a key requirement of enterprise architecture. The issue raised is that interoperability is in a direct conflict with the principles of security. Such security principles as "need to know", physical defence of assets and confidentiality confirm the struggle. The paper's goal is to identify holistic security frameworks that support interoperability. The review provides a description of interoperability aspects and its importance in frameworks, specifically in the areas of technical, organisational and semantic. This inclusion helps the reader better understand the focus of the research. Furthermore, the holistic versus partial section provides a convincing discussion about the utility of holistic frameworks rather than partial frameworks which tend to have a limited domain specific use. The paper does not include a recommendation for a suggested framework that would incorporate interoperability. The Oda et al. review (Oda et al. 2009) aims to determine the effectiveness of ESA frameworks based on a number of criteria including business architecture, information architecture, technology architecture, security architecture, levels of abstraction and case studies. The review/survey looks at three frameworks, including the Zachman framework (Zachman 2011), which does not have a security element but is stated as being the foundation of all enterprise information architecture frameworks, and is included on that basis. The purpose is to determine the effectiveness of the architectures. The paper concludes with a case study of the enterprise information security architecture at the Oakland University in the U.S. The three architectures are explained and analysed in detail. However, the survey only considers two security architectures. Moreover, the Oakland University case study does not consider the introduced criteria.

The Da Veiga and Eloff work (Veiga and Eloff 2007) is centred on governance and, while not titled a review paper, does have a comprehensive "existing approaches" section and reviews four information security governance frameworks. The purpose of the paper is to derive a list of components (a principle or a security control or both) for the development of a new security governance framework. The review derives six components (leadership and governance; security management and organisation; security policies; security program management; user security management; technology protection and operations) placed into three categories: strategic, managerial or operational, and technical. It is not clear from the research why the particular frameworks were chosen because no selection criteria are given.

The 2006 Claycomb and Shin (Claycomb and Shin 2006) research is focused on enterprise security management architectures for mobile devices that use all of the aspects of organisational architectures. It reviews two related works using the criteria authentication, access control and audit. The review provides a detailed description of the suggested new security architecture including diagram specifications and a proof of concept implementation. Although the paper uses the phrase 'enterprise architecture', no reference to enterprise architecture principles is present and there are only two frameworks surveyed, which limits the analysis. The choice of criteria also indicates a technical focus, which would not provide a holistic security view of the organisation. In contrast, the chosen criteria in this research provides a complete view of an organisation choosing EA specifically because of the holistic aspect.

The Eloff and Eloff survey (Eloff and Eloff 2005) reviews five existing ESA frameworks from various fields including risk management and international standards. The survey then draws from the analysis to develop five principles for an ESA framework. The five principles are based on procedures, technology, and people, and are namely: holistic, security control synchronization, risk management, life-cycle implementation, and measures. The inherent challenge with this list of principles is its broadness, in that the scope of the principles is not defined and therefore it might be difficult to develop a comprehensive security architecture that meets all principles. The proposed principles in this work focus on security and enterprise architecture.

SUMMARY

This review of related work indicates a need for a new ESA frameworks survey as the most recent survey was in 2010 (Shariati et al. 2011) and the largest surveys have five frameworks (Eloff and Eloff 2005; Shariati et al. 2011). Given the changes in the security environment, the development of new works, the previous coverage and the time lapse, the conclusion is a comprehensive, criteria-based survey of ESAs was required and is beneficial for the domain.

2.4 Enterprise Security Architecture Review

This section presents a semi-systematic literature review, conducted as a part of this research, within organisational security structures and the research used the learning to establish principles for the foundation of the ESA design.

Google Scholar and the ACM Digital Library database were searched and citations were followed for articles about enterprise security architecture. Google search terms included those associated with 'enterprise ('organisation', 'management', 'information', 'business', 'information systems', 'information technology') AND security AND architecture ('information landscape', 'structure', 'process', 'governance')' AND framework ('model', 'plan')'.

Inclusion	Exclusion
Security focus	No security
Business intent	No framework
Architectural focus	Prior to 1995
Research papers and reports or white papers	Theoretical papers
1995 - 2020	

Table 6: Inclusion/exclusion criteria

Relevant works matching the inclusion/exclusion criteria (Table 6) were entered into EndNote X7.3.1 with the PDF as an attachment. The results were used for classification and analysis.

The inclusion and exclusion criteria were determined based on the simplest version of an ESA framework. An ESA should have security, architecture and business as its focus. If the work was not a framework or security was not the focus, it was excluded. This was done to provide the broadest definition and therefore capture all relevant ESA frameworks developed during the last

26 years. EA frameworks that focused on the organisation but had not included security were excluded, such as Abdullah and Galal-Edeen (2006), Covington and Jahangir(2009), Lange et al. (2012) and Mykhashchuk (2011). Similarly security-based principles papers that did not include a recommended framework were excluded, such as Anderson and Choobineh (2008), Hone and Eloff (2002), Ohki et al. (2009) and Siponen and Willison (2009).

Table 7 is the list of the 27 frameworks that directly matched the criteria and intent. These frameworks were further reviewed and analysed and the following discussion looks at the key aspects that were identified during this analysis; EA principles, technology and people, security standards, ontologies and Zachman based ESA. The importance of the consistencies and differences are observed and explained.

Year	Author	Framework name	Notable features
(1995)	Sherwood, Clark, Lynas	Sherwood Applied Business Security Architecture	Project based implementation
(2000)	Sandhu	The Objective and Model - Architecture Mechanism Framework	Based on a Network Protocol Stack with a many to many relationship between layers
(2002)	Ho	Security Management Framework	Information security professional requirements, Zachman based framework – 6 Columns (Data, Function, Network, People, Time, Motivation)
(2003)	Trcek	Information Systems Security Management Framework	9 Planes (Technology, Organisation, Legislation, Human Interactions, Human-Machine Interactions, Crypto Protocols, Crypto Primitives, Assets, Physical Security)
(2003)	Rees, Bandyopadhyay, Spafford	Policy Framework for Interpreting Risk in E-Business Security	4 Phases (Assess, Plan, Deliver, Operate)
(2004)	Posthumus, Von Solms	Information Security Governance Framework	4 Aspects (Legal, Business, Infrastructure, Standards)
(2005)	Ertaul, Sudarsanam	Enterprise Security Plan	Column 6 of Zachman (Why) replaced with "External Requirements and Constraints"
(2005)	Eloff, Eloff	Information Security Architecture	5 Requirements (Holistic, Controls, Comprehensive, Life-cycle, Measurable)
(2006)	Killmeyer	Information Security Architecture	A “How-To” book for implementing an Information Security Architecture
(2006)	Scholtz	Gartner Enterprise Information Security Architecture	3 Layered Pyramid (Conceptual, Logical, Implementation)

(2008)	Anderson, Rachamadugu	Roadmap for Information Security Across the Enterprise	3 Tiers (Profile, Plan, Protect)
(2008)	Sun, Chen	Intelligent Enterprise Information Security Architecture	Based on the 7 layers of the Open Systems Interconnection (OSI) Reference Model
(2009)	Korhonen, Yildiz, Mykkanen	Service Orientated Architecture Security Governance Model	4 Layers (Strategic, Tactical, Operational, Real-Time)
(2009)	Shen, Lin, Rohm	Enterprise Security Architecture Framework	3 Noted dimensions - Framework, Policy and Technical
(2010)	NIST, OMB, FCIO	US Federal Enterprise Architecture Security and Privacy Policy	3 Stage Methodology - Identification, Analysis, Selection
(2011)	Saleh, Alfantookh	Information Security Risk Management Framework	5 Domains (Strategy, Technology, Organization, People, Environment)
(2011)	TOGAF	Open Enterprise Security Architecture	4 Dimensions (Program Management, Governance, Enterprise Architecture, Operations)
(2013)	ISO/IEC 27000	International Standard for Information Technology - Security	14 Security Control Clauses (Policy, Organisation, Human Resources, Asset Management, Access Control, Cryptography, Physical and Environmental, Operations, Communications, System Acquisition Development and Maintenance, Supplier Relationships, Incident Management, Business Continuity, Compliance)
(2014)	Atoum, Otoom, Ali	Holistic Cyber Security Implementation Framework	A framework / strategy to determine current security level and gap analysis for new security level
(2014)	Webb, Ahmad, Maynard, Shanks	Situation Aware - Information Security Risk Management Model	Collection, analysis and reporting of organisational risk information to improve information security risk assessment
(2015)	Luhach & Luhach	Logical Security Framework	Framework based on Service Orientated Architecture to reduce security attacks
(2015)	DiMase, Collier, Heffner, Linkov	Cyber Physical Systems Security Framework	Cyber physical system security framework using systems engineering principles
(2016)	Jeganathan	Enterprise Security Architecture Framework	An enterprise security architecture framework using people, processes and technologies
(2016)	Bernroider, Margiol, Taudes	Information Security Management Assessment Framework	Design Science Research to create a security critical infrastructure framework - 4 dimensions - security ambition, security process, resilience, business value
(2017)	Bazi, Hassanzadeh, Moeini	Cloud migration framework	A secure cloud computing framework using meta-synthesis - uses 7 stage maturity model

(2018)	Berkel, Singh, van Sinderen	Smart Cities Information Security Architecture	A target enterprise architecture using a meta-model for security to include system developers, ICT experts, administrators, managers and policy makers
(2019)	Mayer, Aubert, Grandry, Feltus, Goettelmann, Wieringa	EAM-ISSRM (Enterprise Architecture Management – Information Systems Security Risk Management)	Assets, risk and risk treatment model

Table 7: Existing Security Frameworks Reviewed

Enterprise Architecture Principles

Among the reviewed frameworks, the Zachman EA framework is the most directly referenced. Sherwood et al. (1995), Ho (2002), Ertaul et al. (2005) and Mayer et al. (2019) all discuss the significant influence the Zachman EA has had on the development of their security frameworks. As an example, the matrices developed by the three works all include at least five of the six English interrogatives of the Zachman framework (what, how, where, who, when, why) and two of the three use all of the interrogatives. Moreover, the audience perspectives identified by Zachman (executive, business management, architect, engineer, technician, enterprise) are also used by all three authors. These three papers agree there is a missing security element to the Zachman and are attempting to remedy the issue with their research. One other paper also references the Zachman framework. Shen et al. (2009), states their framework is a security dimension of the Zachman framework. However, the Zachman principles, theory and structure are not evident in the developed framework.

General EA principles are referenced in four other frameworks, Scholtz (2006), Anderson et al. (2008), Jeganathan (2016) and the U.S. Federal Enterprise Architecture Security and Privacy Policy (FEA-SPP) (NIST 2010). Scholtz (2006), Jeganathan (2016) and Anderson et al. (2008) use EA principles such as translating business requirements into operational solutions; linking organisational vision to enterprise processes, policies and technology; creating a holistic integration of business process management and technical infrastructure; the use of terms such as "viewpoint" instead of perspective, (Zachman inference), “as-is” and “to-be” (the traditional method of EA); the concept of an ESA should be woven into the organisation’s EA not a stand-alone function; the identification of artifacts in the ESA; and ESA is a top-down approach as is EA. The FEA-SPP (NIST 2010), which is for a federal U.S. agency, is fully integrated into the Federal Enterprise Architecture (FEA) and uses all the principles from this extensive, government specific, EA methodology.

The Federal Enterprise Architecture Framework (FEAF) (U.S.Government 2013) (see Figure 3) for the United States (U.S.) Government was created as a common framework for the federal agencies to use and therefore improve interoperability and communication (Sessions 2007). The framework is comprehensive and very large in its implementation, as expected given the U.S. Government is one of the most complex organisations in the world. It is based on five performance reference models: business, service, components, technical, and data. The FEAF is an effective EA however, the challenge is the use of it outside the U.S. federal public sector. It is so large in scale that its application in a private organisation would be incredibly difficult. There was only one reference to the FEAF in our survey which was the security section of the FEAF (NIST 2010).

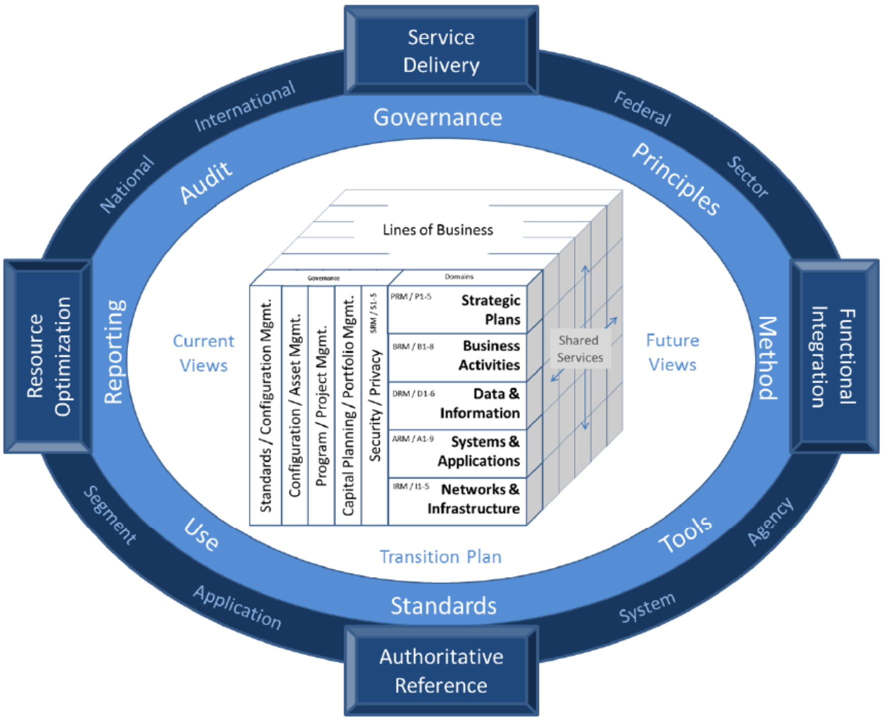


Figure 3: The Federal Enterprise Architecture Framework (U.S.Government 2013)

Technology, People, Process and Information

The assets of an organisation are technology, people, process and information. Most organisations' security is based on technology and policy, both of which are easier to create or buy and implement than security for people, information or process, which is more time consuming and expensive (Roberti 2001). It is still very common for a company to believe that organisational security is solely about virus defence and firewalls (ISACA 2009); both of which are resolved with policy and technology. Most do not include broader organisational security mechanisms in their definitions of security, other than computer security technology and the policies surrounding the technology. The effect is a lack of an organisational security strategy or architecture (ISACA 2009; Juntunen and Virta 2019). Securing these assets is therefore critical and the focus of the assets in the security frameworks reviewed is discussed below.

An example of a framework with a purpose that satisfies the criteria: technology, process and people, is the Eloff and Eloff (Eloff and Eloff 2005) framework. Any computer asset that is used in the running of the day to day business is defined by the authors as technical and includes software, products, application systems, hardware and networks. The framework has developed its own process model which is a continuous feedback life-cycle approach for ESA. People security incorporates security into the organisational culture, training and awareness programs which may include legal and ethical aspects. The framework effectively takes all aspects of an organisation's assets into consideration and demonstrates an all-encompassing purpose.

The focus of both Sandhu (2000) and Sun et al. (2008) is a technical security architecture for the organisation. As an example, Sandhu has created an architecture and has trialled it in a distributed role-based access control application. However, the goal of the architecture is broader and included in the research are organisational perspectives, architectural layers, artifacts, identifying objectives and creating architecture and mechanisms to implement the objectives organisationally. Similarly, Sun et al. have focused on a security aspect of Service Orientated Architecture (SOA) for the technical aspects of an organisation. Both papers are using the Open Systems Interconnection (OSI) reference model to structure their technical architectures. SOA is also the focus of the Korhonen et al. (2009) research but the authors chose a governance view rather than a technical one.

There are three research papers included in this review that provide a security architecture for technology supporting E-Business, two of these were published in 2003, just as E-Commerce began to exponentially grow. They are Trcek (2003) and Rees et al. (2003). Both emphasize the security challenges of the Internet marketplace, the legal issues involved, the policies which need to be developed, technical recommendations, and the management of an E-Business product lifecycle. A later paper from Luhach and Luhach (2015) provides a technical solution to E-Business with a logical security framework using service orientated architecture and validated on Oscommerce (https://www.oscommerce.com/).

Only four frameworks discuss people in their security architectures. Sherwood et al. (1995) has placed a lot of emphasis on the human aspect of their framework including expertise, education, training, experience, appraisals, trustworthy, security vetting etc. Eloff and Eloff (2005) have considered the human–machine interaction, human relationships, security culture and awareness of staff, training, ethics and legal issues for security professionals. Saleh and Alfantookh (2011) discuss the importance of human expertise, employee morale, loyalty, ethics, training and human resource security. Finally the International Standard ISO/IEC 27000 (ISO 2013) dedicates a chapter to human resource security including screening, qualifications, trust, promotion, job specifications etc. ISACA (2009) states that if the human factors of an organisation, such as culture, governance and training are not taken care of, the architecture and the security of the organisation will always be at risk.

Security Standards

Security standards are used as a benchmark by organisations to provide a level of assurance for their security programs (Siponen and Willison 2009). The standards identified after analysis of the 27 frameworks were NIST 800-39, 800-53 and 800-55 (6 frameworks), ISO/IEC 27002 (10 frameworks), ITIL (2 frameworks), CIA (4 frameworks), COBIT (De Haes et al. 2013) (2 frameworks), Standard of Good Practice for Information Security (2014) (1 framework) and 6 Sigma (Linderman et al. 2003) (1 framework). Eight of the 27 papers used no security standard in the development of their framework.

Traditionally confidentiality, integrity and availability (CIA) are the foundational security objectives for all organisations (Stoneburner 2001), and for completeness accountability and assurance are usually included with the triad. Two papers have chosen, for compliance and assurance purposes, the CIA principles rather than a more prescriptive industry standard such as NIST 800-53 or ISO/IEC 27002. Posthumus et al. (2004) present a governance security framework which is strategic in nature, usually providing overarching guidance to an organisation. Choosing a more detailed security standard would be very difficult to implement for a governance structure, therefore the choice is logical. Killmeyer (2006) has developed an organisational security program, commercially available, which is based on CIA. Due to the commercial nature of the program, perhaps the restrictive requirements of a security standard like NIST 800-53 or ISO/IEC 27002 could have limited the scope of work.

12 out of 27 frameworks state explicitly that they are in compliance with at least one industry standard. Four frameworks state they are in compliance with two standards. One claimed compliance with three standards. The most common standard referenced is ISO/IEC 27002 (58% of those claiming standard compliance), and the second most common is NIST 800-53 (25% of those claiming standard compliance), which is expected given both are from highly respected organisations in the security industry. ISO/IEC 27002 is the only standard that can also be considered a framework due to its extensive subject matter and it is used as a standard reference and also as a framework to be analysed.

The Open Enterprise Security Architecture (Wahe 2011) framework, which is a part of the TOGAF (Haren 2011), a large and well respected enterprise architecture, emphasises the importance of using industry standards in the development of the framework. The two standards adopted throughout this framework are NIST 800-53 (NIST 2013) and ISO/IEC 27002 (ISO 2013), and the paper recognises both as well-established and adopted worldwide in the security industry. The use of these standards provides a security assurance to the framework while offering holistic security knowledge for completeness of the framework.

Ontologies

The utility of a framework being an ontology is that an ontology is made up of primitive models or objects, which can be used by an organisation to create an architecture — this is how the Zachman is implemented. These primitive models are the classification name of a required cell in the framework. A descriptive representation of the primitive model is an artifact which is the example of the classification. To clarify with a security example: a primitive model might be access control. A security requirement of an enterprise is the access control. An artifact of access control might be a security guard. The security guard is the descriptive representation of access control. Primitive models are used because they are proscriptive not prescriptive in nature. In the example, the organisation knows it must have access control (the primitive model), but it is free to determine what the implementation (or artifact) is based on budget, company size, staffing number etc. As a part of the analysis on the identified frameworks, it was determined if they are using any primitive models, therefore creating an ontology, or if their framework was artifact based — requiring specific security instances.

The results indicated that there are no security frameworks that are completely ontology based. Just over 40% of the frameworks are partial ontologies in that they used some primitive security models in their work. It is likely that the use of the primitive models was based on common security industry jargon rather than the intentional creation of an ontology as there is no mention of primitive models in the supporting research. Artifact-based frameworks make up 59% of analysed frameworks, which for the purposes of security compliance; require the users to demonstrate specific artifacts.

The Sherwood et al. (Sherwood et al. 1995) framework is a mixed framework type that demonstrates the challenge of creating an ontology- or artifact-based framework. It is one of the frameworks that show indicators of an ontology. This framework uses both artifact and ontological terminology in the description of the requirements for compliance to the framework. Examples of artifacts terms used are data dictionary, network, validation and testing. Examples of ontology terms used are access control, risk management and trust models. The challenge of developing an ontology framework will be the careful choice of security classifications rather than detailed security instances.

Zachman Based Enterprise Security Frameworks Discussion

The concept of using the Zachman Enterprise Architecture framework for the purposes of security is not a new one, however, it has not yet been fully explored. The following discussions describe the three frameworks, Sherwood (1995), Ertaul and Sudarsanam (2005) and Ho (2002) based on the Zachman. The conclusion from the three papers is that the Zachman framework is a well-defined structure to create an Enterprise Security Architecture framework, however, none of the proposed frameworks adheres wholly to its strict principles. An adherence to the principles would create a security ontology for enterprise architecture. Table 8 provides a side by side overview of the key points.

Enterprise Security Plan (Ertaul and Sudarsanam 2005)

This paper uses the second version of the Zachman framework as a starting point to create a "strategic framework for security planning" for government. The plan hopes to address the need for a logical way to view security within an organisation, to organise the complexities that address risk and thus to provide a more secure organisation given the increase in government security attacks.

The similarities to the Zachman include the headings for columns 1 through 5, rows 1 through 4 and row 6. The authors state that they use both the framework and the principles John Zachman identified for his framework.

The paper departs from the Zachman with the replacement of Column 6 (the Why interrogative) with a new column — External Requirements and Constraints. A second replacement is the Row 5 heading, which has gone from Implementers to Sub-Contractors. There is no explanation in the paper for any of these changes. The authors have acknowledged the need for each cell to be unique, however, there are many duplicates in the plan they have created. Finally, the Zachman framework is an ontology however, this framework is a mix of ontological phrases and security instances.

Security Management Framework (Ho 2002)

The security management framework developed by Ho uses the same framework as the Zachman. The author's choice of the Zachman was because "companies must take a total enterprise approach, integrating the security of a myriad of IT activities… into a holistic corporate security solution". The security framework uses the same row and column headings as Version 2 of the Zachman.

There are two departures from Zachman. The first is the Zachman principle of row combination — the combination of all the cells in any single row forms a complete view description for that perspective e.g. a Planner, Owner or Designer perspective. The discussion provided by Ho explains each column as a whole picture – based on the interrogatives, but the horizontal views are not taken into consideration. Secondly, there is a mix of classifications versus instances. Similar to the Ertaul & Sudarsanum framework, the product is actually a security instance of the Zachman framework, not a security ontology.

SABSA (Sherwood et al. 1995)

The Sherwood Applied Business Security Architecture (SABSA) is a commercial methodology for enterprise security architecture. The approach aims to provide all business security needs of customers and compliment any existing EA framework. The SABSA framework documentation states that it is underpinned by risk management, assurance, governance, a maturity profile and ongoing auditing. SABSA is essentially based on the Zachman framework. The layer names are the same, the column headings are also the same but have been re-ordered, however, the views have been re-ordered and renamed. The 6 x 6 matrix has been completed using business and security terminology.

The initial iteration of the SABSA framework was aimed at technical projects only and the company then decided to include corporate views to extend its usability for customers. The result is documentation that discusses security architecture holistically however, the framework artifacts themselves are technical e.g. there is no mention of non-technical security measures such as physical, human security or corporate security strategy. The methodology states it is providing an information security solution as compared to a broader security solution. The SABSA process would support an information technology project and its processes are described for projects not an organisation.

Another important change from the Zachman framework and from EA is the recommendations by SABSA for customers to select the pieces of their framework they feel are useful and disregard the rest. The Zachman framework is a complete enterprise ontology and is used as a whole, not as a piecemeal approach, so the SABSA approach contradicts this philosophy. A foundational tenet of EA is the collation of all organisational views for the purpose of getting a whole-of-organisation "as-is" capture — where the enterprise is now. The organisation then takes a complete view and makes decisions on where they would like "to-be" and an action plan is put into place to achieve this. By selecting only parts of the organisation, the purpose of EA is defeated.

Whilst these departures from the Zachman and EA do not impact the commercial purpose of the SABSA, they do not allow organisations that use the Zachman to directly use the SABSA for their security because the alignment is not there.

	Why Zachman?	Zachman Similarities and Differences	Framework Purpose	Ontological References
Enterprise Security Plan (Ertaul and Sudarsanam 2005)	To create a strategic framework for security planning for government.	<u>Similarities</u> Rows 1 - 4 and Row 6 Columns 1 – 5 <u>Differences</u> Row 5 has been changed from Technicians to subcontractors Column 6 has replaced Why with External Results and Constraints.	Organise complexities of organisational security and therefore secure the government more effectively.	Mix of ontological security phrases and security instances.
Security Management Framework (Ho 2002)	To create a holistic corporate security solution.	<u>Similarities</u> Columns are the same <u>Differences</u> Rows are different and do not use the Zachman principle of "row combination" – that is the combination of all the cells in a row providing a complete view description of the perspective.	Total enterprise approach to integrate security into IT activities.	Mix of ontological security phrases and security instances.
Sherwood Applied Business Security Architecture (Sherwood et al. 1995)	Compliment any existing EA framework.	<u>Similarities & Differences</u> Layer names are the same. Column headings are the same but reordered. Rows have been reordered and renamed Technical focus not holistic. Option to use pieces of the framework – no requirement to use all which is not Zachman principle of whole organisation.	Commercial methodology for enterprise security architecture to provide business security needs of customers.	Uses business and security terminology but the application information is technical instances.

Table 8: Comparison of existing Zachman based frameworks

2.5 Guiding Recommendations

The analysis of the 27 frameworks identified in our review provides an indication of important recommendations that help guide an organisation to a more secure corporate posture and concurrently support the achievement of corporate vision and strategy. Among the 27 frameworks, the only methodology utilised more than once is EA, which has been referenced in seven frameworks. It is the most common and effective methodology implemented to achieve a holistic security strategy.

The following discussion explains the five principles (summarised in Table 9) from the analysis work of the frameworks review, which have guided the development of the enterprise security architecture artifact.

Principle 1	The framework must provide security mechanisms for all organisational assets
Principle 2	The framework must be an ontology
Principle 3	The framework must be in compliance with at least one international security industry standard
Principle 4	The framework must use an enterprise architecture reference
Principle 5	The framework must cover the organisation holistically

Table 9: Principles of Enterprise Security Architecture

Framework Purpose (Principle 1)

The purpose of an effective framework should be to support the organisation's vision. To do this, all assets of a company should be employed e.g., people, technology, process and information. The recommendation derived from this criterion is therefore a holistic framework will include security mechanisms for all of the assets. Providing a separate security strategy for each department or asset; or choosing a select few assets to secure would not provide full security coverage and therefore lacks defence in depth. For example the Sun and Chen (2008) framework focused on securing technology only and the Shen et al. (2009) framework focused on security policy only.

Framework Type (Principle 2)

EA ontologies are classification systems that provide a structured way to articulate the required organisational assets for the purpose of alignment to the corporate vision, whilst allowing the company to choose the implementation based on its specific needs. In contrast, artifact-based framework types require a company to purchase or produce specific artifacts or methodologies to be in compliance. Artifact-based frameworks are restrictive and difficult to comply with particularly if the company is small and has budget constraints and do not take into account the nuances and individuality of each company. The principle from this criterion is to provide the organisation a framework type that is secure but also works with the individual organisational needs – an ontology.

Security Compliance / Assurance (Principle 3)

The concept of security is not new and there are very effective security standards available. Security standards are used as a benchmark by organisations to provide a level of assurance for their security programs (Siponen and Willison 2009). For compliance and assurance purposes, a framework should be in compliance with at least one security standard. From the framework reviews, two standards are used more than any others and either or both would provide an effective compliance tool. The two recommendations are ISO/IEC 27002 and NIST 800-53. The recommendation from this criterion is the use of an internationally recognized standard to provide security assurance.

Enterprise Architecture Reference (Principle 4)

EA is a proven structure for organisations to use to effectively complete their mission (Bittler and Kreizman 2005). From the analysis of the 27 frameworks, seven of the 27 reference EA in some form, with two frameworks specifically named – the Zachman and the FEAF. Moreover some of the most implemented EA structures have used the Zachman as a basis for the development of significant frameworks. These are the TOGAF (Josey 2009), the GEAF (Bittler and Kreizman 2005), the FEAF (U.S.Government 2013) and the DoDAF (DoD 2010). The recommendation from this criterion is therefore the use of an existing and well referenced EA for the basis of the development of a framework.

Framework Coverage (Principle 5)

The need for security initially began with the protection of information stored on computers however, this has broadened to include all departments within an organisation. The difficulty is that most departments have retained the individual control of the security measures they have put in place and this has meant that each security solution is managed separately (see Table 1). The overall effect is a lack of a cohesive strategy for organisational security (Eloff and Eloff 2005). To provide effective security for any entity, the whole entity needs to be considered. The same is true of an organisation. If we choose to only secure a department, the rest of the organisation remains insecure. The recommendation from the criterion is for a framework to regard the whole of the organisation, not just singular departments or assets. A structure that provides an integrated view of all security instances will give a credibility and confidence to business security responsibility (ISO 2013).

Principles Based Framework Development

This work addresses an important and critical issue through the development and objective review of an ESA that relies on thoroughly researched principles. The recommendations discussed form the guiding principles of an organisation-wide ESA ontology and provide a research foundation for a newly developed ESA framework, which this dissertation will detail. The analysis has shown that the majority of the 27 frameworks satisfy a subset of the principles. Specifically, security mechanisms for all organisational assets (Principle 1) is satisfied by six frameworks (Eloff and Eloff 2005; ISO 2013; Killmeyer 2006; Saleh and Alfantookh 2011; Scholtz 2006; Sherwood et al. 1995). The framework should be an ontology (Principle 2) was partially fulfilled by seven frameworks (Eloff and Eloff 2005; Ertaul and Sudarsanam 2005; Ho 2002; ISO 2013; Scholtz 2006; Sherwood et al. 1995; Wahe 2011) and although were not ontologies, did have some reference to ontological security terminology. Nine frameworks satisfied compliance to international security standards (Principle 3) (Anderson and Rachamadugu 2008; Eloff and Eloff 2005; Korhonen et al. 2009; NIST 2010; Saleh and Alfantookh 2011; Shen et al. 2009; Sun and Chen 2008; Trcek 2003; Wahe 2011). Use of an enterprise architecture reference (Principle 4) was indicated by seven frameworks (Anderson and Rachamadugu 2008; Ertaul and Sudarsanam 2005; Ho 2002; NIST 2010; Scholtz 2006; Shen et al. 2009; Sherwood et al. 1995). A holistic framework (Principle 5) was demonstrated by 11 frameworks (Anderson and Rachamadugu 2008; Eloff and Eloff 2005; Ho 2002; ISO 2013; Killmeyer 2006; Korhonen et al. 2009; Posthumus and Von Solms 2004; Scholtz 2006; Shen et al. 2009; Sherwood et al. 1995; Wahe 2011).

Figure 4 shows how the principles effect and interact with each other and the organisation. For example, the organisational vision directs and uses the assets of the organisation (people, information, technology and process) in all departments, whilst being secured and enabled through the ESA. This is done with the use of a security framework that is defined by enterprise architecture primitives. The primitives are defined first to ensure compliance with security standards and are then compared to the organisation to determine what the current situation of the organisation is and what can be improved to strengthen security.

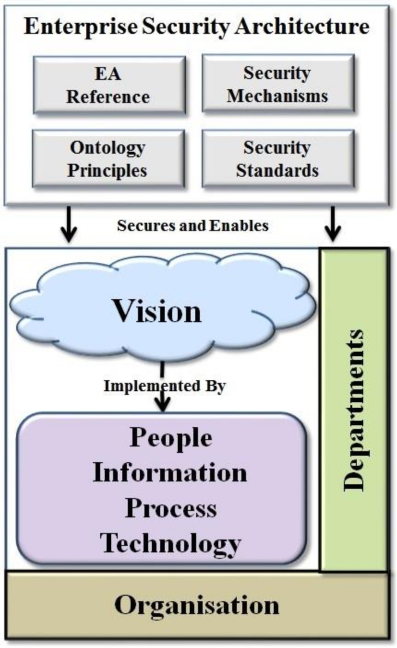


Figure 4: Enterprise Security Architecture Role in an Organisation

2.6 Summary

In summary, this chapter presents a background of the domains of enterprise architecture, security and enterprise security architecture. A semi-systematic review was conducted of security frameworks and it is evident that the grouping of security with EA, through a framework with corresponding security classifications and representations, promises a complete security solution. 27 security frameworks are evaluated and this work finds that grouping security with EA is not new, however, current solutions indicate a lack of research process in development and a disjoint focus in either technical, policy / department, or project. Thus, there is a need for a holistic solution. Through the review, several principles for the development of organisational security models are extracted and the most referenced five principles are identified. The five principles provide a foundation to develop the ESA framework and evaluate the design, which is addressing the problem statement "will a holistic security model using EA provide security benefits to an organisation more effectively than a piecemeal approach".

3 Method

"No research is ever quite complete. It is the glory of a good bit of work that it opens the way for something still better, and this repeatedly leads to its own eclipse."

Mervin Gordon

This research addresses the problem statement "will a holistic security model using Enterprise Architecture (EA) provide security benefits to an organisation more effectively than a piecemeal approach". It does this by evaluating a design founded on the five design principles developed through the semi-systematic literature review described in the previous chapter. The foundation of this research is based on philosophies and methods chosen for their best application to the research and cohesively to each other. This chapter describes these methods, including the rationale for their selection. The careful selection is important because it provides rigour around the structure of the research.

The philosophy for this work is constructivist, the approach is inductive and the choice of data analysis is qualitative, using the grounded theory methodology to analyse an Oppenheim (Oppenheim 2000) qualitative questionnaire. The overarching design methodology is Design Science Research (DSR) (Hevner et al. 2004).

3.1 Philosophy

The philosophy of the development of research is based on a system of beliefs and assumptions that are used in all research stages. The shaping belief system can be drawn from the research field, e.g., information systems, surrounding realities or the human aspects of the researcher themselves and how they interpret the world and the findings (Burrell and Morgan 1979; Crotty 1998). This research is based in the underlying assumptions of constructivism, which are often used in concert with DSR and with qualitative research. This provides a basis for how knowledge is perceived and how it can be obtained (Hirschheim 1985) throughout the DSR activity. Constructivism describes truths not as discovered, but as reliant on human awareness and the struggle of the conflict between personal models and discrepant new insights that create new representations of reality. The new models, using cultural tools and symbols, bring meaning and find authentication through discussion in communities of practice (Fosnot 2013). DSR and our research is representative of this world-view due to the nature of the conception of a problem statement idea (the current world-view model is challenged), development of a design to address the challenge (incorporating the conflict between what we knew and what we now know), the artifact to test the design and the cyclical analysis of the artifact until the design is satisfied (new knowledge and models are created) (Mills et al. 2006; Strauss and Corbin 1998).

Other Philosophies

Through the process of determining the most suitable philosophy for this research, others were considered, including positivism, idealism and interpretivism. Positivism recognises only things that can be scientifically verified, usually using logical or mathematical proofs – quantitative constructs, and is sometimes referred to as the scientific method (Pather and Remenyi 2005). Due to the qualitative nature of this research, and the philosophy's rejection of metaphysics and theism, positivism was not chosen. Idealism believes that thoughts and ideas make up reality and that it is not possible to be sure that anything in the outside world exists (Carlsson 2010). This philosophy did not align to the research requirements. Finally, interpretivism, which along with constructivism is used with DSR, believes knowledge grows from the idea that the natural world and the social world are ontologically different. In contrast, constructivists believe that knowledge develops through the researcher's dealings with the environment (Rahi 2017; Venable 2006; Walsham 1995). Due to the need for cyclical interactions with users and their environments, constructivism was chosen.

3.2 Approach

Inductive reasoning is a logical thought progression in which various propositions, all believed true or found true the majority of the time, are combined to create a definitive assumption or likely conclusion (Lee and Baskerville 2003). Inductive reasoning was chosen for this research because of the nature of DSR. The research itself began with specific observations – the design principles for the security artifact –and used those principles to develop a recommended way forward for the development of a likely artifact that could provide an assumptive solution.

The other options that were considered for the reasoning approach of this research were deductive and abductive. Deductive reasoning begins with generalities to a problem and uses those to develop a specific solution or answer which is the inverse of the reasoning used for the research, so it was not chosen. Abductive reasoning was also not chosen because it did not align to the research, as this type of causal explanation begins with an incomplete set of observations and suggests the likeliest explanation for that set – often referred to as "the simplest and most likely explanation is usually the right one" (Folger and Stein 2017).

3.3 Qualitative Research Method

This research uses *grounded theory* as the chosen qualitative research method. Four other options were considered: *action research*, *phenomenology*, *discourse analysis* and *ethnography*. This section now describes the five methods, including the rationale for the choice, how they were analysed to identify the best suited for this research and for the qualitative data set that would be developed from the questionnaire evaluation of the security artifact.

Action Research

Action research is about doing research while *in* action and is not research about an action. It is performed using four phases – planning, action, evaluation and further planning (Coghlan 2019). This is similar to the plan, do, check, act Deming cycle (Moen and Norman 2006). In action research, those that are in the study are members of the research team, not participants as is more traditional, and the research is done at the same time as the action is taking place, not after (Susman and Evered 1978). Due to the length of time to develop the security artifact and because action was not at the core of the research, this method was not used.

Phenomenology

Phenomenology describes the meaning of an experience lived by understanding the deeper assumptions that the subject already knows. This method is not about the creation of new information, but illuminates already understood information to describe the meaning in every day phenomenon (Merleau-Ponty 1996; Starks and Brown Trinidad 2007). The intent of this research was not to observe other humans during a particular phenomenon, so this research method was considered not suitable.

Discourse Analysis

As the name indicates, discourse analysis is concerned with analysing language-in-use and how people complete tasks through language. This can include following the historical evolution of a language and understanding how that impacts the use of the language in everyday situations. (Fairclough and Wodak 1997; Johnstone 2017; Starks and Brown Trinidad 2007). This research was not primarily about language and as such this method was not used.

Ethnography

Ethnography is one of the most recognised qualitative research methods and involves the researcher spending extensive amounts of time in the field with the participants that they study. It is an immersion of a social and cultural situation. Traditionally ethnography was used in anthropology but is now also being used effectively in organisations and information systems. (Brewer 2000; Hammersley 2007). Due to the dispersion of the security artifact questionnaire participants, it was not possible to use ethnography in this research.

Grounded Theory

Grounded theory is a methodology by which qualitative analysis is iterative – the data (meaningful concepts from the texts) are collected and separated from the conversation and each data unit is assigned codes (Urquhart et al. 2010). The codes are inspected for patterns and then reintegrated to form dominant thematic subjects and connections. (Starks and Brown Trinidad 2007; Strauss and Corbin 1994). The code inspection, or coding, is done iteratively to a level of detail that provides a thematic essence of the original data set or texts. According to Martin & Turner (1986) grounded theory is "an inductive, theory of discovery methodology that allows the researcher to develop a theoretical account of the general features of a topic while simultaneously grounding the account in empirical observations or data". This method was chosen to analyse the results from our Oppenheim questionnaire about our security artifact because it provided a detailed methodology which, through each coding phase, produced a synthesis of the themes that became richer and more meaningful about the artifact's utility.

3.4 Design Science Research

A Design Science Research (DSR) study (Hevner et al. 2004; Nunamaker Jr et al. 1990) suited the research due to the emphasis on the design and creation of an artifact to test a research question (Venable et al. 2016) and the research rigor the DSR methodology provided (Peffers et al. 2006; Sein et al. 2011). The choice of DSR for this information systems research was made because the DSR research paradigm addresses the real-world applicability versus research rigour gap in information systems, by bringing both practical relevance – artifacts, and scientific rigor - design theories, to the activity (Baskerville et al. 2018; Benbasat and Zmud 2003; Galliers et al. 2006). If the research was to be successful, it needed to have a demonstrated use in business but also the research thoroughness that was lacking in the existing artifacts identified during the literature review.

Vaishnavi & Kuechler (2004) describe the body of DSR knowledge, which this dissertation contributes to, as man-made objects – artifacts – that are designed to meet specific goals. DSR creates novel contributions through the design of new artifacts including the analysis of their operation using evaluation and abstraction. It uses design as a research method that maps functional requirements on to a fulfilling artifact. The design action is justified using a *kernel* theory – an established theory that, when the new design action is complete, may improve or broaden the purpose of the initial kernel theory. As indicated in Figure 5 there are five steps: 1) Awareness of the Problem, 2) Suggestion, 3) Development, 4) Evaluation, and 5) Conclusion. These are now described.

Step 1: Awareness of the Problem

An individual becomes aware of a problem that does not appear to have an existing solution and therefore a research proposal is written. For this research, the problem was identified whilst the researcher was working in security and wanted to use a holistic security model for the organisational security approach. Despite the extensive resources of a large Australian Federal Government Agency, and strong ties to international partners, academia and industry; there did not appear to be a demonstrated holistic solution. The problem was then confirmed through a semi-systematic literature review of holistic security models, which identified that there is a lack of fully researched security models looking at security from a complete organisational perspective and not just a category of problem, e.g., computer security or human resource security. The literature review also confirmed that others had searched for a similarly complete solution for all organisational security however, it was not available (Angelo 2001; Copeland 2017; Tamm et al. 2011).

Step 2: Suggestion

Suggestion is the second step where indications of the first sample of the design idea including performance needs of a prototype, are developed. Through the literature review, recommended principles for a security model were identified and developed to provide both the design and the performance needs of the model. The principles included purpose, type, assurance, kernel theory reference, and coverage.

Step 3: Development

In Step 3, the design from Step 2 is used to create the artifact. However, it is important to note that the emphasis is on the *novelty* of the design, not the creation of the artifact. The focus of DSR is the testing of a new design to solve a problem, the developed artifact supports this testing of the design, rather than being the focus itself. Using the principles to guide the design, a security architecture framework artifact was created – a thirty-six cell security instantiation or ontology.

Step 4: Evaluation

To evaluate the initial proposal and design, performance measures are placed on the artifact at Step 4 and any changes are fed into the design to inform the next design iteration. Using the design principles and security domain guidelines, the security framework was given to managers, security professionals, IT professionals and researchers. The participants were also given a questionnaire about the utility of the framework, to evaluate and provide the cyclical feedback to inform the artifact design process.

Step 5: Conclusion

This cyclical evaluation continues until a conclusion is reached – usually the end of the research cycle or when the solution is considered "good enough" and the results are written up. The evaluation process of the security artifact was concluded with the results being published (McClintock et al. 2020). An extended version will also be included in a 2020 book in the "Lecture Notes in Business Information Processing" (LNBIP) series, published by Springer.

The research is overlaid onto the Outputs column in Figure 5 (coloured red) to demonstrate the use of the DSR methodology.

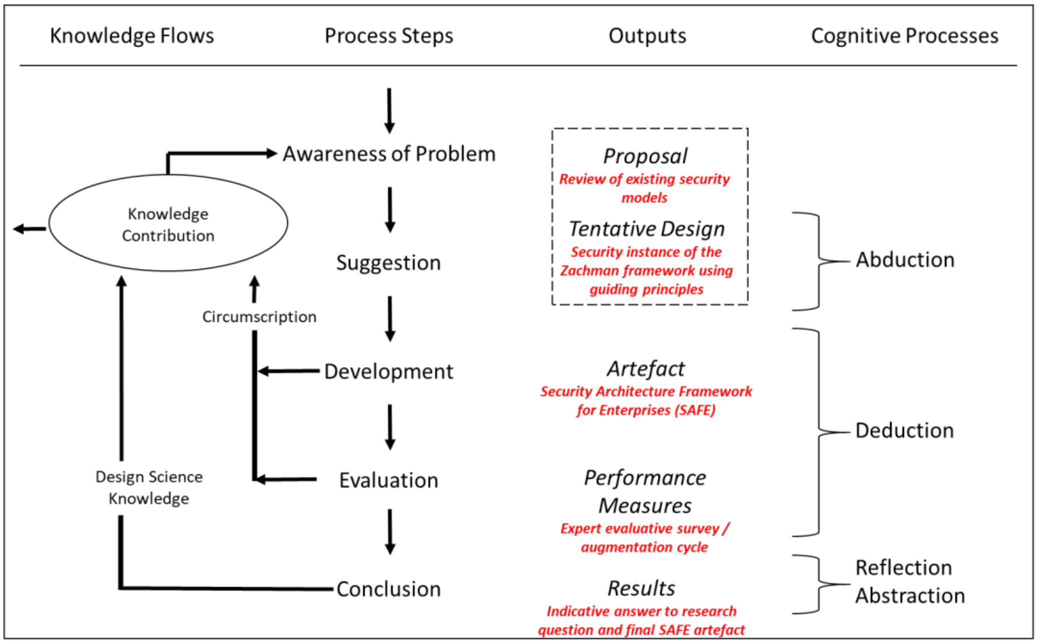


Figure 5. SAFE Outputs in Design Science Research Cycle (Vaishnavi and Kuechler 2004)

The opportunity for the research was also demonstrated using the DSR Knowledge Contribution Framework (Gregor and Hevner 2013) at Figure 6. This framework uses two axes to describe a problem in the DSR context. The first is application domain maturity, which describes the context of the problem – for this research, the domains were enterprise architecture and security. Both are established domains or in this context have a high level of application domain maturity. The second is solution maturity, which indicates the maturity of current existing artifacts to solve the research problem being explored. For this research, the solution maturity is low. This placed the problem set in the Improvement quadrant and provided the prospect of knowledge contribution and a research opportunity.

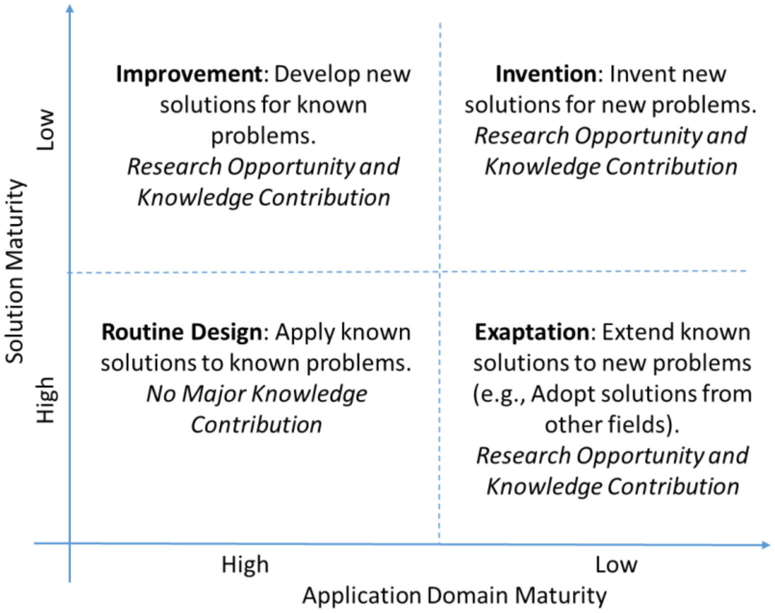

Improvement: Develop new solutions for known problems.
Research Opportunity and Knowledge Contribution
Invention: Invent new solutions for new problems.
Research Opportunity and Knowledge Contribution
Routine Design: Apply known solutions to known problems.
No Major Knowledge Contribution
Exaptation: Extend known solutions to new problems (e.g., Adopt solutions from other fields).
Research Opportunity and Knowledge Contribution
Solution Maturity
Low
High
Application Domain Maturity
High
Low

Figure 6. DSR knowledge contribution framework (Gregor and Hevner 2013)

In summary, this chapter has described the methods and philosophies that were chosen to best frame the research and address the problem statement "will a holistic security model using Enterprise Architecture (EA) provide security benefits to an organisation more effectively than a piecemeal approach". The choices ensured that the outcome of the research - the artifact and design, are both organisationally practical and academically sound. The next chapter will discuss in detail, the artifact, how it was developed, and the three layers of abstraction achieved, using the methods and philosophies selected.

4 Artifact Description

"The desire to create is one of the deepest yearnings of the human soul"

Dieter F Uchtdorf

As described in the previous section, this is a DSR study. Therefore, the development of the artifact to test a theory which was based on principles was critical. The question being tested is "will a holistic security model using EA provide security benefits in an organisation more effectively than a piecemeal approach". Through the literature review, five design principles were identified to inform the design, development and evaluation of the artifact to test this question. Those principles will be used to frame the following discussion, describing the artifact, how it was developed and the three layers of abstraction achieved.

The contributions to practice and knowledge for this research are three-fold. Firstly, the extension of the Enterprise Architecture Domain – the development of a standardised, comprehensive enterprise security architecture. As described above, this is not currently available to a detailed level of complexity. Secondly, the Security Domain – the development of the first fully researched security ontology and ESA based on security industry standards and security regulatory compliance and practices. This research is compliant with both NIST 800-53 (NIST 2013) and

ISO/IEC 27002 (ISO 2013) and will provide an assurance that all aspects or the organisation have been considered for security. Finally, the design of a security dimension to the original EA framework - Zachman. Previous research which has created security constructs for the Zachman, have restricted their scope to a specific organisational focus, such as technical, instead of considering the organisation as a whole (Kreizman and Robertson 2006). Adherence of an ESA to the EA principles from the Zachman extends the utility of the Zachman and provides a security dimension which has otherwise been lacking (Copeland 2017).

The discussion will begin with the Enterprise Architecture Reference principle because this design feature informed the other principles by providing the structure of the artifact.

4.1 Enterprise Architecture Reference Design Principle

For the purposes of this design principle, the EA reference chosen to base the security artifact model on, was the Zachman framework 2013 Version 3.0 because it is the most complete, most referenced in our frameworks review and historically the methodology that is chosen by others to base their frameworks on. The majority of EA frameworks, however, do not have a security component (Posthumus and Von Solms 2004). Despite Zachman's success, it does not include security in any form (Zachman 2001). This lack of security has been identified by others (Copeland 2017) who have used Zachman to create an enterprise security architecture (ESA)(Sherwood et al. 1995). However, the results have been limited and none of the ESA's to date have utilised the Zachman EA concept of an ontology or ensured a strict adherence to the original definitions of Zachman (Zachman 1987). Zachman is the ontological language of EA and building on this concept, a security implementation of Zachman would be the first security ontology available – a defined organisational security language. Furthermore, most existing ESAs are from business white papers, and thus lack in-depth case study analysis, experimental replicability and research exploration (Tamm et al. 2011). The challenge to do so, however, is the complexity. A framework that addresses all organisational security requires extensive research in every aspect of security, not just a singular framework focused on a specific aspect of security. There are some examples in literature (Ertaul and Sudarsanam 2005; Ho 2002; Sherwood et al. 1995), however, they have a smaller scope and their purpose is not to cover the entire spectrum of an organisation. For example EA security governance frameworks tend to be very top heavy – ensuring the highest levels of the organisation are fulfilling their legal responsibilities – but do not include implementation or technology (Anderson and Choobineh 2008). Also, unlike the increasing academic interest in EA, most of the writings about enterprise security architecture are from business white papers and not from academia (Tamm et al. 2011), thus lacking research rigour. The comprehensive use of EA in security will also provide a single capture of all the organisation's security – a holistic security structure that is not yet available in a mature form.

All 36 cells of the Zachman framework were explored and researched to determine exactly what the purpose of the cell was. This included identifying full definitions for each cell and the outer framework terms, and attending a Zachman enterprise architect Level 1 and 2 course with John Zachman to clarify any existing questions not answered by the literature review of EA. Once EA and security were explored adequately and an expert level of knowledge was achieved, the outer edges of the proposed security version of the Zachman framework were identified. To ensure the integrity of the principles of EA, it was important to retain the organisational views (the rows) and the interrogatives (the columns).

The following discussion provides a detailed explanation of the rows and columns in the Zachman and how they were used to define the security artifact.

Audience Perspectives / Stages of Reification (the rows)

The perspectives or rows in the Zachman constitute a complete way to view an organisation, from the people who would initially identify the concept for the business (the first row), to the final instantiation of the running organisation (the final row), as described in Section 2.1 and Table 3. It was important that the security framework retain the intent of the rows – the whole organisational view – to provide a complete description of an organisation's security mechanisms in all parts of the organisation. As a security architect worked their way through the framework, the security instance would align to the organisational instance. The security artifact retained the row perspectives with no changes – they are Identification, Definition, Representation, Specification, Configuration, and Instantiation. As each stage or row of the reification process, moving down the framework, is a transformation not a more detailed view of the previous perspective, in the original architectural intent, so should the security cells. As a reminder, the rows were defined as:

- Row 1 - Executive Perspective / Identification: The executive perspective is defined at the inception of a company. It is the identification of the concept for the business and is externally focused.
- Row 2 - Business Management Perspective / Definition: The business management perspective is internally focused and defines the executive, external concept for the enterprise, into a business model of enterprise design and operational reality.
- Row 3 - Architect Perspective / Representation: The architect perspective represents the business model as the required pieces or building blocks of the enterprise and indicates how they will interact with each other.
- Row 4 - Engineer Perspective / Specification: The requirements and specifications of the systems of the organisation are designed at the engineering perspective.
- Row 5 - Technician Perspective / Configuration: The technician perspective is the business component level and are implemented using specific tooling configurations.

- Row 6 - Enterprise Perspective / Instantiation: The enterprise perspective is the instantiation of the reification process from Row 1 to 5, outworked and demonstrated in the functioning organisation.

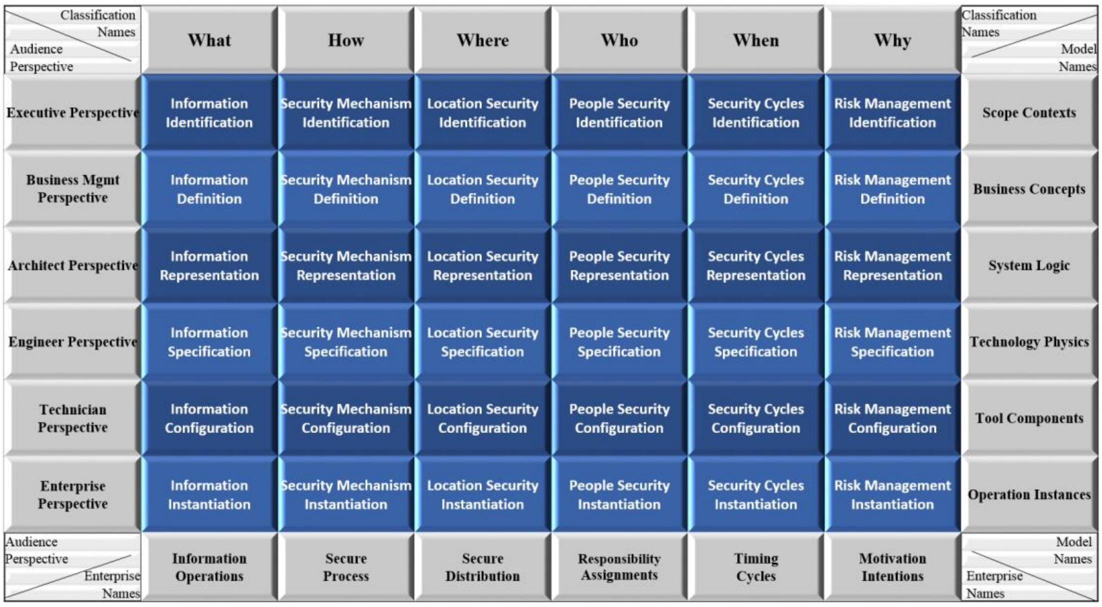
Classification Names (the columns)

The columns of the framework are the English interrogatives and provide the detail of each row or organisational view. A more detailed explanation of the columns can be found in Section 2.1 and Table 2. While the interrogatives were retained, where the differentiation came, was the answers to the interrogative questions. For example, the Zachman "what" column asks the question "what is the most important asset for the organisation" and the Zachman answer is "inventory sets". Whereas the security question for the "what" column is "what is the organisation's most important asset that needs to be secured" and the answer is "information". All columns of the security artifact were addressed in the same way – each having a security question asked of the interrogative rather than the Zachman question, by doing so, the integrity of the Zachman was retained but the security instance was created. Table 10 shows the original Zachman framework interrogative definitions alongside the security artifact definition.

Interrogative	Zachman Definition	Security Artifact Definition
What - Things	The inventory sets, people or information, that are tracked and managed for the organisation to function.	The organisation's most important asset is information and this is what is being secured. Labelled "**Information**" in the artifact.
How - Process	The processing of the organisation through various process types which provide the transformation models of the assets.	How the organisation secures the information. At the conceptual level, the security mechanisms are processes through to the final level of instantiations which are security technologies. Labelled "**Security Mechanism**" in the artifact.
Where - Location	Distribution networks depicted using network models. Includes business, system, technology or tool locations.	Where the organisation's security is conducted. Can be a physical or logical location. Labelled "**Location Security**" in the artifact.
Who - People	The responsibility assignments are allocated to the organisational stakeholders and can be internal or external.	The people of the organisation, which can be defined as both internal and external stakeholders, require various forms of security. Labelled "**People Security**" in the artifact.
When - Events	Timing cycles, the intervals and moments of the organisation and how those are identified as types, defined, represented, specified and configured within the architecture and the organisation.	When the organisation has determined will be the most effective security timing cycles to provide a secure organisation. Examples include compliance, policy, assessment, audit and reviews. Labelled "**Security Cycles**" in the artifact.
Why - Ends	The objectives and strategies explain why the organisation is in business, how those motivations and intentions are outworked through ends and means.	The essential motivation why security is the risk of an event occurring which would damage an organisational asset. The management of that risk is outworked as security - a determination of the strengths, weaknesses, opportunities and threats; and the appropriate mitigation strategies deployed. Labelled "**Risk Management**" in the artifact

Table 10. Column Definitions – Zachman vs Security Artifact

With the row and column definitions completed, each of the 36 cells of the artifact were defined using these definitions. For example, Cell 1 – the Row 1 audience perspective or reification stage is defined as "Identification" and the Column 1 answer to the interrogative What, is "Information", therefore the cell's primitive security model is "Information Identification". As described in Chapter 2, a primitive model is the classification name of a required element in an EA framework – in this case these are the required elements of the security framework, the primitive security models. This design process continued until all cells were completed and the outcome can be found in Figure 7.

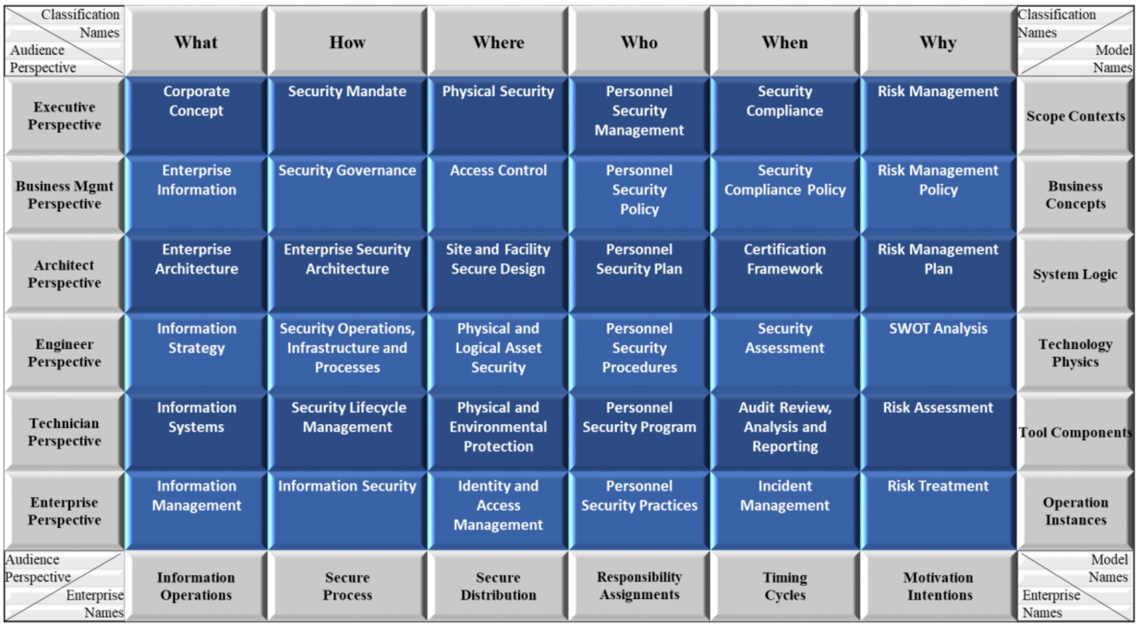


Classification Names Audience Perspective	What	How	Where	Who	When	Why	Classification Names Model Names
Executive Perspective	Information Identification	Security Mechanism Identification	Location Security Identification	People Security Identification	Security Cycles Identification	Risk Management Identification	Scope Contexts
Business Mgmt Perspective	Information Definition	Security Mechanism Definition	Location Security Definition	People Security Definition	Security Cycles Definition	Risk Management Definition	Business Concepts
Architect Perspective	Information Representation	Security Mechanism Representation	Location Security Representation	People Security Representation	Security Cycles Representation	Risk Management Representation	System Logic
Engineer Perspective	Information Specification	Security Mechanism Specification	Location Security Specification	People Security Specification	Security Cycles Specification	Risk Management Specification	Technology Physics
Technician Perspective	Information Configuration	Security Mechanism Configuration	Location Security Configuration	People Security Configuration	Security Cycles Configuration	Risk Management Configuration	Tool Components
Enterprise Perspective	Information Instantiation	Security Mechanism Instantiation	Location Security Instantiation	People Security Instantiation	Security Cycles Instantiation	Risk Management Instantiation	Operation Instances
Audience Perspective Enterprise Names	Information Operations	Secure Process	Secure Distribution	Responsibility Assignments	Timing Cycles	Motivation Intentions	Model Names Enterprise Names

Figure 7: Primitive security models of the artifact (in blue)

4.2 Framework Type Design Principle

This design principle required that each cell be defined using ontological instances rather than artifact-based instances so that organisations would be free to choose their own implementation of the cell rather than be required to find a specific artifact. The purpose is for organisations to be able to consider security in all their facets of business, regardless of the organisations' size, financial position or industry, which a categorisation or ontological framework provides. Using the detailed research process that was conducted to understand the original Zachman cell intent, and then a thorough research process, including the initial semi-systematic literature review, to understand how organisational security related to each cell, authentic ontological security instances were developed for all 36 cells. For example, the "Risk Management Definition" cell – the research conducted was to understand "What is the instrument that an organisation would use to define risk management?" The answer from research for this cell is Risk Management Policy and that answer, therefore, became the instantiation. The outcome of this design process – the security instantiations of each cell – can be found in Figure 8. A detailed explanation of every cell, the questions that were asked, the research conducted, the definitions and purpose of each cell, the pictorial model, the compliance mapping and real-world example artifacts, can be found in Section 4.5.



Classification Names Audience Perspective	What	How	Where	Who	When	Why	Classification Names Model Names
Executive Perspective	Corporate Concept	Security Mandate	Physical Security	Personnel Security Management	Security Compliance	Risk Management	Scope Contexts
Business Mgmt Perspective	Enterprise Information	Security Governance	Access Control	Personnel Security Policy	Security Compliance Policy	Risk Management Policy	Business Concepts
Architect Perspective	Enterprise Architecture	Enterprise Security Architecture	Site and Facility Secure Design	Personnel Security Plan	Certification Framework	Risk Management Plan	System Logic
Engineer Perspective	Information Strategy	Security Operations, Infrastructure and Processes	Physical and Logical Asset Security	Personnel Security Procedures	Security Assessment	SWOT Analysis	Technology Physics
Technician Perspective	Information Systems	Security Lifecycle Management	Physical and Environmental Protection	Personnel Security Program	Audit Review, Analysis and Reporting	Risk Assessment	Tool Components
Enterprise Perspective	Information Management	Information Security	Identity and Access Management	Personnel Security Practices	Incident Management	Risk Treatment	Operation Instances
Audience Perspective Enterprise Names	Information Operations	Secure Process	Secure Distribution	Responsibility Assignments	Timing Cycles	Motivation Intentions	Model Names Enterprise Names

Figure 8: Security instantiation of the primitive security models (in blue)

4.3 Security Compliance / Assurance Design Principle

This principle required that a security framework be compliant to an internationally recognised security standard. The two most referenced in the literature review were ISO/IEC 27002 (ISO 2013) and NIST 800-53 (NIST 2013) therefore both were used for security assurance of the artifact. Table 11 is the compliance summary for 31 cells of the artifact. The five that are not included are the first five in the column "What", which were omitted because the entire column is about the information of the organisation. The security compliance standards do not differentiate from the type of information therefore the final cell in the column, which is the enterprise instantiation of information, represents the entire column.

SAFE PRIMITIVE MODELS	ISO/IEC 27002 CONTROLS (ISO 2013)	NIST SP 800-53 CONTROLS (NIST 2013)
Information Instantiation	Operations Security;	Configuration Management; System and Information Integrity;
Security Mechanism Identification	Information Security Policies;	Planning; Program Management;
Security Mechanism Definition	Information Security Policies; Organisation of Information Security; Compliance;	Certification and Accreditation and Security Assessments; Program Management;
Security Mechanism Representation	Information Security Policies; Organisation of Information Security;	Planning; Program Management;
Security Mechanism Specification	Asset Management; Operations Security; Communications Security; System Acquisition, Development and Maintenance;	System and Services Acquisition; Media Protection; System and Communications Protection;
Security Mechanism Configuration	Information Security Policies; Organisation of Information Security;	Planning; Certification and Accreditation and Security Assessments; Maintenance; Program Management;
Security Mechanism Instantiation	Organisation of Information Security; Access Control; Cryptography; Operations Security; Communications Security;	Program Management;
Location Security Identification	Access Control; Physical / Environmental Security; Information Security Aspects of Business Continuity;	System and Services Acquisition; Physical and Environmental Protection; Maintenance; Media Protection; Access Control; System and Communications Protection;
Location Security Definition	Access Control; Physical / Environmental Security;	Physical and Environmental Protection; System and Information Integrity; Identification and Authentication; Access Control; Audit and Accountability; System and Communications Protection;
Location Security Representation	Access Control; Physical / Environmental Security; Operations Security;	Risk Assessment; Planning; Physical and Environmental Protection; Access Control;
Location Security Specification	Asset Management; Access Control; Physical / Environmental Security; System Acquisition, Development and Maintenance;	Physical and Environmental Protection; Media Protection; Access Control; System and Communications Protection;
Location Security Configuration	Physical / Environmental Security; Information Security Aspects of Business Continuity;	Risk Assessment; Planning; Physical and Environmental Protection; Contingency Planning; Incident Response;
Location Security Instantiation	Human Resource Security; Access Control; Physical / Environmental Security; Supplier Relationships;	System and Information Integrity; Identification and Authentication; Access Control; Audit and Accountability; System and Communications Protection;
People Security Identification	Human Resource Security; Supplier Relationships;	Personnel Security; Awareness and Training;
People Security Definition	Information Security Policies; Human Resource Security; Supplier Relationships;	Personnel Security; Awareness and Training;
People Security Representation	Human Resource Security; Access Control; Supplier Relationships;	Personnel Security; Awareness and Training; Identification and Authentication; Access Control;

People Security Specification	Human Resource Security; Supplier Relationships;	Personnel Security; Awareness and Training;
People Security Configuration	Human Resource Security; Supplier Relationships;	Personnel Security; Awareness and Training;
People Security Instantiation	Human Resource Security; Access Control; Supplier Relationships;	Personnel Security; Awareness and Training;
Security Cycles Identification	Organisation of Information Security; Compliance;	Certification and Accreditation and Security Assessments; Audit and Accountability;
Security Cycles Definition	Information Security Policies; Compliance;	Certification and Accreditation and Security Assessments;
Security Cycles Representation	Organisation of Information Security; Compliance;	Planning; Certification and Accreditation and Security Assessments; Audit and Accountability;
Security Cycles Specification	Compliance;	Risk Assessment; Certification and Accreditation and Security Assessments; System and Information Integrity; Audit and Accountability;
Security Cycles Configuration	Operations Security; Information Security Incident Management; Information Security Aspects of Business Continuity; Compliance;	Planning; Certification and Accreditation and Security Assessments; Maintenance; System and Information Integrity; Audit and Accountability;
Security Cycles Instantiation	Operations Security; Information Security Incident Management; Information Security Aspects of Business Continuity; Compliance;	Risk Assessment; Certification and Accreditation and Security Assessments; Contingency Planning; System and Information Integrity; Incident Response; Awareness and Training; Audit and Accountability; Systems and Communications Protection;
Risk Management Identification	Information Security Policies; Organisation of Information Security; Supplier Relationships; Information Security Incident Management;	Risk Assessment;
Risk Management Definition	Information Security Policies; Organisation of Information Security; Supplier Relationships; Information Security Incident Management;	Risk Assessment;
Risk Management Representation	Information Security Policies; Organisation of Information Security; Supplier Relationships; Information Security Incident Management;	Risk Assessment; Planning; Contingency Planning;
Risk Management Specification	Information Security Policies; Organisation of Information Security; Supplier Relationships; Information Security Incident Management;	Risk Assessment; Contingency Planning; Incident Response;
Risk Management Configuration	Information Security Policies; Organisation of Information Security; Supplier Relationships; Information Security Incident Management;	Risk Assessment; System and Information Integrity; Audit and Accountability;
Risk Management Instantiation	Information Security Policies; Organisation of Information Security; Supplier Relationships; Information Security Incident Management;	Risk Assessment; Personnel Security; Contingency Planning; Incident Response; Awareness and Training;

Table 11: Artifact security compliance mapping to NIST 800-53 and ISO/IEC 27002

4.4 Framework Coverage and Framework Purpose Design Principles

Remaining consistent to the design principle of EA and the rules of the Zachman, the two principles of framework coverage and framework purpose have also been complied with. Framework coverage emphasises the need for the entire organisation to be considered when implementing security, and not just singular departments – a holistic framework. Framework purpose speaks to the organisation's assets – people, process, technology and information all should be considered when securing an organisation. EA is both a holistic instrument and covers all of an organisation's assets therefore the use of it in the design of the artifact, achieved both design principles.

4.5 The 36 Cells of the Artifact

Once the high-level categories were defined for each cell, the detail needed to be developed to explain what each cell actually meant. Also, whilst the high-level definition provided the matching Zachman column / row reference for each security cell, the specific security ontological construct needed to be defined for user guidance when evaluating the framework. This resulted in four factors being defined. Those were:

1. Detailed explanation – what is the definition and purpose of the cell
2. Pictorial model – a pictorial description for ease of understanding to users
3. Artifact example – show the use of the cell using a real-world example
4. Compliance mapping to ISO/IEC 27002 and NIST 800-53

Below are the artifact ontological security cell definitions – four factors, for the 36 cells.

Cell Definitions

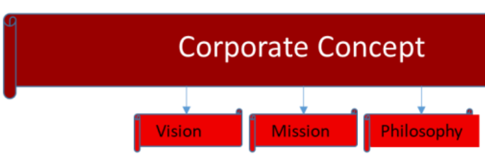
Cell 1 – Information Identification (Corporate Concept)

The concept of the corporation is the description the organisation provides to external parties when explaining what the company does and what it is that differentiates itself from other corporations. Often considered the initial seed idea that begins the company and is eventually matured into a detailed description which will give a clear indication of what information the company will consider proprietary. Ultimately it will become the vision, mission and philosophy the company is founded on. Security should be used in service to the corporate concept (Anderson 2008) – the essence of what the organisation is trying to achieve; therefore the security framework needs the corporate concept as the kernel for all other cells to draw from and be influenced by.

Corporate Concept

Cell A1
Information Identification

Pictorial Model:

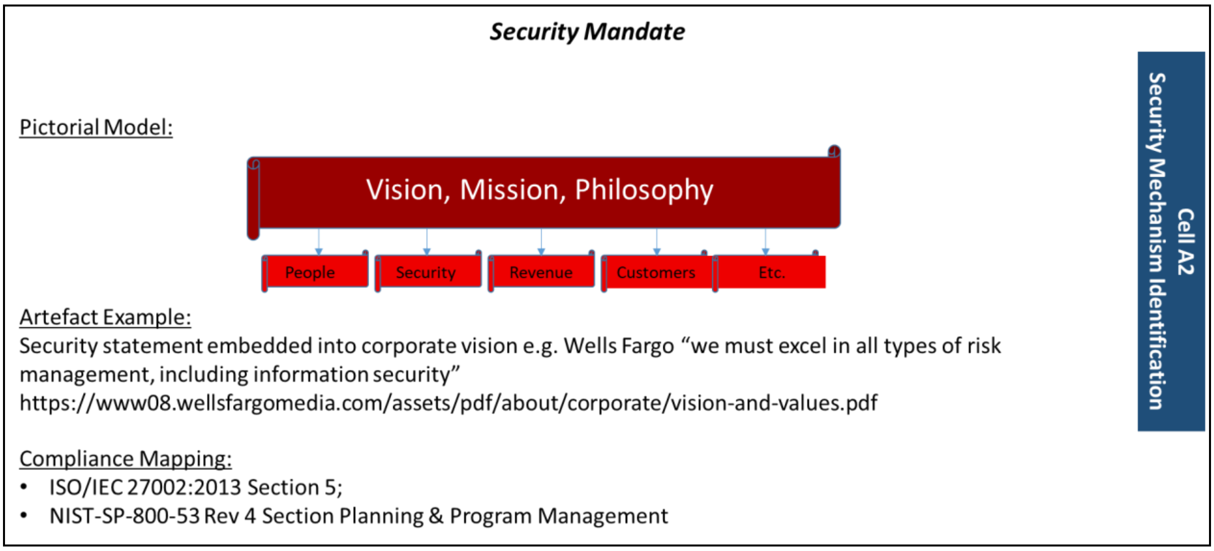


Artefact Example:
The Westpac Banking Corporation describes their corporate concept in this vision document which includes strategy, key organisational elements, the importance of staffing, markets, and what differentiates them as an organisation.
https://www.westpac.com.au/about-westpac/westpac-group/company-overview/our-strategy-vision/

Compliance Mapping:
The Information Definition column (What) does not require security compliance – the purpose is to define the information, its architecture, systems, management and assets that need securing. The rest of the framework provides the security.

Cell 2 – Security Mechanism Identification (Security Mandate)

One of the critical success factors of organisational security is the identification of the need for security within an organisation at the executive level. If senior management are seen to be endorsing and championing security, it is more likely to become a cultural norm. To demonstrate the significance to the organisation, security is included in the corporate vision, mission and philosophy (Anderson 2008; ISO 2013). At this executive level, there are no detailed security plans however, an acknowledgement of security and the risk it mitigates in the most senior organisational document, can become the key driver for organisational security practices, process and programs (Plachkinova and Maurer 2019).



Security Mandate

Pictorial Model:

Artefact Example:
Security statement embedded into corporate vision e.g. Wells Fargo "we must excel in all types of risk management, including information security"
https://www08.wellsfargomedia.com/assets/pdf/about/corporate/vision-and-values.pdf

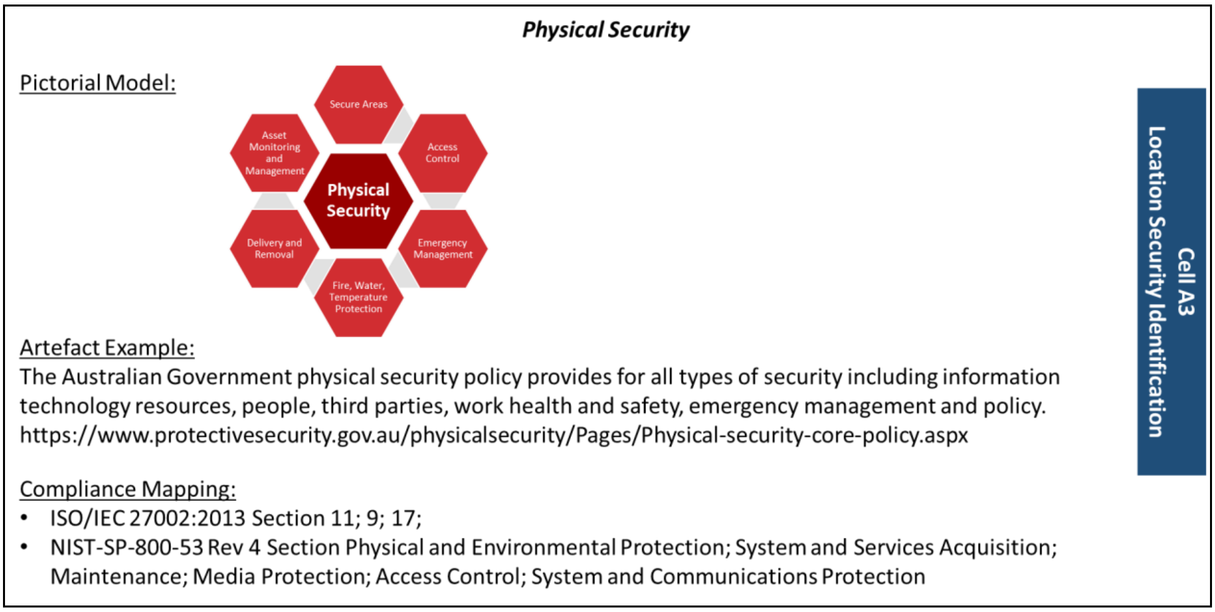
Compliance Mapping:

- ISO/IEC 27002:2013 Section 5;
- NIST-SP-800-53 Rev 4 Section Planning & Program Management

Cell A2
Security Mechanism Identification

Cell 3 – Location Security Identification (Physical Security)

Due to the complex nature of organisations, physical security is no longer limited to the access of a building. Physical security now provides for the physically securing of all assets in the organisation including, people, technology, information and processes (Fennelly 2016).



Physical Security

Pictorial Model:

Artefact Example:
The Australian Government physical security policy provides for all types of security including information technology resources, people, third parties, work health and safety, emergency management and policy.
https://www.protectivesecurity.gov.au/physicalsecurity/Pages/Physical-security-core-policy.aspx

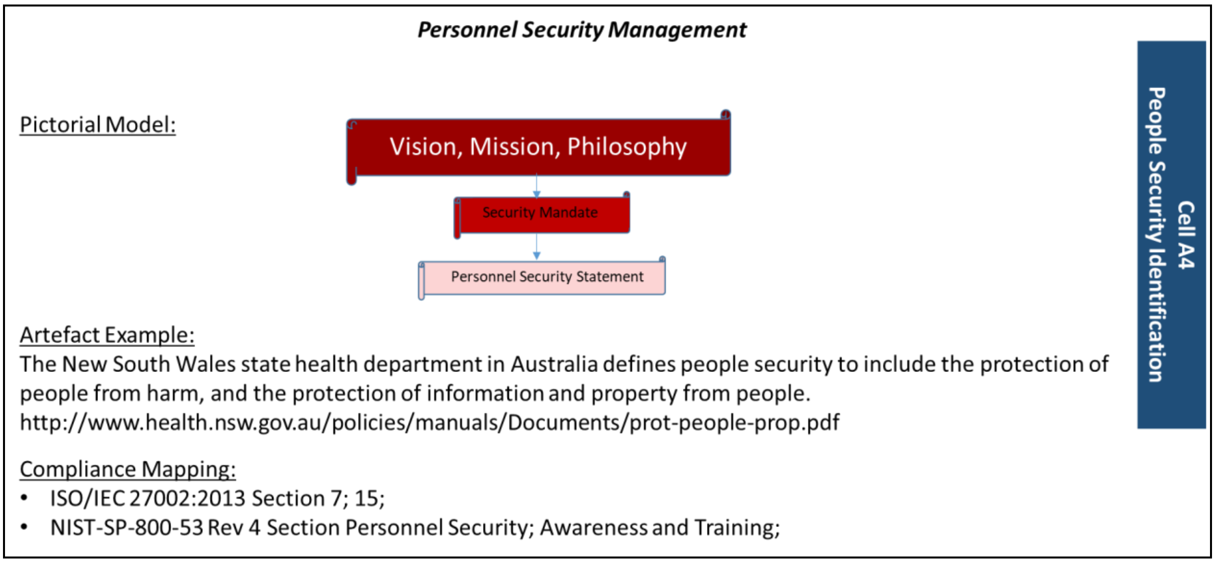
Compliance Mapping:

- ISO/IEC 27002:2013 Section 11; 9; 17;
- NIST-SP-800-53 Rev 4 Section Physical and Environmental Protection; System and Services Acquisition; Maintenance; Media Protection; Access Control; System and Communications Protection

Cell A3
Location Security Identification

Cell 4 – People Security Identification (Personnel Security Management)

At the executive conceptual level, people provide the largest challenge for security. From the beginning of a person joining or associating with an organisation, security training, keeping the individual safe, the identification and authentication of the person to the organisational systems and finally the termination process of the employee when they leave or disassociate with the company; are the most complex processes in an enterprise (Zafar 2013). The goal is to concurrently keep the people, the information and the assets secure, and this is derived from the corporate level commitment statement at the concept of the enterprise (Kirlappos and Sasse 2014).



Personnel Security Management

Pictorial Model:

Vision, Mission, Philosophy

Security Mandate

Personnel Security Statement

Cell A4
People Security Identification

Artefact Example:
The New South Wales state health department in Australia defines people security to include the protection of people from harm, and the protection of information and property from people.
http://www.health.nsw.gov.au/policies/manuals/Documents/prot-people-prop.pdf

Compliance Mapping:
- ISO/IEC 27002:2013 Section 7; 15;
- NIST-SP-800-53 Rev 4 Section Personnel Security; Awareness and Training;

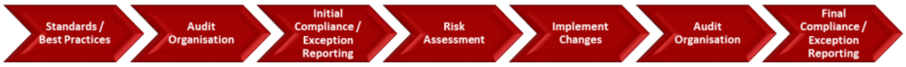
Cell 5 – Security Cycles Identification (Security Compliance)

At the executive level, organisations have an external security responsibility which can be legal, statutory, regulatory or contractual. The requirements to ensure the security within the organisation is in compliance with industry relevant standards, is often legislated and the reporting, mandatory. In addition to these compulsory requirements, organisations also have a moral responsibility to ensure the security of their staff, information, processes and technology. Security compliance provides a cyclic framework and process model to meet these obligations (Siponen et al. 2010; Vance et al. 2012).

Security Compliance

Cell A5
Security Cycles Identification

Pictorial Model:


Standards / Best Practices
Audit Organisation
Initial Compliance / Exception Reporting
Risk Assessment
Implement Changes
Audit Organisation
Final Compliance / Exception Reporting

Artefact Example:
The GEODIS Wilson corporate security policy highlights the importance of compliance, assessment, investigations and management responsibilities.
http://www.geodiswilson.com/upload/USA%20Files/Download%20Center_Tools%20and%20Resources/Policy%20Statements/Corporate%20Security%20Policy%20Statement%20GW_rev6.0.pdf

Compliance Mapping:
- ISO/IEC 27002:2013 Section 18; 6;
- NIST-SP-800-53 Rev 4 Section Certification and Accreditation and Security Assessments; Audit and Accountability

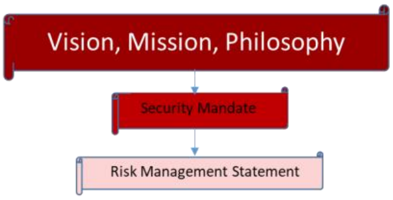
Cell 6 – Risk Management Identification (Risk Management)

The risk management statement is a corporate statement to external interested parties that describes the risk appetite and boundaries of the organisation. It expresses exactly what the company will and will not tolerate and how strongly they will implement safeguards and solutions to mitigate identified or potential risks (Lam 2014). The statement also identifies who is responsible in the organisation for risk and explains, usually based on culture, values or vision, where the risk appetite is motivated from – what the business drivers for risk are (Mayer et al. 2019; Webb et al. 2014). This statement is usually embedded in the corporate vision and may be incorporated with the security mandate.

Risk Management

Cell A6
Risk Management Identification

Pictorial Model:

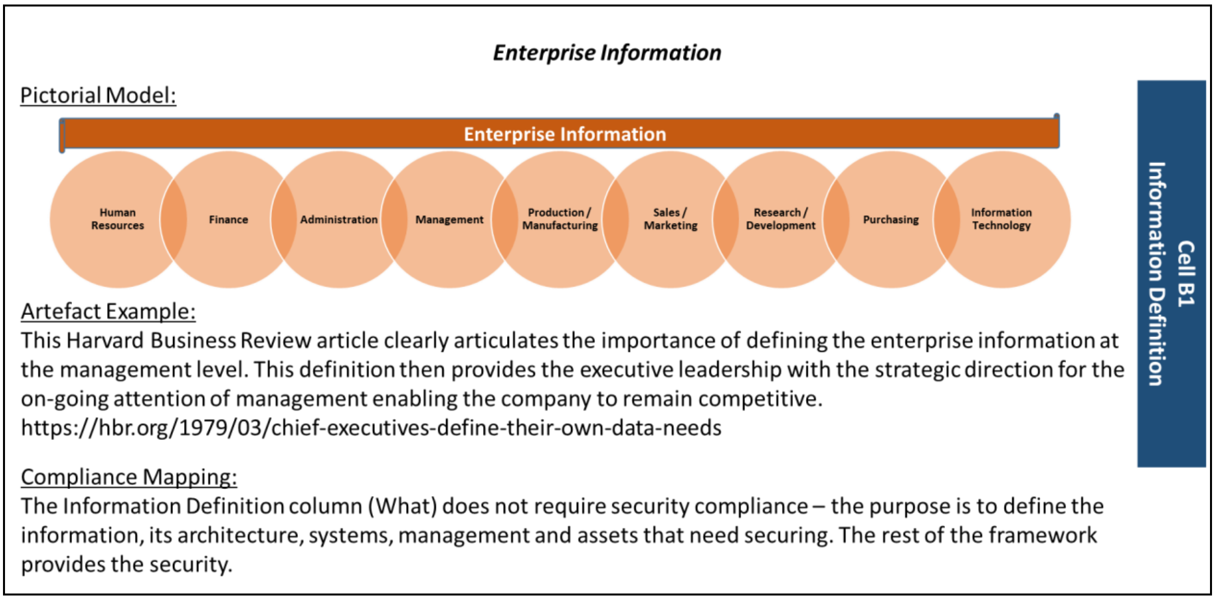


Artefact Example:
The Bank of America describes an open approach in their corporate risk statement which includes strong risk management practices to safeguard their company and customers.
http://about.bankofamerica.com/en-us/our-story/corporate-governance-and-risk.html#fbid=mFPD5IMscsE

Compliance Mapping:
- ISO/IEC 27002:2013 Section 5; 6; 15;
- NIST-SP-800-53 Rev 4 Section Risk Assessment

Cell 7 – Information Definition (Enterprise Information)

The information that is required for the organisation to function is defined here. It is initially a transformation from the corporate concept and evolves into all of the enterprise information that is used by the organisation for business to occur (Kirk 1999).



Enterprise Information

Pictorial Model:

Artefact Example:

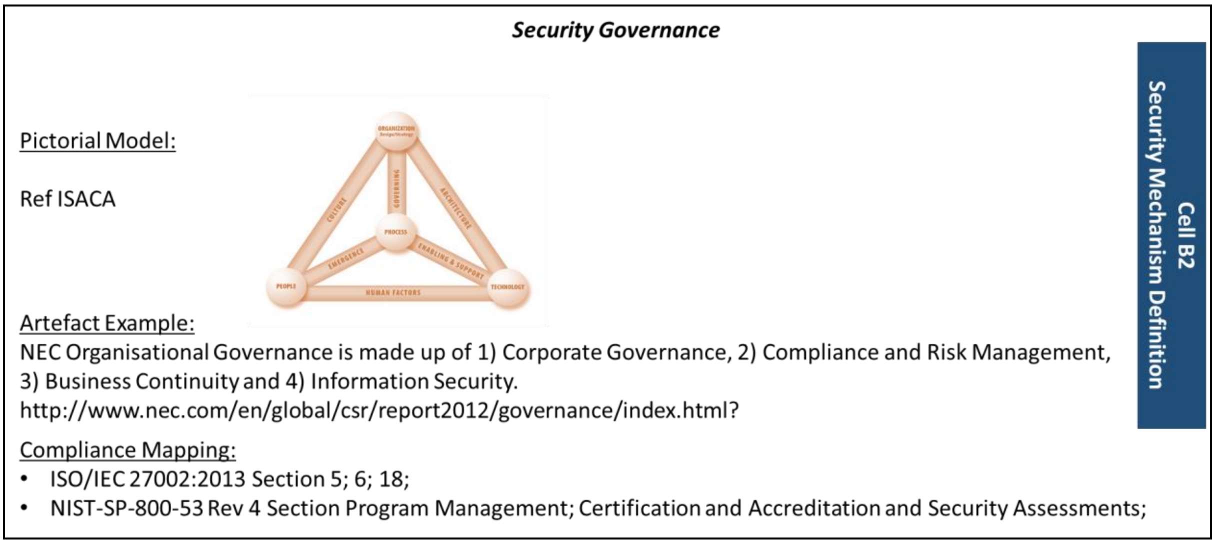
This Harvard Business Review article clearly articulates the importance of defining the enterprise information at the management level. This definition then provides the executive leadership with the strategic direction for the on-going attention of management enabling the company to remain competitive.
https://hbr.org/1979/03/chief-executives-define-their-own-data-needs

Compliance Mapping:

The Information Definition column (What) does not require security compliance – the purpose is to define the information, its architecture, systems, management and assets that need securing. The rest of the framework provides the security.

Cell 8 – Security Mechanism Definition (Security Governance)

A part of the organisational governance framework, security governance is the inclusion of a commitment to the securing of an organisation's information, its greatest asset, at the highest level – usually the board of directors or the CEO. This may include regulatory or statutory requirements and is the mechanism by which security is conceptualised within the organisation and provides a framework for the security to be implemented organisationally. It should include risk management and strategic alignment of security with business strategy (De Haes et al. 2013; Fitzgerald 2011; Moulton and Coles 2003).



Security Governance

Cell B2
Security Mechanism Definition

Pictorial Model:

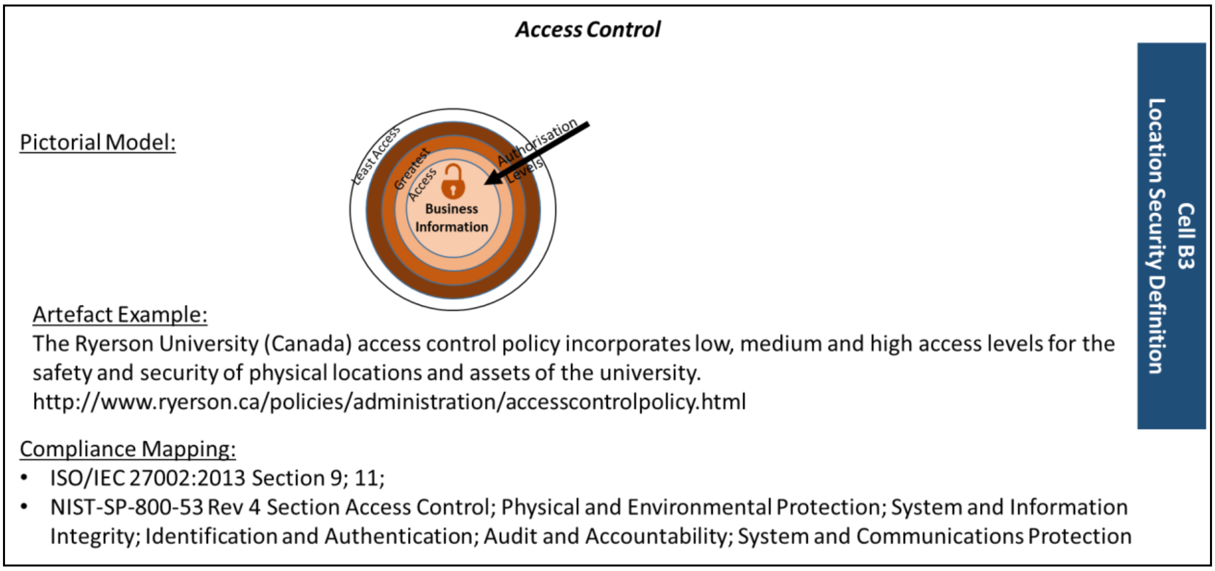
Ref ISACA

Artefact Example:
NEC Organisational Governance is made up of 1) Corporate Governance, 2) Compliance and Risk Management, 3) Business Continuity and 4) Information Security.
http://www.nec.com/en/global/csr/report2012/governance/index.html?

Compliance Mapping:
- ISO/IEC 27002:2013 Section 5; 6; 18;
- NIST-SP-800-53 Rev 4 Section Program Management; Certification and Accreditation and Security Assessments;

Cell 9 – Location Security Definition (Access Control)

Fundamentally, physical or locational security is access control. Being externally focused, it is the restriction of unauthorised external entities accessing organisational information whether that information be stored on a computer, in a filing cabinet, on a server or at a geographical location. Access control is normally managed through a layered approach. Those on the outer layers have zero access and those on the innermost layer have the highest level of access. The access changes as the entities role or need for the information changes. For example a line manager may have specific file access to their relevant staff information however, the managing director may have access to all staff (Anderson 2008; Sandhu et al. 1996; Sandhu and Samarati 1994).



Access Control

Pictorial Model:

Artefact Example:
The Ryerson University (Canada) access control policy incorporates low, medium and high access levels for the safety and security of physical locations and assets of the university.
http://www.ryerson.ca/policies/administration/accesscontrolpolicy.html

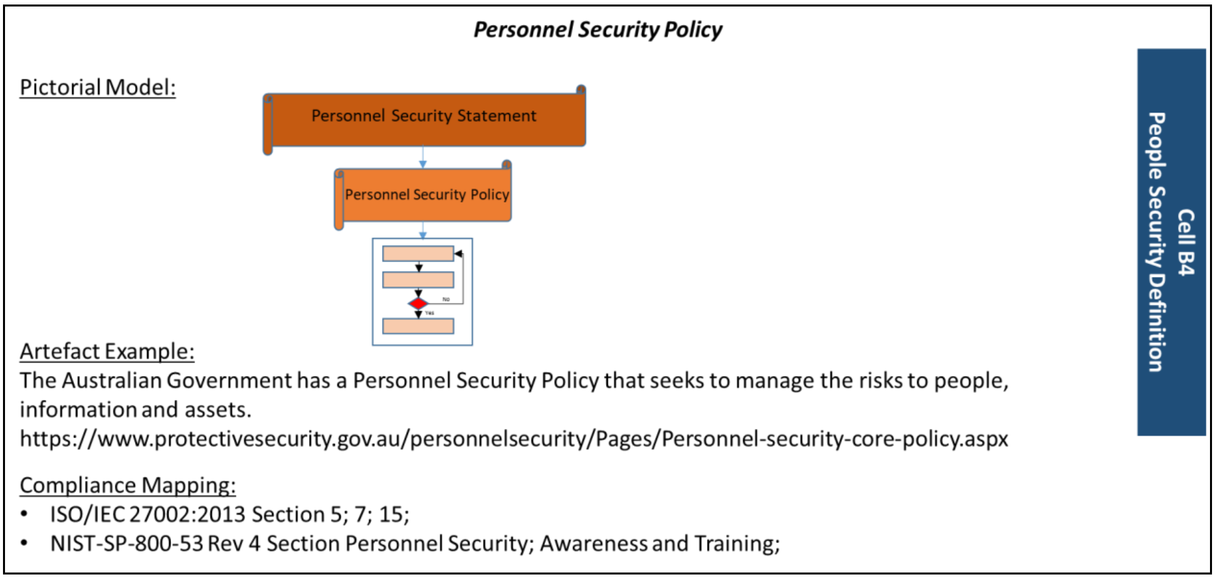
Compliance Mapping:

- ISO/IEC 27002:2013 Section 9; 11;
- NIST-SP-800-53 Rev 4 Section Access Control; Physical and Environmental Protection; System and Information Integrity; Identification and Authentication; Audit and Accountability; System and Communications Protection

Cell B3
Location Security Definition

Cell 10 – People Security Definition (Personnel Security Policy)

Internally focused, the personnel security policy provides the detailed guidelines and direction for the organisation. It is derived from the personnel security statement and articulates the organisational commitment to a personnel security program that includes identification and authentication, hiring and termination practices, the safety of people who interact with the company in any way, and the security training of personnel (Chaisiri and Ko 2016; Ifinedo 2012; Panchenko et al. 2018).



Personnel Security Policy

Pictorial Model:

Artefact Example:
The Australian Government has a Personnel Security Policy that seeks to manage the risks to people, information and assets.
https://www.protectivesecurity.gov.au/personnelsecurity/Pages/Personnel-security-core-policy.aspx

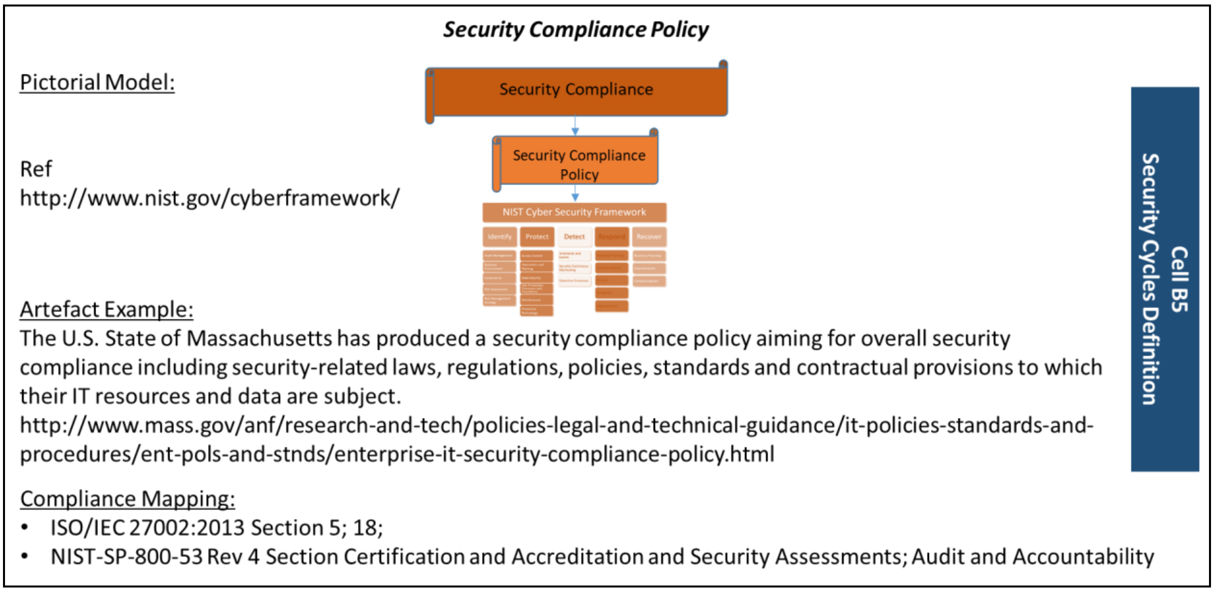
Compliance Mapping:

- ISO/IEC 27002:2013 Section 5; 7; 15;
- NIST-SP-800-53 Rev 4 Section Personnel Security; Awareness and Training;

Cell B4
People Security Definition

Cell 11 – Security Cycles Definition (Security Compliance Policy)

The security compliance policy is an internal business management tool that describes, for the organisation, what security standards will be implemented in the organisation, how often they will be audited and the level of commitment to the process the business stakeholders should expect (Ifinedo 2012; NIST 2013; Safa et al. 2016).



Security Compliance Policy

Pictorial Model:

Ref
http://www.nist.gov/cyberframework/

Security Compliance
Security Compliance Policy
NIST Cyber Security Framework
Identify
Protect
Detect
Respond
Recover

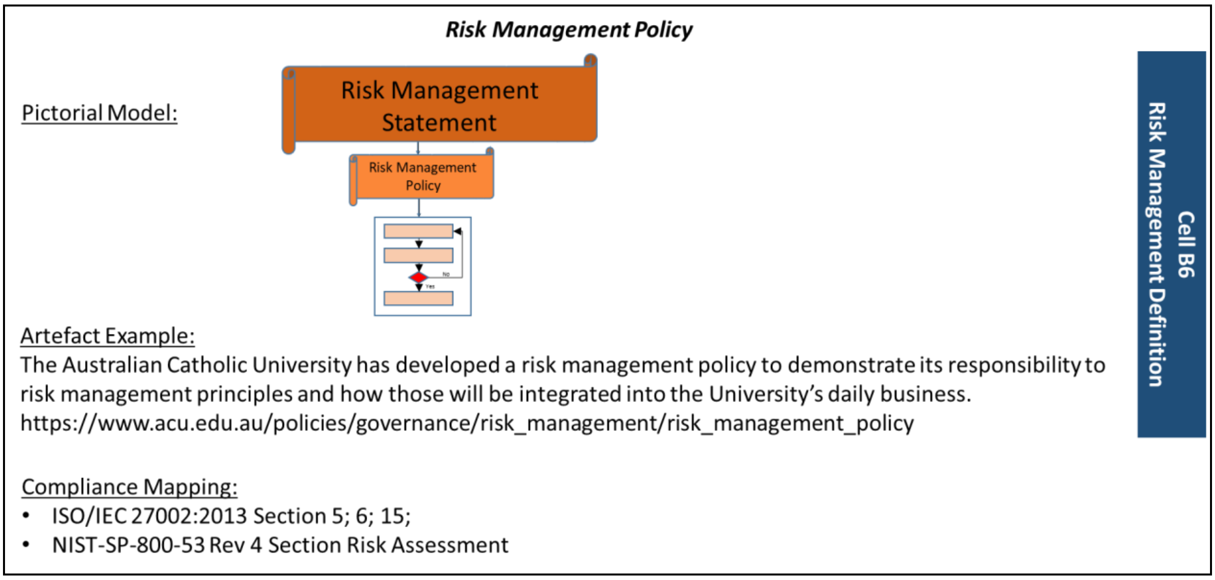
Artefact Example:
The U.S. State of Massachusetts has produced a security compliance policy aiming for overall security compliance including security-related laws, regulations, policies, standards and contractual provisions to which their IT resources and data are subject.
http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/it-policies-standards-and-procedures/ent-pols-and-stnds/enterprise-it-security-compliance-policy.html

Compliance Mapping:
- ISO/IEC 27002:2013 Section 5; 18;
- NIST-SP-800-53 Rev 4 Section Certification and Accreditation and Security Assessments; Audit and Accountability

Cell B5
Security Cycles Definition

Cell 12 – Risk Management Definition (Risk Management Policy)

The risk management policy provides a clear intention to internal staff of the organisation's commitment to risk management and is the guidance for the implementation of the risk management statement. Broadly, it should provide the purpose and scope of the policy, place the information in context with the organisation's business management, define the risk management model that is being used and specify responsibilities and roles within the organisation. (Hopkin 2018; Lam 2014; Mayer et al. 2019; Webb et al. 2014)



Risk Management Policy

Pictorial Model:

Risk Management Statement
Risk Management Policy
No
Yes

Cell B6
Risk Management Definition

Artefact Example:
The Australian Catholic University has developed a risk management policy to demonstrate its responsibility to risk management principles and how those will be integrated into the University's daily business.
https://www.acu.edu.au/policies/governance/risk_management/risk_management_policy

Compliance Mapping:

- ISO/IEC 27002:2013 Section 5; 6; 15;
- NIST-SP-800-53 Rev 4 Section Risk Assessment

Cell 13 – Information Representation (Enterprise Architecture)

EA states that an organisation is at least as complex as a large construction project and should be engineered using the same process; the context, the concept, the design, the build, the implementation and the use. EA provides a link between organisational goals and mission statements, through the organisational layers, down to the project level, just as an initial engineering concept document is traceable to a final built product. The organisation's assets are defined in EA as people, information, process and technology, and these are used to implement the vision of the organisation (DoD 2010; Gampfer et al. 2018; Gerber et al. 2020; Mentz et al. 2014; Zachman 2015).

Enterprise Architecture

Cell C1
Information Representation

Pictorial Model:

Artefact Example:
The Australian Government EA provides the government departments a common language and structure for cost-effective, consistent and cohesive delivery of ICT services.
http://www.finance.gov.au/policy-guides-procurement/australian-government-architecture-aga/

Compliance Mapping:
The Information Definition column (What) does not require security compliance – the purpose is to define the information, its architecture, systems, management and assets that need securing. The rest of the framework provides the security.

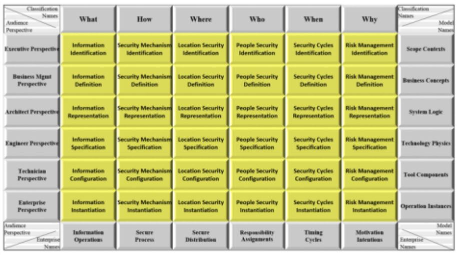
Cell 14 – Security Mechanism Representation (Enterprise Security Architecture)

The security mechanism used for representation of security in the organisation is enterprise security architecture. It is a holistic strategy that includes all security controls (not just IT security) in the organisation and places them in the most advantageous position. This organisational view provides an assurance that the organisation is meeting its corporate and moral requirements for security (Killmeyer 2006; McClintock et al. 2020; Sherwood et al. 1995).

Enterprise Security Architecture

Cell C2
Security Mechanism Representation

Pictorial Model:



Classification Names Audience Perspective	What	How	Where	Who	When	Why	Classification Names Model Names
Executive Perspective	Information Identification	Security Mechanism Identification	Location Security Identification	People Security Identification	Security Cycles Identification	Risk Management Identification	Scope Contexts
Business Mgmt Perspective	Information Definition	Security Mechanism Definition	Location Security Definition	People Security Definition	Security Cycles Definition	Risk Management Definition	Business Concepts
Architect Perspective	Information Representation	Security Mechanism Representation	Location Security Representation	People Security Representation	Security Cycles Representation	Risk Management Representation	System Logic
Engineer Perspective	Information Specification	Security Mechanism Specification	Location Security Specification	People Security Specification	Security Cycles Specification	Risk Management Specification	Technology Physics
Technician Perspective	Information Configuration	Security Mechanism Configuration	Location Security Configuration	People Security Configuration	Security Cycles Configuration	Risk Management Configuration	Tool Components
Enterprise Perspective	Information Instantiation	Security Mechanism Instantiation	Location Security Instantiation	People Security Instantiation	Security Cycles Instantiation	Risk Management Instantiation	Operation Instances
Audience Perspective Enterprise Names	Information Operations	Secure Process	Secure Distribution	Responsibility Assignments	Timing Cycles	Motivation Intentions	Model Names Enterprise Names

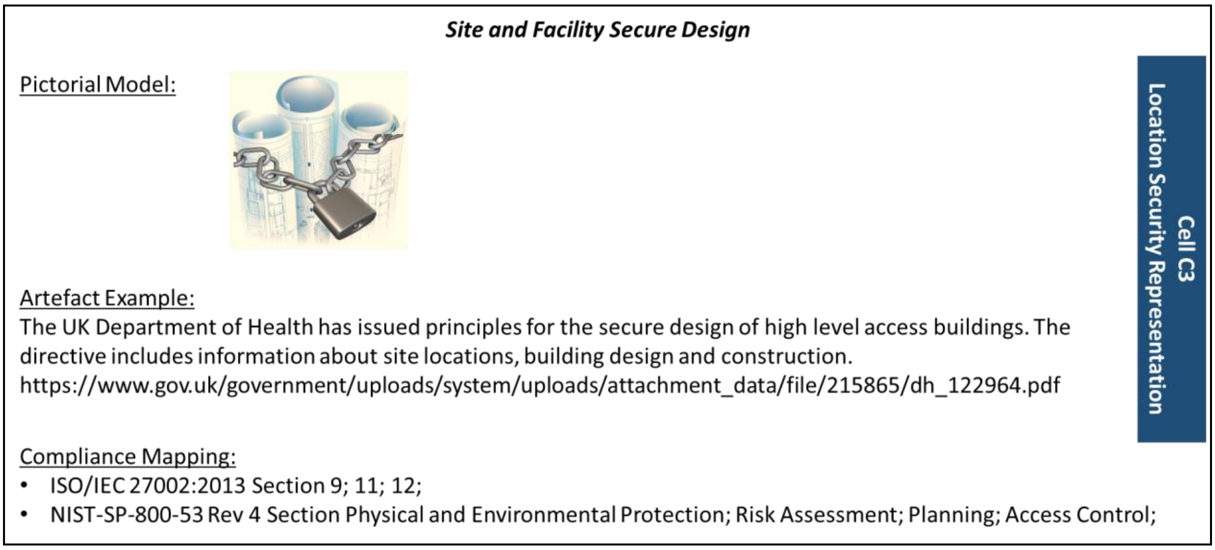
Artefact Example:
SABSA is an example of an enterprise security architecture framework that is commercially used by organisations.
http://www.sabsa.org/

Compliance Mapping:

- ISO/IEC 27002:2013 Section 5; 6;
- NIST-SP-800-53 Rev 4 Section Program Management; Planning

Cell 15 – Location Security Representation (Site & Facility Secure Design)

The secure design of facilities and sites is the first line of physical defence for organisations. Whether the facility be existing or a new site, the security design process can be applied for maximum benefit. The design will at least include secure designs for neighbourhood, perimeter, access and parking, operations and the building (DiMase et al. 2015; Fennelly 2016; Peltier 2013).



Site and Facility Secure Design

Pictorial Model:

Artefact Example:
The UK Department of Health has issued principles for the secure design of high level access buildings. The directive includes information about site locations, building design and construction.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/215865/dh_122964.pdf

Compliance Mapping:
- ISO/IEC 27002:2013 Section 9; 11; 12;
- NIST-SP-800-53 Rev 4 Section Physical and Environmental Protection; Risk Assessment; Planning; Access Control;

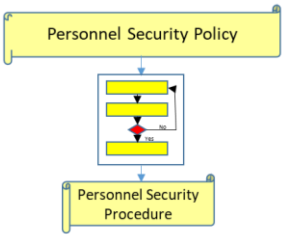
Cell C3
Location Security Representation

Cell 16 – People Security Representation (Personnel Security Plan)

The personnel security plan is derived from the personnel security policies. It is the high level building block from which the procedures and security program are created. How the processes will interact with each other and the technologies which may be used are formalised. The concepts of the personnel security plan are translated to the actions that will achieve the personnel security policy goals (Clark et al. 2014; Höne and Eloff 2002; ISO 2013).

Personnel Security Plan

Pictorial Model:



Artefact Example:
The United States Department of Homeland Security personnel security process is focused on the employment aspect of security for personnel. Each organisation will have a personnel security process based on their needs.
https://www.fas.org/sgp/othergov/dhs/persec.pdf

Compliance Mapping:

- ISO/IEC 27002:2013 Section 7; 9; 15
- NIST-SP-800-53 Rev 4 Section Personnel Security; Planning; Awareness and Training; Access Control; Identification and Authentication;

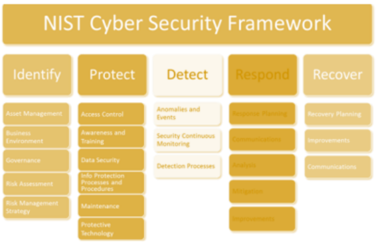
Cell C4
People Security Representation

Cell 17 – Security Cycles Representation (Certification Framework)

The security certification framework has already been named in the security compliance policy and is now articulated in detail. The framework is used to audit for compliance and assurance and will include enough detail for organisational accountability. The security framework will cover all aspects of the organisation (ISO 2013; NIST 2013; Whitman and Mattord 2011).

Certification Framework

Pictorial Model:



Ref
http://www.nist.gov/cyberframework/

Artefact Example:
The NIST Cyber Security framework is a security framework which an organisation can use to certify their security program against.
https://www.nist.gov/topics/cybersecurity

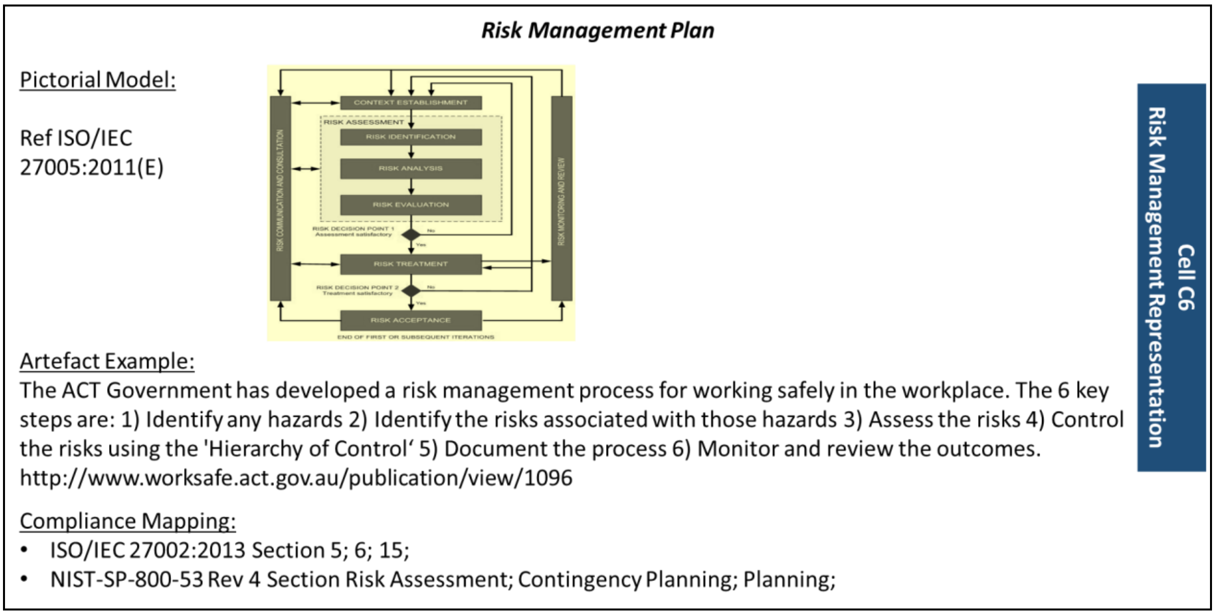
Compliance Mapping:

- ISO/IEC 27002:2013 Section 6; 18;
- NIST-SP-800-53 Rev 4 Section Certification and Accreditation and Security Assessments; Audit and Accountability; Planning;

Cell C5
Security Cycles Representation

Cell 18 – Risk Management Representation (Risk Management Plan)

According to ISO 31000:2009, a risk management plan is one that systematically applies management policies, procedures, and practices to a set of activities intended to establish the context, communicate and consult with stakeholders, and identify, analyse, evaluate, treat, monitor, and review risk (Hopkin 2018; Lam 2014; Mayer et al. 2019).



Risk Management Plan

Pictorial Model:

Ref ISO/IEC 27005:2011(E)

Artefact Example:

The ACT Government has developed a risk management process for working safely in the workplace. The 6 key steps are: 1) Identify any hazards 2) Identify the risks associated with those hazards 3) Assess the risks 4) Control the risks using the 'Hierarchy of Control' 5) Document the process 6) Monitor and review the outcomes. http://www.worksafe.act.gov.au/publication/view/1096

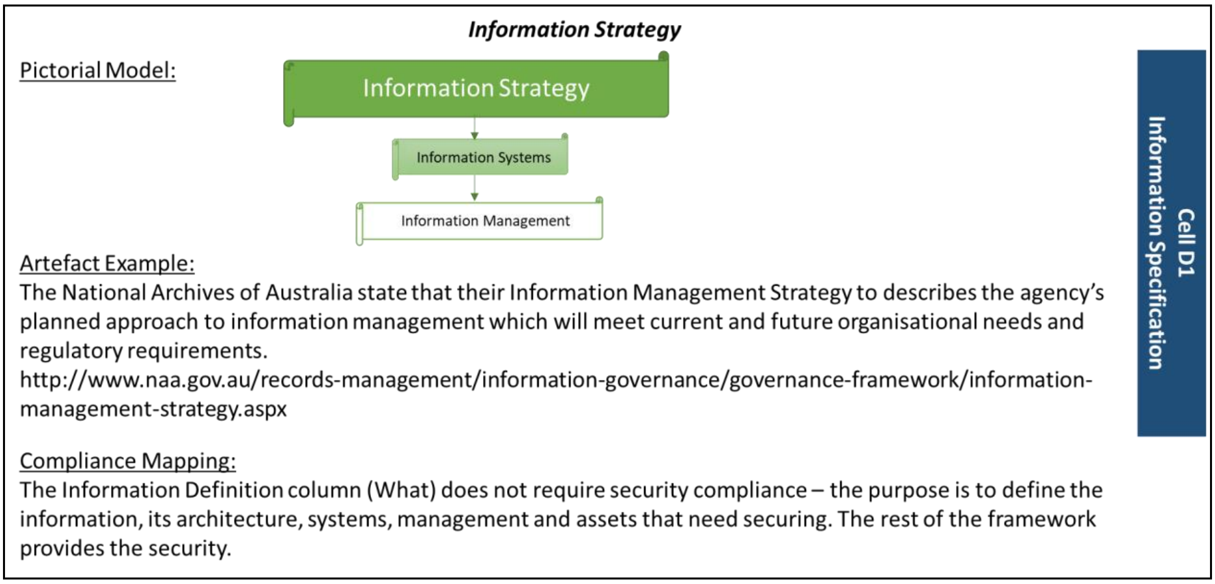
Compliance Mapping:

- ISO/IEC 27002:2013 Section 5; 6; 15;
- NIST-SP-800-53 Rev 4 Section Risk Assessment; Contingency Planning; Planning;

Cell C6
Risk Management Representation

Cell 19 – Information Specification

The organisational information strategy is a management instrument that ensures information assets of the organisation are linked to the delivery of the organisation's mission. It will include the purpose, strategic direction, responsibilities, reporting and the detailed requirements and specifications for the use of the information assets. Security is an intrinsic and an explicit part of the information strategy (Applegate et al. 2006; Malhotra 2000; Orna 2017).



Information Strategy

Pictorial Model:

Artefact Example:

The National Archives of Australia state that their Information Management Strategy to describes the agency's planned approach to information management which will meet current and future organisational needs and regulatory requirements.
http://www.naa.gov.au/records-management/information-governance/governance-framework/information-management-strategy.aspx

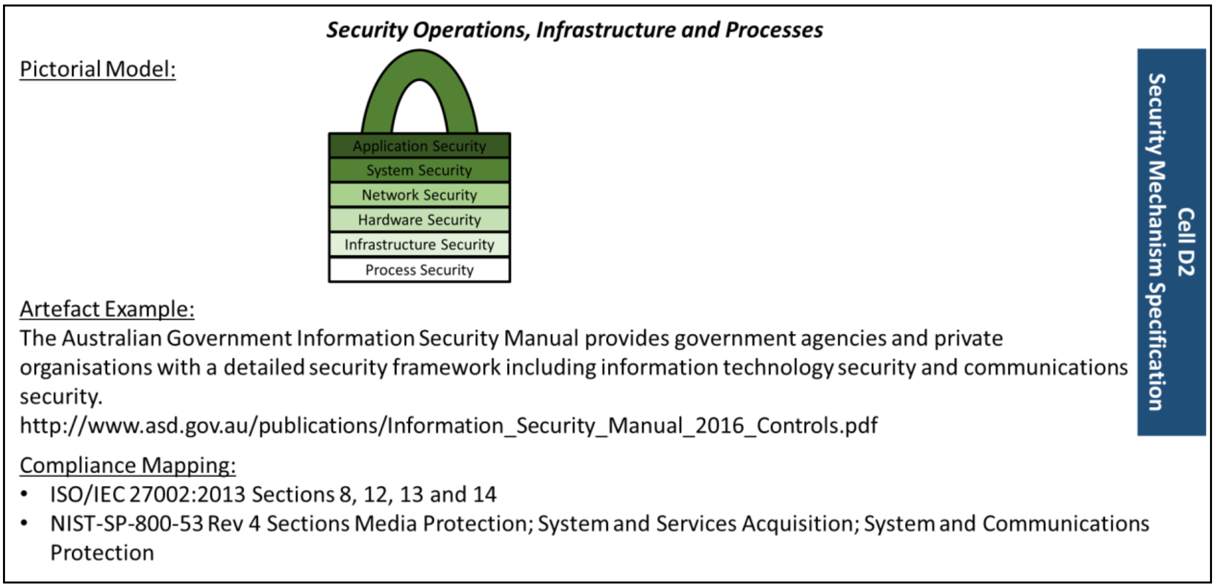
Compliance Mapping:

The Information Definition column (What) does not require security compliance – the purpose is to define the information, its architecture, systems, management and assets that need securing. The rest of the framework provides the security.

Cell D1
Information Specification

Cell 20 – Security Mechanism Specification (Security Operations, Infrastructure and Processes)

The security controls policy and the architectures developed from Rows 2 and 3 become physically depicted in the security operations, infrastructure and processes. This is where the traditionally held view of information security can be found such as security mechanisms for applications, operating systems and networks. It also extends to hardware, infrastructure and process security (Anderson 2008; Gollmann 2010; McCrie 2015).



Security Operations, Infrastructure and Processes

Pictorial Model:

Artefact Example:

The Australian Government Information Security Manual provides government agencies and private organisations with a detailed security framework including information technology security and communications security.
http://www.asd.gov.au/publications/Information_Security_Manual_2016_Controls.pdf

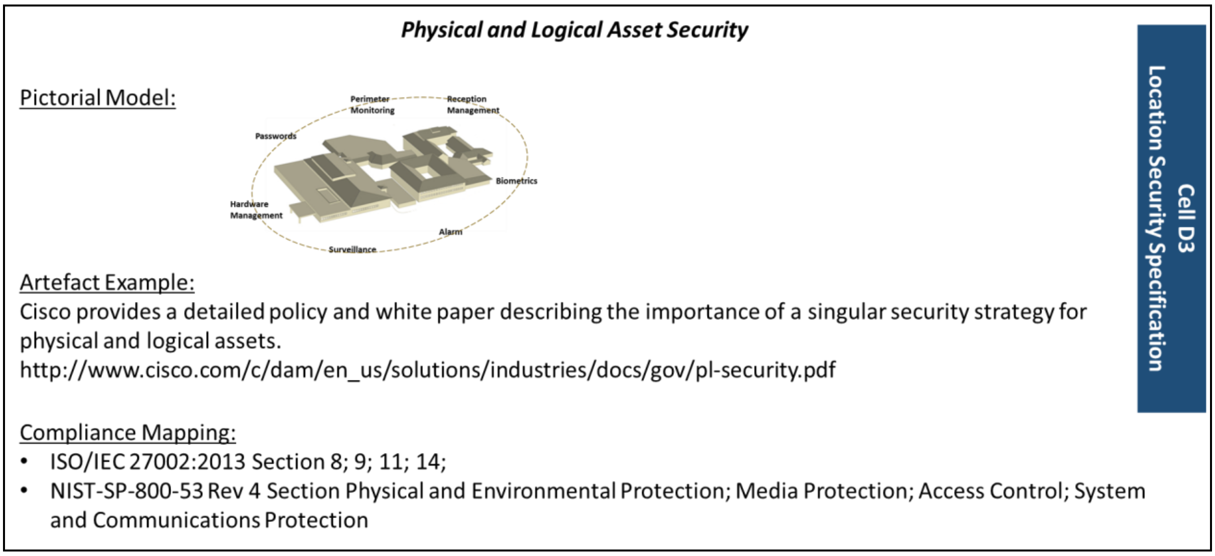
Compliance Mapping:

- ISO/IEC 27002:2013 Sections 8, 12, 13 and 14
- NIST-SP-800-53 Rev 4 Sections Media Protection; System and Services Acquisition; System and Communications Protection

Cell D2
Security Mechanism Specification

Cell 21 – Location Security Specification (Physical and Logical Asset Security)

Physical security restricts the physical access to buildings but also includes restricting the access to the physical aspects of computing like system hardware and wiring. Logical security is the use of information and communications technology to restrict the logical access to the information and systems in an organisation. Combining these two strategies provides a greater level of security than the individual components and achieves a strong defence-in-depth security model (DiMase et al. 2015; Fennelly 2016; Lindsay 2009).



Physical and Logical Asset Security

Pictorial Model:

Perimeter Monitoring
Reception Management
Passwords
Biometrics
Hardware Management
Alarm
Surveillance

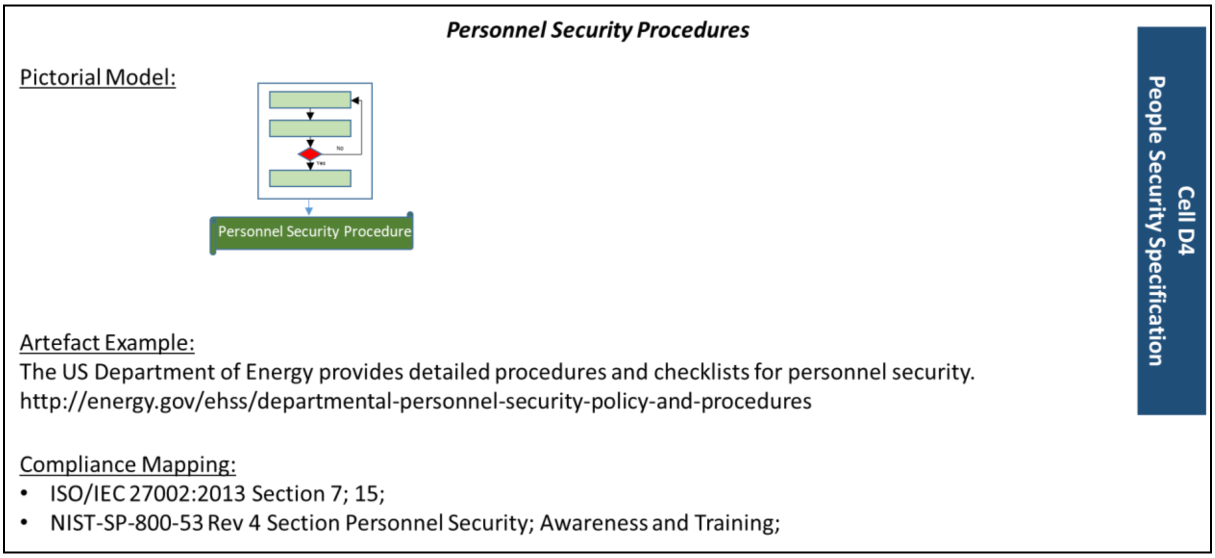
Artefact Example:
Cisco provides a detailed policy and white paper describing the importance of a singular security strategy for physical and logical assets.
http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/pl-security.pdf

Compliance Mapping:
- ISO/IEC 27002:2013 Section 8; 9; 11; 14;
- NIST-SP-800-53 Rev 4 Section Physical and Environmental Protection; Media Protection; Access Control; System and Communications Protection

Cell D3
Location Security Specification

Cell 22 – People Security Specification (Personnel Security Procedures)

The personnel security procedures are the detailed specifications of the personnel security process. It is a physical depiction of how the processes are to be conducted. The procedures often include who is responsible, where it will be done and how. Step by step, sequenced instructions are included for each personnel security procedure. The procedures are tested and proven before being implemented (Peltier 2016; Zafar 2013).



Personnel Security Procedures

Pictorial Model:

No
Yes
Personnel Security Procedure

Artefact Example:
The US Department of Energy provides detailed procedures and checklists for personnel security.
http://energy.gov/ehss/departmental-personnel-security-policy-and-procedures

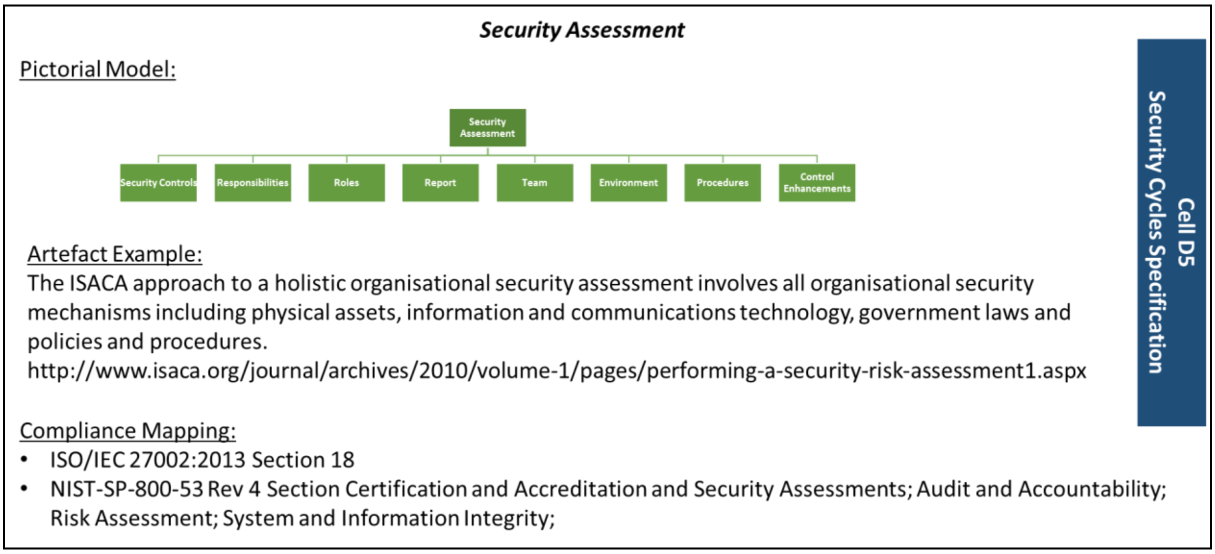
Compliance Mapping:

- ISO/IEC 27002:2013 Section 7; 15;
- NIST-SP-800-53 Rev 4 Section Personnel Security; Awareness and Training;

Cell D4
People Security Specification

Cell 23 – Security Cycles Specification (Security Assessment)

Once implemented, the organisation must be assessed for compliance against the security certification framework. This process is called security assessment and measures the degree to which security system controls are correctly implemented, whether they are functioning as anticipated and whether they are generating the desired level of security (Clinch 2009; Jordan et al. 2018; Theoharidou and Gritzalis 2007).



Security Assessment

Pictorial Model:

Security Assessment
Security Controls
Responsibilities
Roles
Report
Team
Environment
Procedures
Control Enhancements

Artefact Example:
The ISACA approach to a holistic organisational security assessment involves all organisational security mechanisms including physical assets, information and communications technology, government laws and policies and procedures.
http://www.isaca.org/journal/archives/2010/volume-1/pages/performing-a-security-risk-assessment1.aspx

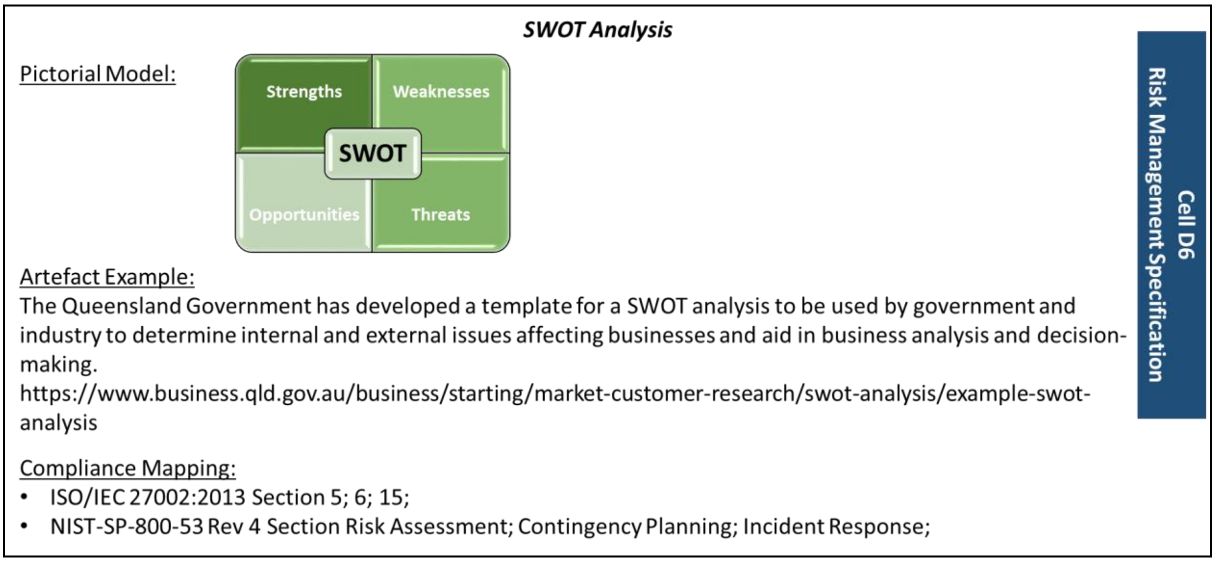
Compliance Mapping:

- ISO/IEC 27002:2013 Section 18
- NIST-SP-800-53 Rev 4 Section Certification and Accreditation and Security Assessments; Audit and Accountability; Risk Assessment; System and Information Integrity;

Cell D5
Security Cycles Specification

Cell 24 – Risk Management Specification (SWOT Analysis)

A strengths, weaknesses, opportunities and threats (SWOT) analysis identifies the internal strengths and weaknesses, as well as its external opportunities and threats of an organisation. The purpose is to provide a detailed list of risks that could adversely affect the organisation and decide how these should be managed. Additionally the advantages the organisation has are also available to be leveraged into the business model (Akman 2019; Gürel and Tat 2017; NIST 2010).



SWOT Analysis

Pictorial Model:

Strengths
Weaknesses
SWOT
Opportunities
Threats

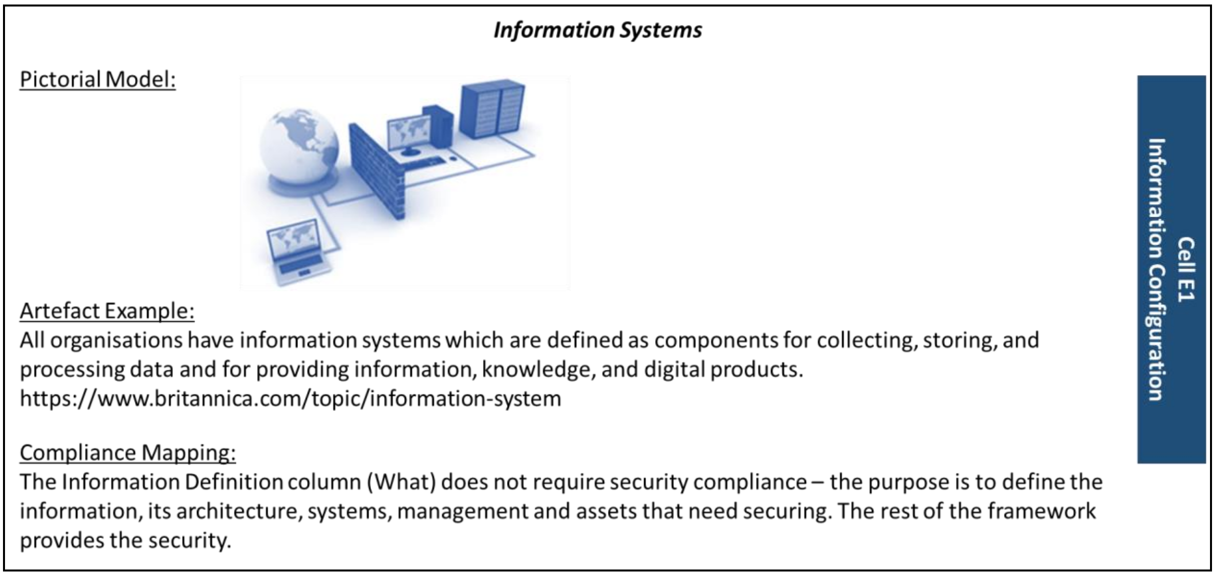
Artefact Example:
The Queensland Government has developed a template for a SWOT analysis to be used by government and industry to determine internal and external issues affecting businesses and aid in business analysis and decision-making.
https://www.business.qld.gov.au/business/starting/market-customer-research/swot-analysis/example-swot-analysis

Compliance Mapping:
- ISO/IEC 27002:2013 Section 5; 6; 15;
- NIST-SP-800-53 Rev 4 Section Risk Assessment; Contingency Planning; Incident Response;

Cell D6
Risk Management Specification

Cell 25 – Information Configuration (Information Systems)

The systems that manage the informational assets of the organisation and are used to collect, filter, process, create and distribute the information for the purpose of achieving the corporate strategy (Acuña 2016; DeLone and McLean 2016; Galliers et al. 2006).



Information Systems

Pictorial Model:

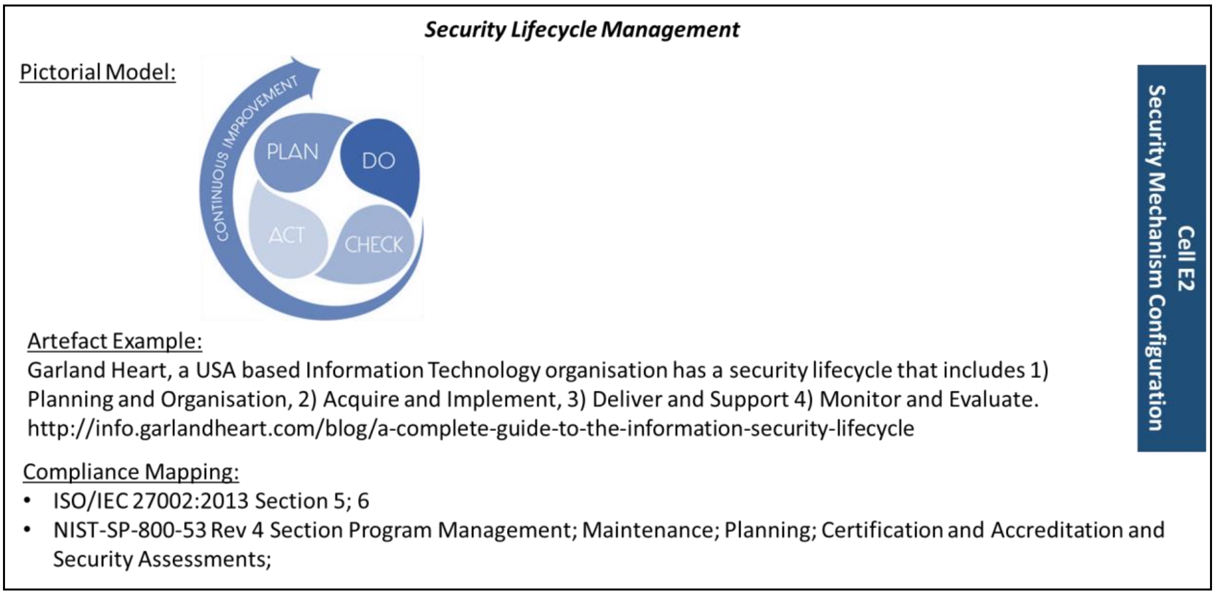
Artefact Example:
All organisations have information systems which are defined as components for collecting, storing, and processing data and for providing information, knowledge, and digital products.
https://www.britannica.com/topic/information-system

Compliance Mapping:
The Information Definition column (What) does not require security compliance – the purpose is to define the information, its architecture, systems, management and assets that need securing. The rest of the framework provides the security.

Cell E1
Information Configuration

Cell 26 – Security Mechanism Configuration (Security Lifecycle Management)

Security within an organisation should be constantly monitored, evaluated and improved when necessary. It is not a static program that is put in place and never visited again. The Deming cycle of Plan, Do, Check, Act provides a good basis for a security lifecycle which should be a part of the lifecycle from its inception (Gilliam et al. 2003; Moen and Norman 2006).


CONTINUOUS IMPROVEMENT
PLAN
DO
ACT
CHECK

Security Lifecycle Management

Pictorial Model:

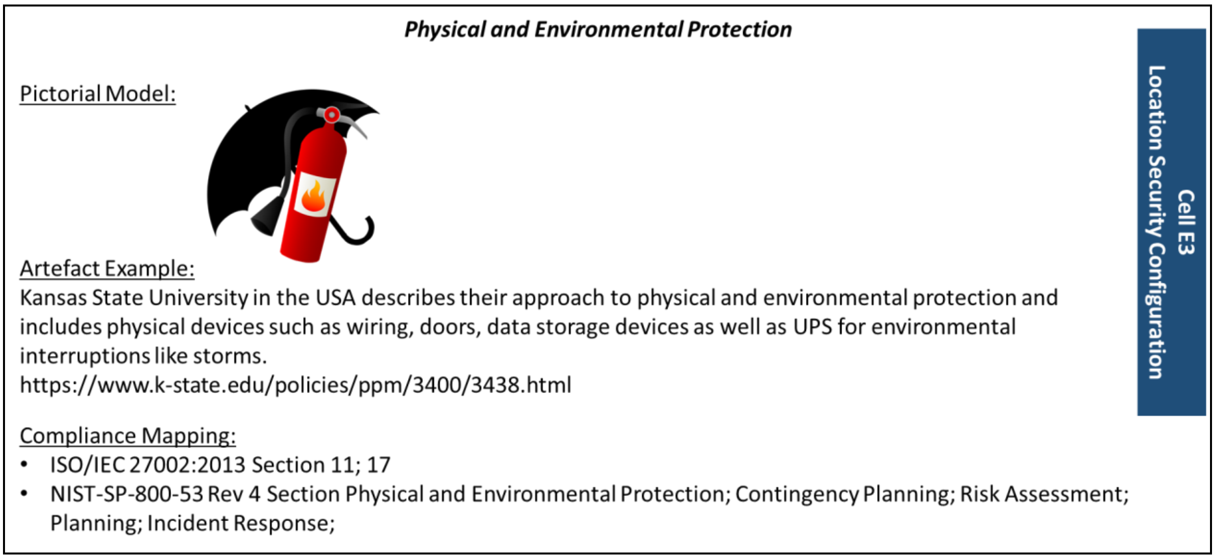
Artefact Example:
Garland Heart, a USA based Information Technology organisation has a security lifecycle that includes 1) Planning and Organisation, 2) Acquire and Implement, 3) Deliver and Support 4) Monitor and Evaluate.
http://info.garlandheart.com/blog/a-complete-guide-to-the-information-security-lifecycle

Compliance Mapping:
- ISO/IEC 27002:2013 Section 5; 6
- NIST-SP-800-53 Rev 4 Section Program Management; Maintenance; Planning; Certification and Accreditation and Security Assessments;

Cell E2
Security Mechanism Configuration

Cell 27 – Location Security Configuration (Physical and Environmental Protection)

Physical and environmental security and protection takes asset security one step further. It includes all threats to the physical environment of the organisation, particularly non-nefarious threats. These can include fire, flood, storms, power outages, interruption to business, chemical spills and electromagnetic interference. The protection is in the form of proactive planning and securing of the organisational information against these kinds of threats and often includes such measures as offsite backup mechanisms (Comfort 2005; Snedaker 2013; Stanton 2005).



Physical and Environmental Protection

Cell E3
Location Security Configuration

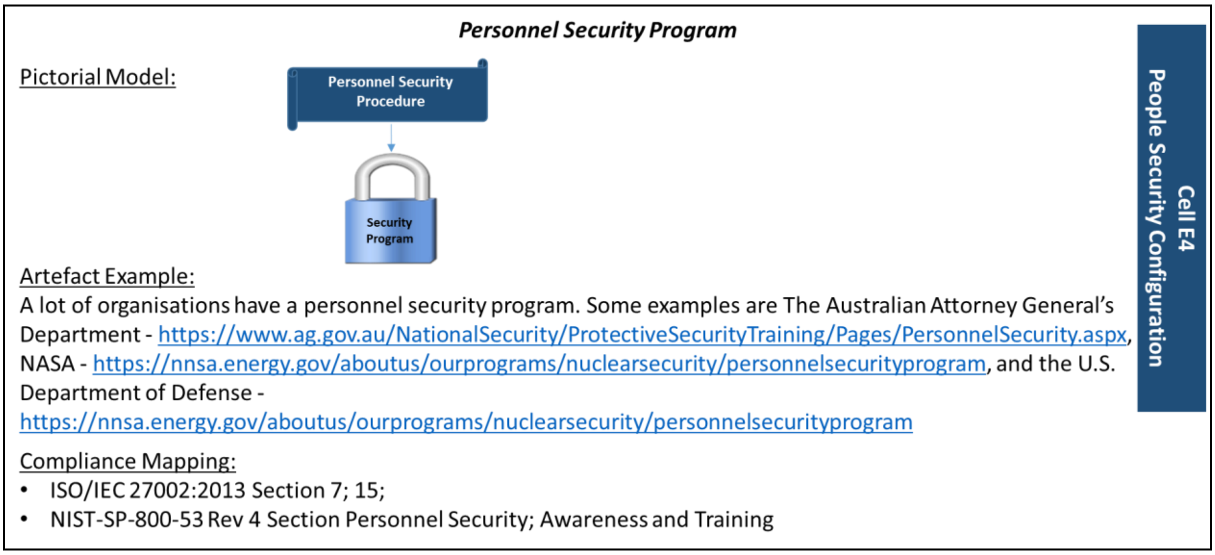
Pictorial Model:

Artefact Example:
Kansas State University in the USA describes their approach to physical and environmental protection and includes physical devices such as wiring, doors, data storage devices as well as UPS for environmental interruptions like storms.
https://www.k-state.edu/policies/ppm/3400/3438.html

Compliance Mapping:
- ISO/IEC 27002:2013 Section 11; 17
- NIST-SP-800-53 Rev 4 Section Physical and Environmental Protection; Contingency Planning; Risk Assessment; Planning; Incident Response;

Cell 28 – People Security Configuration (Personnel Security Program)

The implemented vision of the personnel security statement is the personnel security program. It is the organisational program that includes all aspects of personnel security that are conducted to keep people secure. This includes securing access by people to organisational information and assets; ensuring the hiring and termination of people is conducted in a secure manner; the safety of staff, contractors and any person who interacts with the organisation; and the ongoing security training of personnel (Wilson and Hash 2003; Zafar 2013).



Personnel Security Program

Cell E4
People Security Configuration

Pictorial Model:

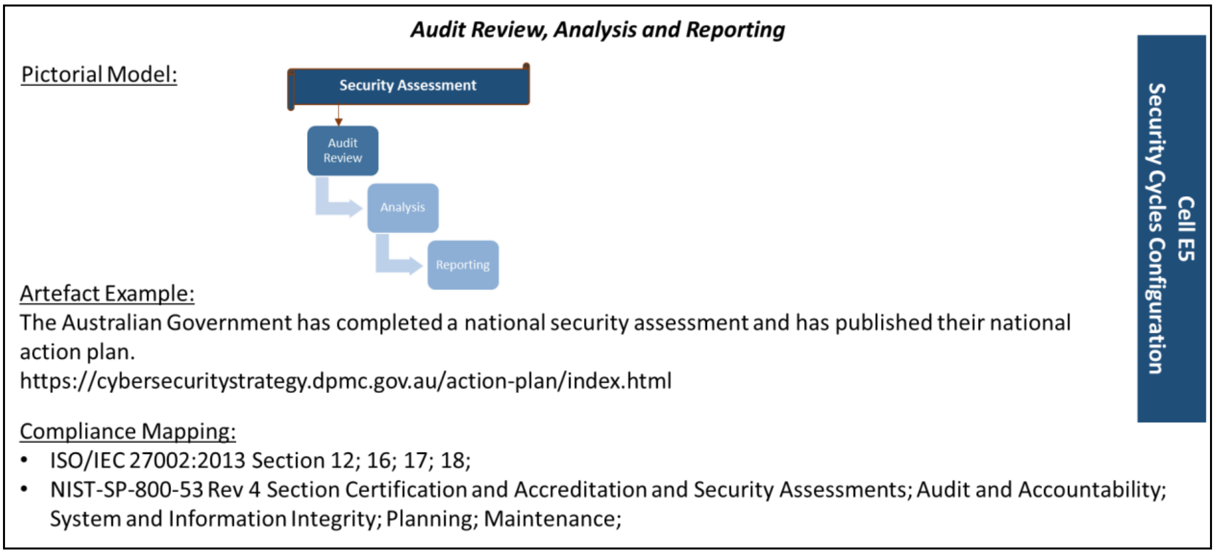
Personnel Security Procedure
Security Program

Artefact Example:
A lot of organisations have a personnel security program. Some examples are The Australian Attorney General's Department - https://www.ag.gov.au/NationalSecurity/ProtectiveSecurityTraining/Pages/PersonnelSecurity.aspx, NASA - https://nnsa.energy.gov/aboutus/ourprograms/nuclearsecurity/personnelsecurityprogram, and the U.S. Department of Defense - https://nnsa.energy.gov/aboutus/ourprograms/nuclearsecurity/personnelsecurityprogram

Compliance Mapping:
- ISO/IEC 27002:2013 Section 7; 15;
- NIST-SP-800-53 Rev 4 Section Personnel Security; Awareness and Training

<u>Cell 29 – Security Cycles Configuration (Audit Review, Analysis and Reporting)</u>

Once the security assessment or audit is complete, an action plan is done which involves review, analysis and reporting of the audit. The results of the security assessment are weighed using a risk assessment process (see column 6, row 5) and a strategy is developed for any non-compliance items. The outcome is the re-alignment of the organisation with the security compliance policy and the certification framework. (De Haes et al. 2013; Korpela 2015; Shackleford 2016).



Audit Review, Analysis and Reporting

Cell E5
Security Cycles Configuration

Pictorial Model:

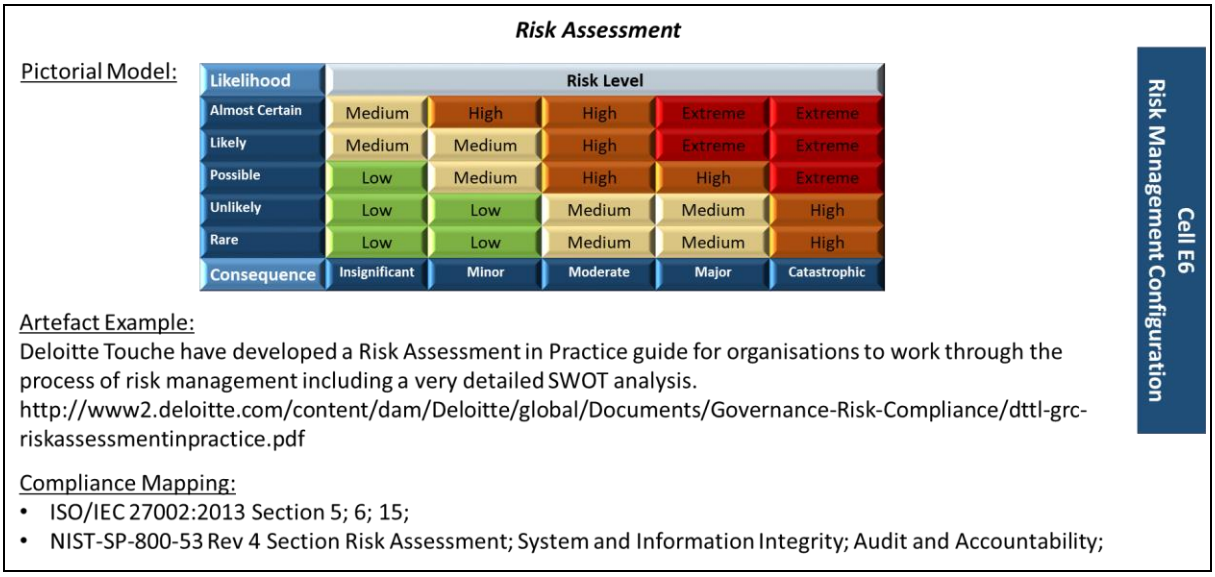
Security Assessment
Audit Review
Analysis
Reporting

Artefact Example:
The Australian Government has completed a national security assessment and has published their national action plan.
https://cybersecuritystrategy.dpmc.gov.au/action-plan/index.html

Compliance Mapping:
- ISO/IEC 27002:2013 Section 12; 16; 17; 18;
- NIST-SP-800-53 Rev 4 Section Certification and Accreditation and Security Assessments; Audit and Accountability; System and Information Integrity; Planning; Maintenance;

Cell 30 – Risk Management Configuration (Risk Assessment)

Risk assessment involves the evaluation and estimation of the levels of risks for each identified weakness and threat produced from the SWOT analysis. This is done using a likelihood versus consequence matrix where the likelihood that the risk will occur is compared against the consequences if the risk were to occur. A risk level is assigned and based on this level, the risk is appropriately managed (NIST 2014; Zio 2018).



Risk Assessment

Pictorial Model:

Likelihood	Risk Level				
Almost Certain	Medium	High	High	Extreme	Extreme
Likely	Medium	Medium	High	Extreme	Extreme
Possible	Low	Medium	High	High	Extreme
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium	High
Consequence	Insignificant	Minor	Moderate	Major	Catastrophic

Artefact Example:
Deloitte Touche have developed a Risk Assessment in Practice guide for organisations to work through the process of risk management including a very detailed SWOT analysis.
http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf

Compliance Mapping:
- ISO/IEC 27002:2013 Section 5; 6; 15;
- NIST-SP-800-53 Rev 4 Section Risk Assessment; System and Information Integrity; Audit and Accountability;

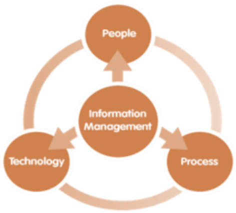
Cell E6
Risk Management Configuration

Cell 31 – Information Instantiation (Information Management)

The management of the information assets for an organisation is a part of the instantiated daily business. It is the ownership and distribution of information to stakeholders within and outside of the company. This management can also involve the archival or deletion of the information. The purpose is to achieve the organisation's vision, mission and philosophy through the effective use of the corporate information (Kirk 1999; Prajogo et al. 2018).

Information Management

Pictorial Model:



Artefact Example:
The Tasmanian Department of Health manages their patient information through a system which supports services to hospital staff, such as training in the hospital patient management applications and other computer applications, business queries and medical record forms design.
http://www.dhhs.tas.gov.au/hospital/mersey-community-hospital/departments/patient_information_management_services_pims

Compliance Mapping:
- ISO/IEC 27002:2013 Section 12
- NIST-SP-800-53 Rev 4 Section Configuration Management; System and Information Integrity;

Cell F1
Information Instantiation

Cell 32 – Security Mechanism Instantiation (Information Security)

At this level in the framework, information security is the day to day business of executing information security. The protection of the informational asset of the business in all its forms (Anderson 2001; Clinch 2009; Sherwood et al. 1995).

Information Security

Pictorial Model:

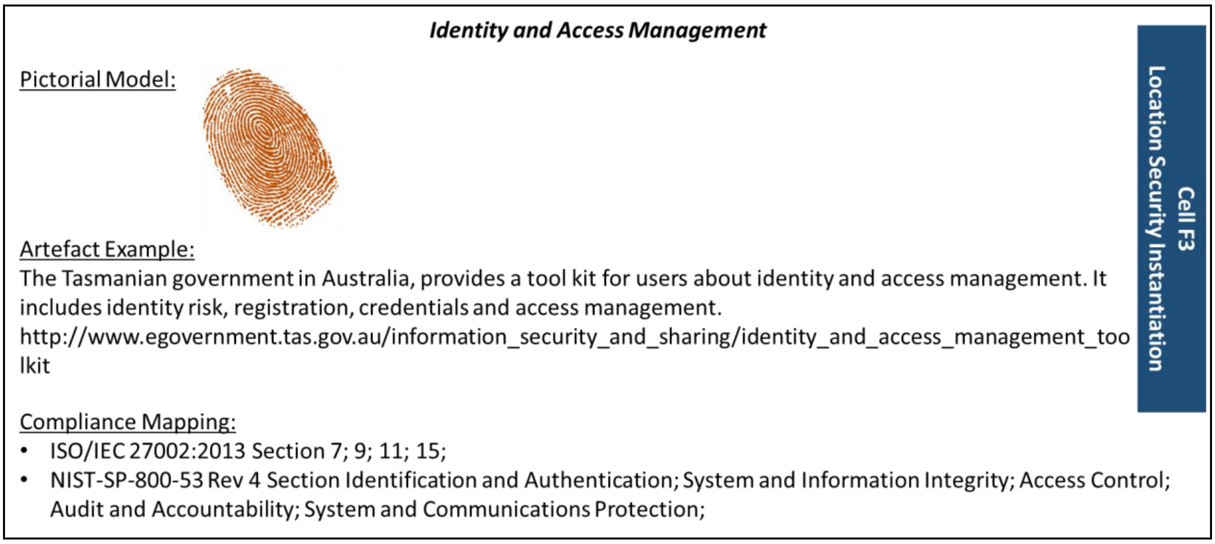
Artefact Example:
The Federal Reserve of the USA states that information security is the process by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its operations and provides guidance for relevant stakeholders to achieve this.
https://www.federalreserve.gov/bankinforeg/topics/info_security.htm

Compliance Mapping:
- ISO/IEC 27002:2013 Section 6; 9; 10; 12; 13;
- NIST-SP-800-53 Rev 4 Program Management;

Cell F2
Security Mechanism Instantiation

Cell 33 – Location Security Instantiation (Identity and Access Management)

The daily business of an organisation relies on the identification and authorisation of the correct people to access the organisation data and information and the repudiation of the nefarious attackers. Identity and access management is the system that keeps this process secure and can include tracking, auditing and management of users data (Adams and Sasse 1999; Haren 2011; ISO 2013).



Identity and Access Management

Pictorial Model:

Artefact Example:
The Tasmanian government in Australia, provides a tool kit for users about identity and access management. It includes identity risk, registration, credentials and access management.
http://www.egovernment.tas.gov.au/information_security_and_sharing/identity_and_access_management_toolkit

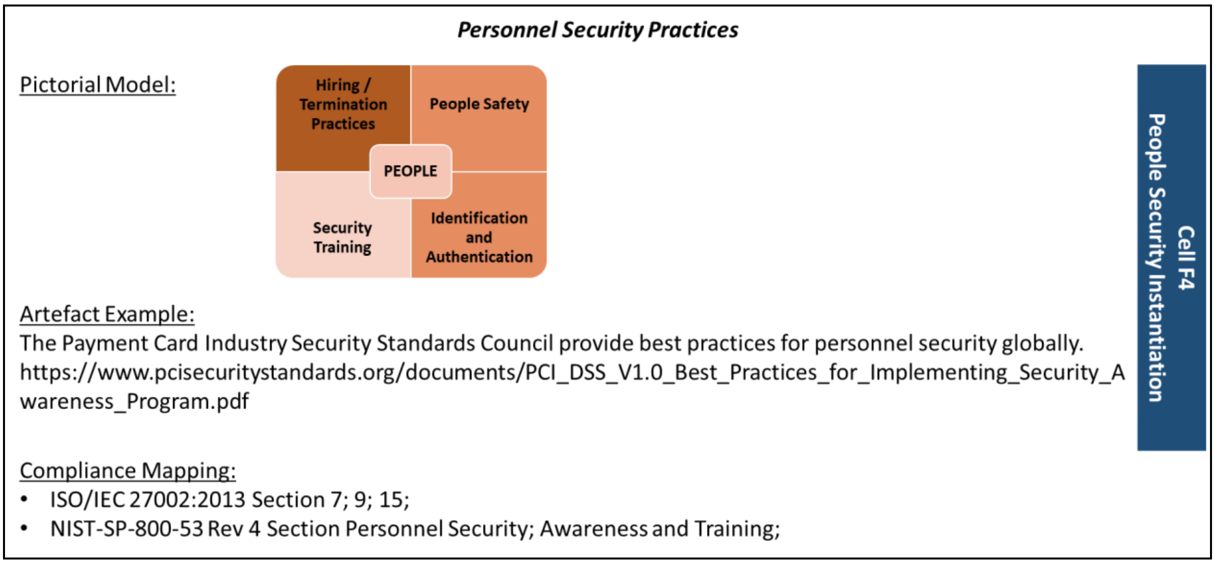
Compliance Mapping:

- ISO/IEC 27002:2013 Section 7; 9; 11; 15;
- NIST-SP-800-53 Rev 4 Section Identification and Authentication; System and Information Integrity; Access Control; Audit and Accountability; System and Communications Protection;

Cell F3
Location Security Instantiation

Cell 34 – People Security Instantiation (Personnel Security Practices)

Personnel security practices are the detailed daily business of the personnel security program. They are how the program is implemented in the organisation, also called the instantiation of the personnel security statement. The practices are not static but are planned, assessed and reviewed regularly to ensure effective personnel security (Clark et al. 2014; Korpela 2015; Panchenko et al. 2018).


Hiring / Termination Practices
People Safety
PEOPLE
Security Training
Identification and Authentication

Personnel Security Practices

Pictorial Model:

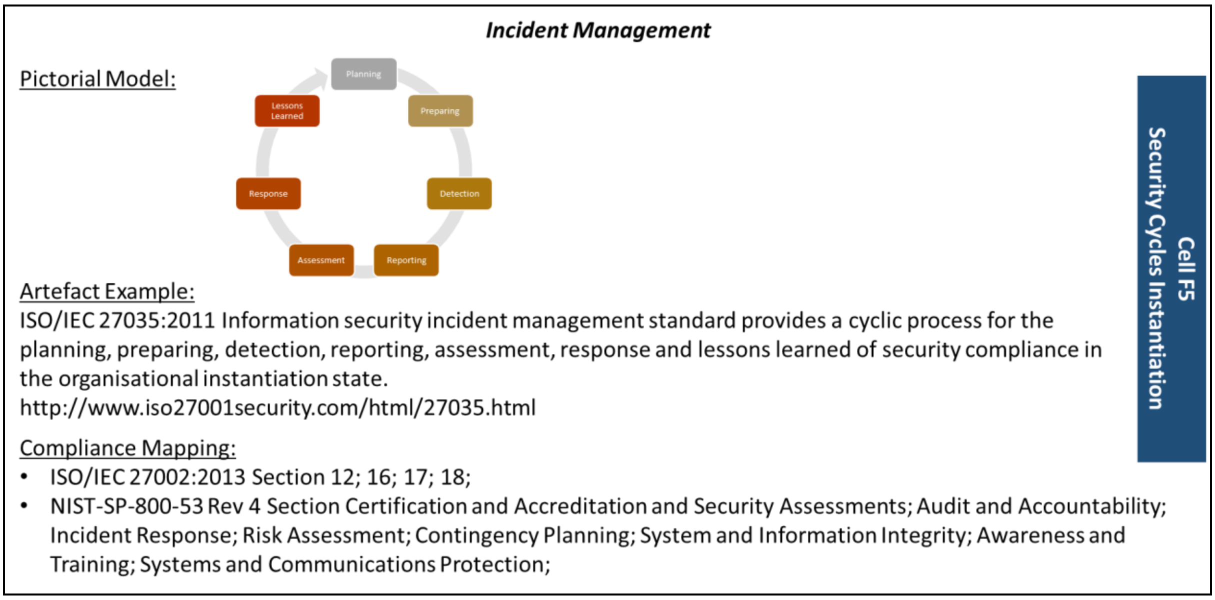
Cell F4
People Security Instantiation

Artefact Example:
The Payment Card Industry Security Standards Council provide best practices for personnel security globally. https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

Compliance Mapping:
- ISO/IEC 27002:2013 Section 7; 9; 15;
- NIST-SP-800-53 Rev 4 Section Personnel Security; Awareness and Training;

Cell 35 – Security Cycles Instantiation (Incident Management)

At an operational level, the daily business of security compliance is the continuous monitoring, audit events and investigations. The cycle of incident management begins with the planning and preparation for potential security incidents and ends with the response to the incident and lessons learned after the incident (Metzger et al. 2011; Shen et al. 2009; Tøndel et al. 2014).



Incident Management

Pictorial Model:

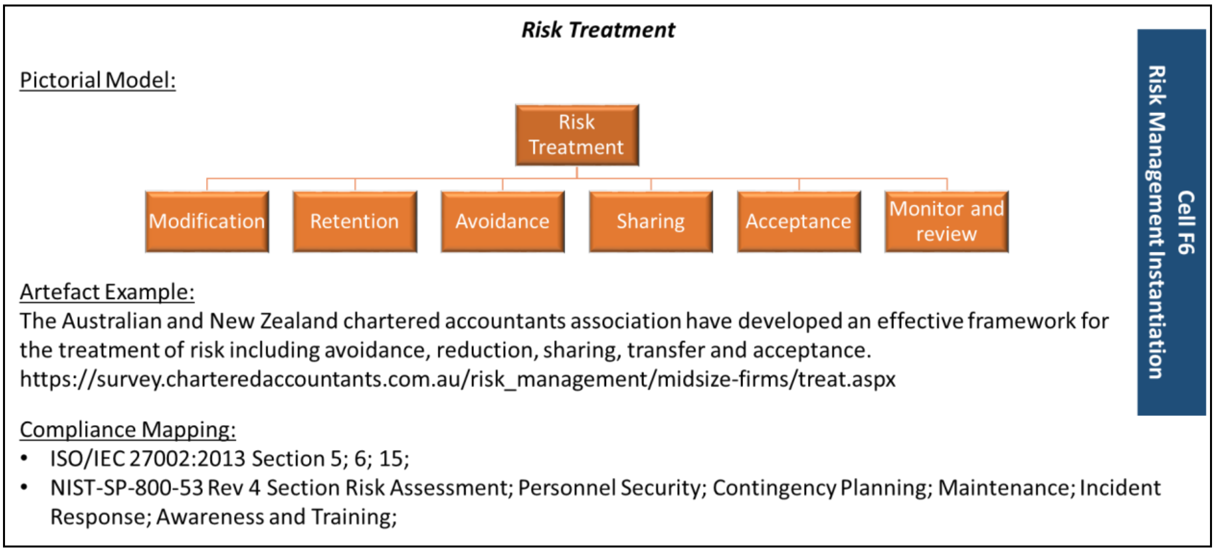
Cell F5
Security Cycles Instantiation

Artefact Example:
ISO/IEC 27035:2011 Information security incident management standard provides a cyclic process for the planning, preparing, detection, reporting, assessment, response and lessons learned of security compliance in the organisational instantiation state.
http://www.iso27001security.com/html/27035.html

Compliance Mapping:
- ISO/IEC 27002:2013 Section 12; 16; 17; 18;
- NIST-SP-800-53 Rev 4 Section Certification and Accreditation and Security Assessments; Audit and Accountability; Incident Response; Risk Assessment; Contingency Planning; System and Information Integrity; Awareness and Training; Systems and Communications Protection;

Cell 36 – Risk Management Instantiation (Risk Treatment)

Once risks are identified and a risk level has been allocated, a treatment should be applied. The treatment or mitigation of the risk is based on the impact the risk may have on the organisation and there are various choices. Most importantly it is ok to accept a risk and take no action – but this must be a decision that has been made, not a default. The time it takes to develop a treatment can be costly and time consuming, so it is important to begin with the highest-level risks and work down to the lowest level, balancing the costs with the resulting benefits (Hopkin 2018; Purdy 2010; Zio 2018).



Risk Treatment

Cell F6
Risk Management Instantiation

Pictorial Model:

Risk Treatment

Modification | Retention | Avoidance | Sharing | Acceptance | Monitor and review

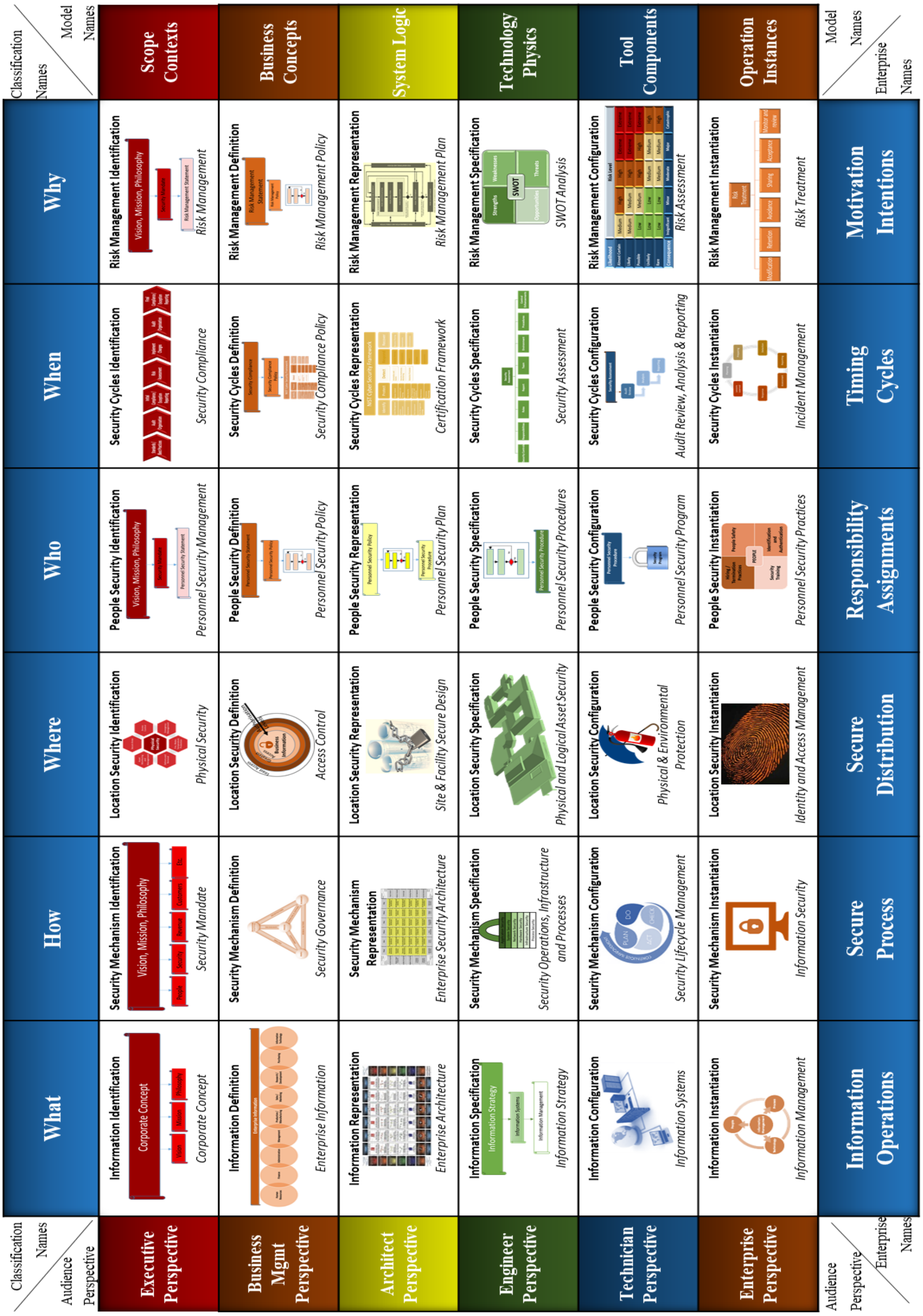
Artefact Example:
The Australian and New Zealand chartered accountants association have developed an effective framework for the treatment of risk including avoidance, reduction, sharing, transfer and acceptance.
https://survey.charteredaccountants.com.au/risk_management/midsize-firms/treat.aspx

Compliance Mapping:

- ISO/IEC 27002:2013 Section 5; 6; 15;
- NIST-SP-800-53 Rev 4 Section Risk Assessment; Personnel Security; Contingency Planning; Maintenance; Incident Response; Awareness and Training;

4.6 The Security Architecture Framework for Enterprises Artifact

In summary, the notional artifact was completed and three layers of abstraction developed. The primitive security models - row / column categories; the security instantiations of the primitive security models - detailed security definitions; and the ontological security cell definitions - pictorial model, artifact example and compliance mapping. The final framework is compliant with the five guiding design principles identified in Chapter 2 by the literature review and the framework survey. Figure 9 is the completed Security Architecture Framework for Enterprises (SAFE) artifact. The evaluation by expert industry participants of the SAFE artifact will be described in the next chapter.



Classification Names / Audience Perspective	What	How	Where	Who	When	Why	Classification Names / Model Names
Executive Perspective	Information Identification Corporate Concept	Security Mechanism Identification Security Mandate	Location Security Identification Physical Security	People Security Identification Personnel Security Management	Security Cycles Identification Security Compliance	Risk Management Identification Risk Management	Scope Contexts
Business Mgmt Perspective	Information Definition Enterprise Information	Security Mechanism Definition Security Governance	Location Security Definition Access Control	People Security Definition Personnel Security Policy	Security Cycles Definition Security Compliance Policy	Risk Management Definition Risk Management Policy	Business Concepts
Architect Perspective	Information Representation Enterprise Architecture	Security Mechanism Representation Enterprise Security Architecture	Location Security Representation Site & Facility Secure Design	People Security Representation Personnel Security Plan	Security Cycles Representation Certification Framework	Risk Management Representation Risk Management Plan	System Logic
Engineer Perspective	Information Specification Information Strategy	Security Mechanism Specification Security Operations, Infrastructure and Processes	Location Security Specification Physical and Logical Asset Security	People Security Specification Personnel Security Procedures	Security Cycles Specification Security Assessment	Risk Management Specification SWOT Analysis	Technology Physics
Technician Perspective	Information Configuration Information Systems	Security Mechanism Configuration Security Lifecycle Management	Location Security Configuration Physical & Environmental Protection	People Security Configuration Personnel Security Program	Security Cycles Configuration Audit Review, Analysis & Reporting	Risk Management Configuration Risk Assessment	Tool Components
Enterprise Perspective	Information Instantiation Information Management	Security Mechanism Instantiation Information Security	Location Security Instantiation Identity and Access Management	People Security Instantiation Personnel Security Practices	Security Cycles Instantiation Incident Management	Risk Management Instantiation Risk Treatment	Operation Instances
Audience Perspective / Enterprise Names	Information Operations	Secure Process	Secure Distribution	Responsibility Assignments	Timing Cycles	Motivation Intentions	Model Names / Enterprise Names

Figure 9: The Security Architecture Framework for Enterprises (SAFE) artifact

5 Evaluation

"It is not the strongest of the species that survive, not the most intelligent,

but the one most responsive to change."

Charles Darwin

The final artifact design to be tested with participants, as described in Chapter 4 and Figure 9, is the 36 cell Security Architecture Framework for Enterprises (SAFE), with the supporting documentation which included the cell definitions and purpose, the pictorial model, the real-world artifact example and the security standard compliance mapping. The evaluation employed, an Oppenheim structured expert evaluation survey, was created with questions designed to elicit indications from a group of participants about the artifact in terms of the efficacy – does the artifact produce the intended results, validity – is the artifact factually sound, utility – is the artifact fit for purpose, and quality – when compared to other similar security frameworks, is there a degree of excellence; and to confirm if the artifact design met the design principles explained in the Background and Literature Review. The responses were gathered and an inductive grounded theory qualitative analysis was completed to derive the foremost themes indicated by the participants. The survey, its design, the participants and the analysis process will all be discussed in this chapter.

5.1 Evaluation Survey Design

Within Design Science Research (DSR) studies, there are two types of evaluation actions which can be taken to evaluate an artifact. The first is artificial evaluation – creating a non-realistic situation in which to assess the artifact. Examples include laboratory experiments, simulations, mathematical proofs and theoretical arguments. The second is naturalistic evaluation – the testing of the artifact in a real-world environment such as an organisation or with experts from the field of research. Examples include action research, surveys, case studies and field experiments. For the purposes of the evaluation of the SAFE artifact, a naturalistic evaluation was chosen due to the emphasis and effectiveness of the research as a practical application in the real-world, the low risk to users and the increased quality of the knowledge outcomes from a naturalistic evaluation versus an artificial one. (Venable 2006; Venable et al. 2016) The naturalistic evaluation tool chosen was a participant survey of experts in the security and architecture field of research.

To gather the participant's inputs a survey / questionnaire was designed using an Oppenheim (1992) approach and following a successful rigorous ethical research approval process, distributed the survey. The Oppenheim approach was published in 1992 with further detail published in 2000 and 2017, and is purely dedicated to the design of questionnaires and surveys. It has now become a seminal work for the development of surveys (Rowley 2012), and other survey design research has drawn key principles from the original book (Fowler Jr 2013; Gillham 2008; Gray 2013). The 1992 Oppenheim text provides detailed advice including on the length, clarity, grammar and specificity of the questions and using these prescriptive methods, attempts to avoid such bias in questions as social desirability, double barrelled questions and negatively worded questions. It also provides detailed description on the survey planning, wording, measurement and actual statements. The Oppenheim design approach does this through detailed descriptions of the right and wrong way to phrase a question to a participant and gives example surveys in the Appendix. There are also workshops throughout the text for practice and learning. (Oppenheim 1992; Oppenheim 2000; Williams 2003) The type of responses gathered from an Oppenheim survey lend itself to provide effective inputs to the grounded theory qualitative analysis conducted in this research, described in Chapter 3, as grounded theory produces theories and thematic results that fit with the real-world based on grounded empirical data – the survey responses (Gregory 2011).

5.2 Evaluation Survey

Using the techniques described and the Oppenheim method, the survey was designed and developed to answer the research question detailed in Chapter 1, the design principles explained in Chapter 2 and the dimensions of efficacy, utility, validity and quality. As indicated in Table 12 and 13, the survey was made up of two sections. The first section was used to elicit demographic information about the participants, and the second section was for the evaluation of the artifact and its design. Each question was developed with specific goals in mind to satisfy the evaluation and are indicated in Table 12 and 13.

The survey is made up of five demographic questions - including security industry experience, job category, years of expertise; and 14 questions aimed at drawing out selected aspects of the initial research question and expert opinions of the design. Table 12 provides the demographic questions and the reason they were included in the survey.

Demographic Question	Purpose of Question
Q1. You work for • Industry • Academia • Government • Other… please state…	Background information on the participant's employment.
Q2. How large is the company you work for? • Small (1-19 employees) • Medium (20-199 employees) • Large (200+ employees)	The size of organisation they are employed could indicate the extent to which they have experienced or implemented security programs. The categories are based on the Australian Bureau of Statistics definition.
Q3. Which of the following best describes your role? • Manager • Security professional • IT professional • Other… please state…	Background information on the participant's position in their organisation.
Q4. How many years have you been in this role? • 0-2 years • 3-5 years • 6-10 years • 10+ years	Indicates the level of expertise in their current role.
Q5. Do you or have you ever worked in the security industry? • Yes… how many years? • No	Indicates the level of security industry expertise.

Table 12. Demographic survey questions and purpose

There were 14 questions in the second section of the survey intended to evaluate the artifact and its design. The questions were intended to provide overall thematic characterisations of the framework, address the principles for design and the four dimensions of validity, efficacy, utility and quality, and therefore provide indicative answers to the research question. Table 13 provides the 14 questions and the design principle(s) they are mapped to or the purpose for inclusion.

Artifact Survey Questions	Design Principle Mapping / Question Purpose
Q1. What is the biggest security challenge facing organisations today?	Background security question to help participants begin thinking about security in preparation for completing the survey.
Q2. Referencing the background information and the framework, please indicate if you believe any security categories or elements are missing and should be included?	Principle 1, Principle 2, Principle 3 and validity.
Q3. Do you believe a holistic approach to security is likely to provide a more secure organisation? Why or why not?	Principle1, Principle 5 and efficacy.
Q4. Do you believe a holistic approach to security is likely to help with financial decision making for security resources? Why or why not?	Principle 5
Q5. Does the use of a framework with all possible security categories included provide assurance to the process of securing an organisation? Why or why not?	Principle 2, Principle 3
Q6. After inputting an organisations security mechanisms into the framework, cell by cell, do you believe you could see the security gaps in an organisation and determine what else needs to be secured? Why or why not?	Principle 1, Principle 5, efficacy and utility.
Q7. Would the analysis from a completed security framework help senior management or the CEO make security decisions or provide beneficial management information? Please give an example.	Principle 1, Principle 4, Principle 5 and utility.
Q8. What do you see as the benefits or features of the framework for an organisation using it?	Anecdotal free text from participants to encourage additional response not brought out by previous questions and focused on the utility and quality of

	the artifact.
Q9. What are the problems or challenges of the framework for an organisation using it? Can they be solved?	Anecdotal free text from participants to encourage additional response not brought out by previous questions and focused on the challenges of the artifact.
Q10. This framework is compliant to NIST 800-53 and ISO27002 (international security industry standards). Does this information give you more confidence in the framework? Is the compliance important to you?	Principle 3, validity and quality.
Q11. Is the framework easy to understand and use? Why or why not?	Utility, quality and efficacy.
Q12. Does it help to have the security categories broken down into organisational levels (the row perspectives)? Why or why not?	Principle 2, Principle 4
Q13. Have you found the framework and the background information educational? Please give an example.	Anecdotal free text from participants to encourage additional response not brought out by previous questions and focused on education. Supports utility and validity.
Q14. Please provide any final thoughts on the theory, framework and supporting documentation?	Anecdotal free text from participants to encourage additional response not brought out by previous questions.

Table 13. Artifact survey questions and design principle mapping

5.3 Survey Participants

The artifact and supporting documentation was shared for critique to 4 four categories of professionals – manager, security professional, IT professional and researcher, 22 requests in total. The four categories were selected to represent the significant users of the artifact and those who would gain the greatest benefits if the artifact was successful. The initially identified cohorts and the perceived benefits (noting duplication is intentional) were:

- Manager – develop a security program, support decision making in security investment and resourcing, support prioritisation of activities, include privacy and human factors into security program, shared security language across organisation, organisational risk management and compliance, demonstration of due care and governance, secure supply chain, budgetary efficiency

- Security Professional – understand current security status, develop a security program, describe security requirements to stakeholders, demonstrate need for change or improvements in security posture, support prioritisation of activities, collaboration opportunities
- IT Professional – identify tools and technology to support security, develop technology profiles and roadmaps with security posture, collaboration opportunities, secure technology assets
- Researcher – develop academic understanding of enterprise security architecture, collaboration opportunities

Of the 22 requests six respondents indicated they did not have the expertise to provide an appropriate response and when probed further had little to no expertise in security, architecture or information technology despite working in technology organisations, and 4 of the professionals did not respond at all. Of the 12 respondents who became participants, 75% were employed by a large company (200+ employees), 17% were from a small (1-19 employees) and 8% from a medium (20-199 employees). 42 % had security industry experience and 75% had been in their current role for more than 10 years and considered themselves experts in the field. The participants came from Industry (58%), Government (33%) or the Military (8%).

The participants were asked to review the framework and supporting documentation in the context of their own organisations and their expertise, carefully considering the utility of the design and its application in a working environment and compared to their current security situation. To test the utility, the participants worked through each cell and determined if their organisation has a suitable security instance of the requirements indicated for that cell, using the provided explanatory notes. Just as an EA framework can build an organisation from its inception, so the security dimension created should functionally be able to build security into all aspects of the organisation. Theoretically a form of an organisational security ontology.

5.4 Evaluation Survey Results Analysis

The survey responses were collated from the participants and the grounded theory method, described in Chapter 3, was used to draw out themes through an inductive data collection, analyse the results from the questionnaire about the framework, and enable the participants to tell the story. The grounded theory is a methodology by which qualitative analysis is iterative – the data (meaningful concepts, in this case the survey responses) are collected and each data unit is assigned codes. The codes are inspected for patterns and then reintegrated to form dominant thematic subjects and connections. (Starks and Brown Trinidad 2007; Strauss and Corbin 1994)Through the cyclical nature of the grounded theory methodology, each coding phase provides richer thematic results.

To explain the process - an example question from the survey: "Have you found the framework and background information educational?" The first coding phase saw 13 participant responses:

- Shows the full extent of issues involved in security - difficulties and complexity
- Would be good for implementing a new security program
- Definitions, an example and references are a very strong tool
- Provoked how to better inform the risk appetites of lower level capabilities
- Definitions and context provide scope but introduce flexibility in interpretation
- Seeing all the elements together shows how broad security really is
- Underpinned by standards shows a framework that can be usable
- Very educational - pictorial models, artifact examples
- Seeing it a such a high level demonstrates how hard it would be to coordinate
- Would be an enhancement across the whole security spectrum
- Saw security policies and practices can be used to form a cohesive framework
- Introduced new aspects of security for me at the executive and business levels
- A reminder of how complex security is

To get to the second phase, the first phase raw responses are reviewed and responses that are the same or have similar intent are combined, retaining the intent behind the theme. This reduces the number of responses, and distils the information thematically. The first coding process took a list of 13 responses to a total of eight response themes.

- Definitions, an example and references are a very strong tool
- Shows the full extent of issues involved in security - difficulties and complexity
- Saw security policies and practices can be used to form a cohesive framework
- Would be good for implementing a new security program
- Provoked how to better inform the risk appetites of lower level capabilities
- Very educational - pictorial models, artifact examples
- Would be an enhancement across the whole security spectrum
- Introduced new aspects of security for me at the executive and business levels

The process or coding is done a second time, creating a third list of six response themes.

- Definitions, artifacts, models and references are a very strong tool
- Shows the full extent of issues involved in security - difficulties and complexity
- Saw security policies and practices can be used to form a cohesive framework
- Would be good for implementing a new security program
- Provoked how to better inform the risk appetites of lower level capabilities
- Introduced new aspects of security for me at the executive and business levels

And finally, after the last iteration of distilling commonalities, the list of three dominant themes emerges from the original 13 responses.

- Definitions, artifacts, models and references are a very strong tool
- Shows the full extent of issues involved in security - risk, difficulties and complexity
- Security policies and practices can be used to form a cohesive framework / security program

Table 14 demonstrates the final thematic results for all of the questions in Section 2 of the survey using the grounded theory methodology.

Artifact Survey Questions	Grounded Theory Thematic Results
Q1. What is the biggest security challenge facing organisations today?	• Lack of risk management • Constrained cost environment

	• Protection of ICT assets • Qualified and experienced security staff • Complete employee engagement • Company branding damage
Q2. Referencing the background information and the framework, please indicate if you believe any security categories or elements are missing and should be included?	• No new elements were identified
Q3. Do you believe a holistic approach to security is likely to provide a more secure organisation? Why or why not?	• Security is properly engaged across the business reducing risk of gaps • Organises the complete security function • Provides security education to new organisations • Provides a roadmap for decision makers towards security assurance including resources
Q4. Do you believe a holistic approach to security is likely to help with financial decision making for security resources? Why or why not?	• Base financial decisions on security risk levels – highest risk gets attention it needs • Provide a basis for future security cost prediction and planning • Should include effects and costs of not doing each cell to highlight seriousness • Educate staff that all cells are not equal in terms of costs – the use of cells may indicate equality
Q5. Does the use of a framework with all possible security categories included provide assurance to the process of securing an organisation? Why or why not?	• Yes – ensures all aspects of security are covered and assessed • Yes – allows for changes in the environment and emerging threats • Yes – teaches about security and guides the users • Yes – allows activities to be tracked, measured and monitored • No – complex and difficult to understand so will not feel assured
Q6. After inputting an organisations security mechanisms into the frame-	• Yes – needs to address implementation and risk mitigation

work, cell by cell, do you believe you could see the security gaps in an organisation and determine what else needs to be secured? Why or why not?	• Yes – forces organisations to include security elements not traditionally addressed • Yes – provides good governance for security • Yes but would take a lot of resources to complete accurately.
Q7. Would the analysis from a completed security framework help senior management or the CEO make security decisions or provide beneficial management information? Please give an example.	• Yes – provide understanding of the gaps in security, the risks and remediation • Yes – because it tiles the problems and solutions with the business value in the top row • Yes - demonstrates the interconnected and broad nature of security in a single nomenclature • Yes – aids cost efficiencies
Q8. What do you see as the benefits or features of the framework for an organisation using it?	• Provides an as-is and a to-be so can create a plan for gap • Holistic comprehensive analysis of security – high level and detailed cell views • Roles and skill requirements are easy to define for each cell • Fits within the Enterprise Architecture of the organisation • Easier to assign accountability for security • Better communication about security between all levels of the organisation • Could provide profit and existential benefits
Q9. What are the problems or challenges of the framework for an organisation using it? Can they be solved?	• Will initially require specialist resourcing or project team • Executive buy-in and support is key • Could be used as a check box instead of doing the thoughtful analysis • Quite complex • Human bias and resistance to change may be a problem
Q10. This framework is compliant to NIST 800-53 and ISO27002 (interna-	• Yes – validates framework in terms of academic rigour • Yes – model based on best practice for company com-

tional security industry standards). Does this information give you more confidence in the framework? Is the compliance important to you?	pliance • Yes – management more likely to accept • No – risk based security is better than compliance based
Q11. Is the framework easy to understand and use? Why or why not?	• Yes – may require education for non-security people • It is complex but intuitive, logical and easy to use • The examples help clarify what artifacts may look like and what to include • Yes – based on known and users best practice • Testing the framework within an organisation would help
Q12. Does it help to have the security categories broken down into organisational levels (the row perspectives)? Why or why not?	• The large number of boxes diminishes the simplicity of the approach • Helps to articulate each level's security mechanisms, their responsibilities and considerations • The structural configuration shows that security is a whole of organisation responsibility not just ICT • Helps build trust because the right information is comprehensive and usable to the right audience
Q13. Have you found the framework and the background information educational? Please give an example.	• Definitions, artifacts, models and references make it a very strong tool • Show the full extent of issues involved in security – risk, difficulties and complexity • Security policies and practices can be used to form a cohesive framework / security program
Q14. Please provide any final thoughts on the theory, framework and supporting documentation?	• Include a simplified high level view, no pictures, 4-5 words • The framework is scalable and adaptable to any organisation • It is well researched, written and presented • Implementation would need to be centrally managed and championed by executive • Move the why (risk) column to after the what column to emphasise risk to executives

	• Requires the practical implementation toolset such as a gap assessment workbook • This nomenclature holistically applied could be a key to success • Fantastic concept that provides a single awareness view for all about security • Could easily continue on and become a commercial product or products • A single framework that could be implemented and is industry standard compliant • Nice to see a table explaining how departments fit in where and what responsibilities • The artifact examples are extremely useful and the first thing to look for

Table 14. Thematic results per survey question from Grounded Theory analysis

5.5 Summary

In summary the artifact was evaluated by 12 expert participants using an Oppenheim survey. The results were analysed using the qualitative analysis tool, grounded theory method, and the results and anecdotal evidence supports the design and the artifact. Comments from the participants include “definitions, artifacts, models and references are a very strong tool”, “could easily continue on and become a commercial product” and “fantastic concept that provides a single awareness view for all security”. The next chapter will provide a discussion of the results generated from the evaluation of the survey including impact on design principles, new design knowledge gained from the research, and both theoretical and practical significance of the research.

6 Discussion

"Learn something new. Try something different. Convince yourself that you have no limits."

Brian Tracy

The research gap discussed in the Introduction highlighted the critical need for a new way to define security within organisations given the high number of breaches still occurring daily. Approaching security, instance by instance, within an organisation can create confusion, gaps and duplication of resources. There is a significant opportunity for a reduction of security breaches, increased economic security and cyber resilience in organisations through a holistic approach to an organisational security framework with methodological supporting documentation, the importance and benefits of which have been mentioned in research (Anderson 2008; Moulton and Coles 2003). This research developed a novel, fully researched enterprise security architecture (ESA) framework for organisations. The framework, analysed by industry professionals, determines that a holistic security model can provide the much needed solution to the identified organisational security gaps and provide security benefits. The framework, the Security Architecture Framework for Enterprises (SAFE), is a comprehensive security solution based on the enterprise architecture methodology and, through the research contribution, addresses the gap and the research question by providing security benefits to an organisation more effectively than a piecemeal approach.

The research reviewed cohesive security frameworks or models available for organisations to use. The security framework literature review that was conducted, highlighted that a complete solution, addressing this gap was not currently available and as security has never been more important in this interconnected society, this significant gap was therefore worth pursuing. Through the review, this work discovered that the most effective and holistic construct for an organisational framework was enterprise architecture but found that, although previous iterations of security frameworks using enterprise architecture had been attempted, there was no fully researched instance to test the theory of a holistic model and provide security benefits to an organisation more effectively than a piecemeal approach. Using Design Science Research, this research tested a design to address this gap and created an artifact for evaluation by experts. The outcome of the evaluation, described in the previous chapter, was that the design does address the gap effectively and the holistic artifact could be used by organisations to improve their security profile more effectively than piecemeal approach.

6.1 Thematic Interpretation of Results

The purpose of the artifact was to test the design and design principles developed in support of the research question. The analysis of the expert evaluation responses provided insight as to the effectiveness of the design.

The most common theme in the responses is the importance and utility of the holistic nature of the framework – demonstrating the interconnected and broad nature of security in a single nomenclature. Of note was the ability of the framework to reduce the risk of security gaps, the categorisation of the complete security function, the uses including security governance, security program, best practice and a security nomenclature. Both the compliance to international standards and the holistic nature provide an assurance for company security certification. Comments by the participants include "compliance to NIST and ISO validates the framework in terms of academic rigour", "ensures all aspects of security are covered and assessed", "organises the complete security function" and "focuses organisations to include security elements not traditionally addressed".

From a financial decision making perspective, the framework is said to provide a combination of a risk-based approach and ensures the highest security risks will get the highest priority spend. Comments by the participants include "provides a bases for future security cost prediction and planning" and "could provide profit and existential benefits".

Improved organisational communication in security is a theme that is cited as a significant benefit of the framework. Other benefits include defining who is accountable for security functions and the roles and skills of the security team defined which will provide better communication between all levels of the organisation, ensuring all aspects of security are covered and assessed. It is acknowledged several times that setting up this kind of model in an organisation will require significant resourcing, including a project team, but once implemented and functioning it can be maintained. Comments by the participants include "provides better communication about security between all levels of the organisation", "provide an understanding of the gaps in security, the risks and remediation" and "provides good governance for security".

An educational theme for the framework is highlighted, that it will provide a security education for organisations. Security is a complex and difficult subject and the risks involved are high therefore using the framework can show the full extent of issues involved in security, something not easily known without a holistic tool. The framework is identified as a very strong educational tool based on the provided definitions, frameworks, models and references. Comments by the participants include "helps build trust because the right information is comprehensive and usable to the right audience", "security policies and practices can be used for a cohesive framework and security program" and "the structural configuration shows that security is a whole of organisation responsibility not just IT".

A challenge of the framework is complexity. This is raised more than five times and through deeper analysis it is noted that the participants most challenged by the complexity of security do not have strong security experience. Comments from participants include "quite complex", "the large number of boxes diminishes the simplicity of the approach", "it is complex but is intuitive, logical and easy to use" and "scalable and adaptable to any organisation".

Other comments worthy of noting for the future evolution of the framework include the need for a practical implementation toolset such as a gap assessment workbook / a user manual, and testing the framework within an organisation.

6.2 Results For Design Principles

As first described in the Background and Literature Review chapter, the following five design principles were developed, after an analysis of 27 security frameworks, to guide the design of the artifact. Each principle, as described in the Evaluation chapter, was then aligned to specific survey questions given to the participants, to test the artifact's application and efficacy to the principles and the research question. The following discussion describes the participant results to the questions related to the Principles. Table 13 provides the direct mapping of the principles to the survey questions. The outcome shows an effective implementation of the Principles in guiding the design of the framework and the responses indicate that such an artifact would provide significant organisational security benefits more effectively than a piecemeal approach which successfully answers the research question.

Principle 1 – Security mechanisms for all organisational assets

Survey questions two, three, six and seven were designed to test the principle that all organisational assets should be assessed for security mechanisms, noting that all security is risk based and therefore the answer can be that the organisation chooses not to secure the asset and accepts the risk, but the key is that all assets – people, process, technology and information, should be considered in the securing of an organisation. The participants indicated in question two that the artifact was very comprehensive and there were no organisational assets missing from the artifact grid. To support this notion, the third question asked if a holistic approach – all assets, all departments, is likely to provide a more secure organisation. The responses were 100% in agreement with this question. One participant expanded further and explained how often media describes the extent an organisation will spend time and money on securing one part of an organisation, such as ICT, and the successful attack is in an area that was treated as less important or received less focus, such as physical security. The best security can be applied to a computer but if the attacker can simply walk away with the computer, then the organisational security has failed.

Questions six and seven focused on the potential gap analysis that is required to ensure all assets are secured and the executive buy-in that is required to make those security decisions. Participants highlighted that the ontological nature of the grid – a list of security terms and the relationships between them, gives an organisation a complete list to work through to conduct the gap analysis and then bring the needs or risk choices to the executive to make a decision. The framework also demonstrates the interconnected system of security and the subsequent consequences of softening one aspect. It was also highlighted that the framework would provide an assurance to management that the recommendations they bring are based on a methodology.

Principle 2 – Ontological phrases are used

Survey questions two, five and 12 were designed to test the principle of ontological security phrases rather than instances of a security mechanism. The ontological design principle provides flexibility to the users that the requirement for instances would not. For example if an organisation is required to have a specified type of physical security such as a retina scanner for biometric screening of visitors to the building but the organisation is only 10 people, it is unlikely that the organisation could afford or actually need such a large scale form of physical security. The use of the ontological phrase for physical security such as "identity and access management" from the artifact, emphasises to the organisation that physical security is required to be considered but the instance type is not mandated, allowing all organisation types, sizes and budgets to use the artifact. The responses from the participants indicated the categories allowed their subject matter experts, like physical security, to determine the best implementation for their organisation. It was also highlighted that the ontological phrases not being prescriptive allowed for flexibility and change when the organisational environment changed, such as growth or structure, or new threats emerged in the security environment. One participant mentioned that the categories were encouraging to their small organisation and that they felt they were more likely to achieve a level of security assurance because categories were achievable but previous prescriptive instance-based frameworks they had tried to implement had been too costly, difficult and as a small organisation they did not have the expertise, leaving the organisation exposed to significant security risk.

Principle 3 – Compliance to security industry standard

Survey questions two, five and 10 were designed to test the principle that it is important for the artifact to be in compliance with at least one security industry standard. In the literature review it was determined that the two most commonly used standards for security were ISO/IEC 27002 and NIST 800-53. The artifact was therefore designed to be in compliance with both of these standards and the survey questions were designed to understand the importance of compliance and assurance to organisations. Participants highlighted the two standards as best practice and therefore the framework, by association, would also be perceived as best practice and the use of a framework that was in compliance would aid in security audits as most audits now require compliance to pass. It was also noted that there is a level of credibility associated with standards, that it builds more confidence in the benefits and provenance of the framework, and this would lend a credibility to security programs and also to conversations with executive about security.

Principle 4 – Use of an enterprise architecture reference

Survey questions four, seven, eight and 12 were designed to test the principle that the use of enterprise architecture as the primary model for the foundation of the framework is an effective choice. Enterprise architecture was chosen for two key reasons. The first is that EA was the most commonly used model for security frameworks when the review of 27 frameworks was done. Secondly EA adheres to and supports Principle 1 and Principle 5 directly and indirectly supports Principle 2 and 3 because EA is a model to build a complete organisation. In the same way, the research question and design principles were intended to develop a whole organisational security framework, not just for a department or a specific type of security.

The responses from participants discussed the importance of articulation of security mechanisms, including responsibilities for all levels of the organisation, the use of the architectural categories would provide the right information to the best people to understand it, and the rows and columns break up the complexity of security into identifiable chunks. The use of EA was also mentioned as helpful because large numbers of organisations are turning to EA to define the best use of their resources and having a security framework based on EA will complement, align and implement the organisations business models more effectively. Another response noted the use of a multi-faceted model like EA, aids understanding that security is also multi-faceted and that each department has something to contribute in the decision making and execution of security – fundamentally security is a whole-of-organisation responsibility.

Principle 5 – Coverage is organisationally holistic

Survey questions three, four, six and seven were designed to test the principle that security should be considered in all departments of an organisation and not just individual departments like ICT and that all security in an organisation should be cohesively considered and managed not as separate departmental responsibilities or instances. The most frequent response to these survey questions was about the framework helping the organisations understand the other parts of the organisation that need security. By taking a holistic view, there was an educational factor involved, and security would be considered and implemented in areas that had not previously been considered, effectively closing security gaps and minimising risk. Mapping all of an organisations security in the single model provides a view of security that had not previously been available and changes the perspective of security in an organisation from the singular departmental focus to an organisationally holistic security eco-system with highly interdependent primitive security models. Within the eco-system concept, the framework also provides a depiction of the essential relationships between the cells for business security modelling. The consequences highlighted the contributions and future work made possible by the framework with respondents mentioning better security coverage, strong gap analysis and therefore remediation, departmental responsibility definition and considered security decision making in understanding the organisation's risk exposure. A holistic view of an organisation's security is a balanced view of security and directly drives resource discussions where ICT or physical security is usually the focus.

6.3 New Design Knowledge

Within DSR, there are eight components of a design that are used to describe the design knowledge that was gained during research in the design process and the resulting artifact (Gregor and Jones 2007). The purpose of this component structure is to "specify design theory so that it can be communicated, justified and developed cumulatively" (Gregor and Jones 2007).

Table 15 uses this schema to communicate the summary of the new design knowledge contributions within this research, evaluated through the artifact - the security architecture framework for enterprises.

Component Type	SAFE Component Concepts
Purpose and scope	The research question for this work is to determine if a holistic security model, using enterprise architecture, provides security benefits to an organisation more effectively than a piecemeal approach. The model or framework is for evaluation by industry experts to consider in terms of their own organisations and expertise. The framework is applicable to organisation of all sizes, budget and staffing levels. Principles of utility and design were considered.
Constructs	Incremental development using the evaluative responses. Compliance to industry security standards. Organisational security cohesion. Security benefits such as education, responsibility allocation and financial decision guidance.
Principles of form and function	A security architecture framework that includes all perspectives of an organisation - scope, business, system, technology, tools and operations. An organisational security ontology.
Artifact mutability	To aid complexity a practical implementation toolset such as gap assessment workbook or user manual.
Testable propositions	Further testing of the design in using a longitudinal study to assess the changes in security.
Justificatory knowledge	The kernel theory was enterprise architecture.
Principles of implementation	An architect would use all 36 cells of the framework as a guide to describe the security profile of the organisation. For each cell the organisation would decide if an instance of the cell exists or if not, are they willing to accept the risk of not having it and will it be mitigated. For use by organisations with and without Zachman implementations.
Expository instantiation	The instantiation of the design is the security architecture framework for enterprises artifact.

Table 15. Components of a design theory for the artifact (Gregor and Jones 2007)

Theoretical Significance

The kernel knowledge for this research was the domain of enterprise architecture. As described in the Background and Literature Review chapter, EA is an established, comprehensive body of knowledge and models that are used to describe an organisation and its assets. Until this research and design study was conducted, security within EA had not been considered with the same depth as EA. There were other frameworks that used some of the principles of EA to describe security but none that strictly adhered to EA and all of its principles, and then used a fully researched process to create an artifact. This increased the novelty of the research and the outcome in both the artifact, the design and the evaluation, all indicate success to the extension of the kernel theory. There now exists a true enterprise security architecture framework and design principles to guide future users and researchers.

Similarly, the security domain is also well established, however, there are very few models that address all forms of security within an organisation in a structured format that is fully compliant with industry standards. The collection of the security categories as a framework is also a form of ontology or categorisation system for organisational security. This research has extended the security domain body of knowledge by creating a design that provides both an ontology and a model for all organisations regardless of their size, budget or resources. The use of the framework as an ontology provides shareable and reusable knowledge across the security domain or an organisation using the framework, and, as Zachman recommends, describe the relationships and connections between the cells, or the organisational security instances, which can be used for business modelling. This form of business security modelling has not been available before and changes the perspective of security in an organisation from the piecemeal approach to a holistic security eco-system with highly interdependent primitive security models.

Practical Significance

The evaluation indicates that all participants believe their practice of security within their organisations would be significantly improved if such a design were available. As described in the evaluation by the expert participants, the opportunities to improve organisational security using the design and artifact include management, financial resourcing, security education, compliance obligations and audit, risk management and security awareness and confidence. Within the practice of securing organisations, which the artifact was designed to address, the implications to practice indicate the gap has been bridged through convincing evidence. Respondents from the survey agree, "security is intrinsically linked and best practice should be holistic", "the holistic approach provides a recognition by Boards and Executive Management that security is a business risk, not a technical risk", "shows the full extent of security issues", "a holistic approach will be very powerful in any organisation", "demonstrates the interconnected nature of security in a single nomenclature" and "it ties the problems and solutions with the business value".

6.4 Summary

Through the evaluation of the artifact by expert respondents, we learned that the artifact and its design directly addresses the research question "Will a holistic security model, using EA, provide security benefits to an organisation more effectively than a piecemeal approach?" The contributions of this research include providing a clear link between a holistic security approach and the organisational security benefits by developing and testing a framework that addresses these concerns. The research also demonstrates the interconnected nature of security in a single nomenclature, supports financial decision making, provides educational benefits, demonstrates assurance to organisational compliance, improved communication within organisations, and provides an organisation's structural configuration for better understanding. The five guiding design principles, when used effectively in a framework implementation do address the research question and gap. And finally this research changes the way we fundamentally view security in an organisation, from individual silo capabilities to a holistic security eco-system with highly interdependent primitive security models.

The conclusions discussed in the next chapter will summarise the thesis, confirm the findings and that the research gap has been bridged; and provide a recommended way forward for the research domain and future works.

7 Conclusions

"Devote yourself to an idea. Go make it happen. Struggle on it. Overcome your fears.

Smile. Don't forget: this is your dream."

Rishaabh Kumar

Security has never been more important to our connected world and to organisations, with the number of security breaches increasing every year and the high profile discussions of security issues in the media. A new approach to organisational security is a priority. In security, the whole is clearly greater than the sum of its parts and security maturity is not just technical but involves consideration of all parts of the organisation in a holistic manner. The benefits of a holistic approach require all aspects of security to be considered and risk managed based on the budget, size and mechanisms of the organisation, and provides a reduction in responsibility confusion and appropriate resourcing, would reduce security breaches and improve security factors in organisations. This research has designed a new holistic model for organisations to address security and the evaluation results indicate the research gap and practical organisational need have been achieved.

The research conducted a semi-systematic literature review of 27 organisational security structures to determine if a fully researched and holistic security methodology was available. The survey analysis showed that current security models lack research process and therefore lack case study analysis, replicability and research exploration. This was identified by a careful examination and review of the 27 security structures, their supporting documentation and the methodologies used. The result is very few structures met the holistic test and the most common construct to address an organisation holistically was Enterprise Architecture (EA). Furthermore, one of the important findings in the survey was the ontology gap. EA uses an ontology to describe the organisational classifications, simplifying structures for use. Organisational security does not currently have this classification structure. The development of an Enterprise Security Architecture (ESA) ontology is the first of its kind and provides an ESA language to articulate security in all its forms throughout an organisation. The structure can be used for compliance and assurance purposes, providing management with a tangible solution to the fiduciary and moral responsibilities of organisational security. The need for further research was highlighted.

Our analysis identified the similarities and differences amongst the frameworks and proposed a set of design principles to guide the development of a security artifact. The design principles for the artifact were: 1) the securing of all assets, 2) the use of ontological phrases, 3) compliance to international security standards, 4) the use of EA as the reference model and 5) organisationally holistic in its implementation. The principles respect the key aspects of the two domains of security and enterprise architecture and provided a first step towards effectively combining them for the new artifact. The resulting research question was therefore:

Will a holistic security model, using Enterprise Architecture, provide security benefits to an organisation more effectively than a piecemeal approach?

The design of a holistic enterprise security architecture highlights that security is not just technical but requires a focusing on all the organisational assets of people, technology, processes and information, which provides enterprise security management guidance to contemporary digitalised organisations of the 21st Century.

This research used the Design Science Research methodology due to the need for a designed and evaluated artifact. The qualitative analysis of an Oppenheim questionnaire given to expert evaluators to provide feedback for the artifact, was completed using the Grounded Theory Method, and the approach of the research was constructivist and inductive.

The designed and fully researched artifact produced in this work is the Security Architecture Framework for Enterprises (SAFE) (Figure 9) and is based on the Zachman 2013 Version 3.0 EA construct which allows for the artifact to be used in conjunction with the Zachman EA or as a stand-alone organisational security model. SAFE is compliant with the five guiding design principles identified in the initial literature review and has been completed to three layers of abstraction including; the primitive security models - row / column categories; the security instantiations of the primitive security models - detailed security definitions; and the ontological security cell definitions - pictorial model, artifact example and compliance mapping. The completed artifact is a 6 x 6 framework and each cell was defined using 1) a detailed explanation, 2) pictorial model, 3) artifact example in the real world and 4) compliance mapping to ISO 27002 and NIST 800-53.

To determine the effectiveness of the framework in meeting security concerns and test the efficacy within real-world organisational environments, the framework and supporting documentation is shared with industry professionals together with a questionnaire for evaluation and asked them to consider the artifact in the context of their own organisations and expertise. The questionnaire was made up of five demographic questions about the participants and 14 questions about the artifact. The participants were made up of managers, security professionals, IT professionals and researchers. The questions about the artifact were mapped to the five design principles and the research question, and were designed to elicit meaningful responses to further guide the development and usability of the design and the artifact. The responses were analysed using the qualitative analysis methodology, Grounded Theory.

The analysis of the questionnaire responses evaluating the security artifact, SAFE, indicates that the research gap has been bridged and that a holistic approach to organisational security, using EA, can provide security benefits more effectively than a piecemeal approach. The evaluation highlighted the usability of a holistic structure which demonstrates to the organisation, the interconnectedness and broad nature of security. Other benefits included reduction of security gaps, a categorisation framework for the entire security function, security governance structure, improved security program, compliance to best practice and a security nomenclature. Other opportunities include better financial decision making for the security function, improved organisational communication regarding security, and a strong educational tool for the organisation with the use of the provided definitions, framework, models and references. One challenge to non-security practitioners was the complexity of the artifact and a recommendation for a future improvement of the framework was a gap assessment workbook or user manual.

The theoretical significance of this research is the successful extension of the kernel theory, enterprise architecture, with a fully researched enterprise security architecture including all definitions and the five design principles successfully implemented. The security domain has benefited by the development of the first security categorisation system for organisations or an organisational security ontology.

To mature the concept further there would be benefit from future work to explore further the ideas discussed in this research. The first recommendation would be a larger design study – the analysis of a larger study could provide a larger sample size of the input data to provide detailed focus areas for additional research and further application to business units. Secondly a user guide or manual was identified in this research as being particularly important to non-security professionals, the creation and inclusion of one would therefore extend the usability of the framework beyond experts to a much wider audience, improving security architectures more broadly. A case study in an organisation would test the efficacy of the framework and provide practical nuances and adjustments to the work that research cannot. Finally an organisational implementation study would take the case study concept further and provide longitudinal data as the organisation implemented and changed through the use of the framework. In both the organisational case study and implementation study, it would be useful to work with multiple organisations and therefore capture data from varying types of organisations to test the applicability of the framework despite the relevant industry or sector.

This work is important because organisational security has never been more necessary and the successful design and development of a security framework artifact that looks at all of the aspects of security throughout an organisation is an important step forward to achieve a comprehensive solution to a complex and challenging problem for our digital society. This research changes the way we fundamentally view security in an organisation, from individual silo capabilities to a holistic security eco-system with highly interdependent primitive security models. The success of this important security research provides an opportunity and a significant foundation for future ESA studies.

8 References

"If I have seen further it is by standing on the shoulders of giants."

Isaac Newton

2014. "The Standard of Good Practice for Information Security." Information Security Forum.

Abdallah, S., and Galal-Edeen, G. H. 2006. "Towards a Framework for Enterprise Architecture Frameworks Comparison and Selection," *INFOS 2006*.

Acuña, D. 2016. "Enterprise Computer Security: A Literature Review," *Journal of the Midwest Association for Information Systems| Vol* (2016:1), p. 37.

Adams, A., and Sasse, M. A. 1999. "Users Are Not the Enemy," *Communications of the ACM* (42:12), pp. 40-46.

Agarwal, R., Thakur, V., and Chauhan, R. 2017. "Enterprise Architecture for E-Government," *Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance*, pp. 47-55.

Akman, M. K. 2019. "Swot Analysis and Security Management," *European Journal of Management and Marketing Studies*).

Anderson, E., and Choobineh, J. 2008. "Enterprise Information Security Strategies," *Computers & Security* (27:1), pp. 22-29.

Anderson, J. A., and Rachamadugu, V. 2008. "Managing Security and Privacy Integration across Enterprise Business Process and Infrastructure," *IEEE SCC*: IEEE, pp. 351-358.

Anderson, R. 2001. "Why Information Security Is Hard-an Economic Perspective," in: *Proceedings 17th Annual Computer Security Applications Conference pp. 358-365*. IEEE, pp. 358-365.

Anderson, R. 2008. *Security Engineering*. John Wiley & Sons.

Angelo, S. 2001. "Security Architecture Model Component Overview," *Sans Security Essentials*).

Applegate, L. M., Austin, R. D., and McFarlan, F. W. 2006. *Corporate Information Strategy and Management*. McGraw-Hill/Irwin Custom Publishing.

ASD. 2020. "Cyber Crime in Australia July to September 2019 ".

Atoum, I., Otoom, A., and Abu Ali, A. 2014. "A Holistic Cyber Security Implementation Framework," *Information Management & Computer Security* (22:3), pp. 251-264.

Baskerville, R., Baiyere, A., Gregor, S., Hevner, A., and Rossi, M. 2018. "Design Science Research Contributions: Finding a Balance between Artifact and Theory," *Journal of the Association for Information Systems* (19:5), pp. 358-376.

Benbasat, I., and Zmud, R. W. 2003. "The Identity Crisis within the Is Discipline: Defining and Communicating the Discipline's Core Properties," *MIS quarterly*), pp. 183-194.

Bente, S., Bombosch, U., and Langade, S. 2012. *Collaborative Enterprise Architecture: Enriching Ea with Lean, Agile, and Enterprise 2.0 Practices*. Newnes.

Berkel, A. R., Singh, P. M., and van Sinderen, M. J. 2018. "An Information Security Architecture for Smart Cities," *International Symposium on Business Modeling and Software Design*: Springer, pp. 167-184.

Bernroider, E. W., Margiol, S., and Taudes, A. 2016. "Towards a General Information Security Management Assessment Framework to Compare Cyber-Security of Critical Infrastructure Organizations," *Research and Practical Issues of Enterprise Information Systems: 10th IFIP WG 8.9 Working Conference, CONFENIS 2016, Vienna, Austria, December 13–14, 2016, Proceedings 10*: Springer, pp. 127-141.

Bittler, R. S., and Kreizman, G. 2005. "Gartner Enterprise Architecture Process: Evolution 2005," *G00130849, Gartner, Stamford, CT*), pp. 1-12.

Boucharas, V. 2010. "The Contribution of Enterprise Architecture to the Achievement of Organisational Goals,").

Brewer, J. 2000. *Ethnography*. McGraw-Hill Education (UK).

Burrell, G., and Morgan, G. 1979. "Two Dimensions: Four Paradigms," *Sociological paradigms and organizational analysis*), pp. 21-37.

Carlsson, S. A. 2010. "Design Science Research in Information Systems: A Critical Realist Approach," in *Design Research in Information Systems*. Springer, pp. 209-233.

Chaisiri, S., and Ko, R. K. 2016. "From Reactionary to Proactive Security: Context-Aware Security Policy Management and Optimization under Uncertainty," *2016 IEEE Trustcom/BigDataSE/ISPA*: IEEE, pp. 535-543.

Clark, P. C., Irvine, C. E., and Nguyen, T. D. 2014. "Trusted Computing Exemplar: Personnel Security Plan," NAVAL POSTGRADUATE SCHOOL MONTEREY CA.

Claycomb, W., and Shin, D. 2006. "Mobile-Driven Architecture for Managing Enterprise Security Policies," *ACMSE 2006*: ACM, pp. 555-559.

Clinch, J. 2009. "Itil V3 and Information Security," *Best Management Practice*).

Coghlan, D. 2019. *Doing Action Research in Your Own Organization*. SAGE Publications Limited.

Comfort, L. K. 2005. "Risk, Security, and Disaster Management," *Annu. Rev. Polit. Sci.* (8), pp. 335-356.

Contesti, D.-L., Andre, D., Henry, P. A., Goins, B. A., and Waxvik, E. 2007. *Official (Isc) 2 Guide to the Sscp Cbk*. CRC Press.

Copeland, M. 2017. *Cyber Security on Azure: An It Professional's Guide to Microsoft Azure Security Center*. Springer.

Covington, R., and Jahangir, H. 2009. "The Oracle Enterprise Architecture Framework,").

Crossler, R. E., Bélanger, F., and Ormond, D. 2017. "The Quest for Complete Security: An Empirical Analysis of Users' Multi-Layered Protection from Security Threats," *Information Systems Frontiers* (21), pp. 343–357.

Crotty, M. 1998. *The Foundations of Social Research: Meaning and Perspective in the Research Process*. Sage.

De Haes, S., Van Grembergen, W., and Debreceny, R. S. 2013. "Cobit 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities," *Journal of Information Systems* (27:1), pp. 307-324.

DeLone, W. H., and McLean, E. R. 2016. "Information Systems Success Measurement," *Foundations and Trends® in Information Systems* (2:1), pp. 1-116.

DiMase, D., Collier, Z. A., Heffner, K., and Linkov, I. 2015. "Systems Engineering Framework for Cyber Physical Security and Resilience," *Environment Systems and Decisions* (35:2), pp. 291-300.

DoD, C. 2010. "Dodaf Architecture Framework Version 2.02," *Website, August*).

Eloff, J., and Eloff, M. 2005. "Information Security Architecture," *Computer Fraud & Security* (2005:11), pp. 10-16.

Ertaul, L., and Sudarsanam, R. 2005. "Security Planning Using Zachman Framework for Enterprises " *EURO mGOV 2005* pp. 153-162.

Fairclough, N., and Wodak, R. 1997. "Critical Discourse Analysis," *Discourse studies: A multidisciplinary introduction* (2:357-378).

Fatolahi, A., and Shams, F. 2006. "An Investigation into Applying Uml to the Zachman Framework," *Information Systems Frontiers* (8:2), pp. 133-143.

Fennelly, L. J. 2016. *Effective Physical Security*. Butterworth-Heinemann.

Fitzgerald, T. 2011. *Information Security Governance Simplified: From the Boardroom to the Keyboard*. CRC Press.

Folger, R., and Stein, C. 2017. "Abduction 101: Reasoning Processes to Aid Discovery," *Human Resource Management Review* (27:2), pp. 306-315.

Fosnot, C. T. 2013. *Constructivism: Theory, Perspectives, and Practice*. Teachers College Press.

Fowler Jr, F. J. 2013. *Survey Research Methods*. Sage publications.

Galliers, R. D., King, J., and Lyytinen, K. 2006. *Information Systems, the State of the Field*. John Wiley & Sons, Ltd. West Sussex, England.

Gampfer, F., Jürgens, A., Müller, M., and Buchkremer, R. 2018. "Past, Current and Future Trends in Enterprise Architecture—a View Beyond the Horizon," *Computers in Industry* (100), pp. 70-84.

Gerber, A., le Roux, P., Kearney, C., and van der Merwe, A. 2020. "The Zachman Framework for Enterprise Architecture: An Explanatory Is Theory," *Conference on e-Business, e-Services and e-Society*: Springer, pp. 383-396.

Gillham, B. 2008. *Developing a Questionnaire*. A&C Black.

Gilliam, D. P., Wolfe, T. L., Sherif, J. S., and Bishop, M. 2003. "Software Security Checklist for the Software Life Cycle," *WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003.*: IEEE, pp. 243-248.

Gokhale, A. 2010. "Increasing Effectiveness of the Zachman Framework Using the Balanced Scorecard,").

Gollmann, D. 2010. "Computer Security," *Wiley Interdisciplinary Reviews: Computational Statistics* (2:5), pp. 544-554.

Gorazo. 2014. "Enterprise Architecture Literature Review,").

Gray, D. E. 2013. *Doing Research in the Real World*. Sage.

Gregor, S., and Hevner, A. R. 2013. "Positioning and Presenting Design Science Research for Maximum Impact," *MIS quarterly* (37:2), pp. 337-355.

Gregor, S., and Jones, D. 2007. "The Anatomy of a Design Theory," Association for Information Systems.

Gregory, R. W. 2011. "Design Science Research and the Grounded Theory Method: Characteristics, Differences, and Complementary Uses," in *Theory-Guided Modeling and Empiricism in Information Systems Research*. Springer, pp. 111-127.

Guarino, N., Oberle, D., and Staab, S. 2009. "What Is an Ontology?," in *Handbook on Ontologies*. Springer, pp. 1-17.

Gürel, E., and Tat, M. 2017. "Swot Analysis: A Theoretical Review," *Journal of International Social Research* (10:51).

Hammersley, M. 2007. "Ethnography," *The Blackwell encyclopedia of sociology*).

Haren, V. 2011. *Togaf Version 9.1*. Van Haren Publishing.

Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," *MIS quarterly*), pp. 75-105.

Highland, H. 1988. "The Brain Virus—Fact and Fantasy," *Computer Fraud & Security Bulletin* (10:11), pp. 4-9.

Hirschheim, R. 1985. "Information Systems Epistemology: An Historical Perspective," *Research methods in information systems*), pp. 13-35.

Ho, L. 2002. "Security Management Framework: A New Approach Based on John Zachman's Framework for Enterprise Architecture,").

Höne, K., and Eloff, J. H. P. 2002. "Information Security Policy—What Do International Information Security Standards Say?," *Computers & Security* (21:5), pp. 402-409.

Hopkin, P. 2018. *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*. Kogan Page Publishers.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security* (31:1), pp. 83-95.

ISACA. 2009. "An Introduction to the Business Model for Information Security,").

ISO. 2013. "I.S.O./I.E.C. 27000, 27001 and 27002 for Information Security Management."

ITGI, I. G. I. 2001. *Board Briefing on It Governance*. Information Systems Audit and Control Foundation.

ITIL. 2015. "Information Technology Infrastructure Library." 2015, from https://www.axelos.com/best-practice-solutions/itil/what-is-itil

Jeganathan, S. 2016. "Enterprise Security Architecure,").

Johnstone, B. 2017. *Discourse Analysis*. John Wiley & Sons.

Jordan, A., Haken, G., and Creasey, J. 2018. "The Standard of Good Practice for Information Security 2018," *Information Security Forum, United Kingdom*.

Josey, A. 2009. "Togaf Version 9.1 Enterprise Edition: An Introduction," *The Open Group* (11).

Juntunen, T., and Virta, S. 2019. "Security Dynamics: Multilayered Security Governance in an Age of Complexity, Uncertainty, and Resilience," *Leading Change In A Complex World: Transdisciplinary Perspectives*).

Killmeyer, J. 2006. *Information Security Architecture: An Integrated Approach to Security in the Organization*. CRC Press.

Kirk, J. 1999. "Information in Organisations: Directions for Information Management," *Information research* (4:3), pp. 4-3.

Kirlappos, I., and Sasse, M. A. 2014. "What Usable Security Really Means: Trusting and Engaging Users," in *Human Aspects of Information Security, Privacy, and Trust*. Springer, pp. 69-78.

Korhonen, J. J., Yildiz, M., and Mykkanen, J. 2009. "Governance of Information Security Elements in Service-Oriented Enterprise Architecture," *ISPAN 2009*: IEEE, pp. 768-773.

Korpela, K. 2015. "Improving Cyber Security Awareness and Training Programs with Data Analytics," *Information Security Journal: A Global Perspective* (24:1-3), pp. 72-77.

Kreizman, G., and Robertson, B. 2006. "Integrating Security into the Enterprise Architecture Framework." Stamford CT: Gartner Inc.(G00137069).

Lam, J. 2014. *Enterprise Risk Management: From Incentives to Controls*. John Wiley & Sons.

Lange, M., Mendling, J., and Recker, J. 2012. "A Comprehensive Ea Benefit Realization Model--an Exploratory Study," *HICSS 2012*: IEEE, pp. 4230-4239.

Lee, A. S., and Baskerville, R. L. 2003. "Generalizing Generalizability in Information Systems Research," *Information systems research* (14:3), pp. 221-243.

Linderman, K., Schroeder, R. G., Zaheer, S., and Choo, A. S. 2003. "Six Sigma: A Goal-Theoretic Perspective," *Journal of Operations management* (21:2), pp. 193-203.

Lindsay, J. D. 2009. "Security Systems for Protecting an Asset." Google Patents.

Luhach, A. K., and Luhach, R. 2015. "Research and Implementation of Security Framework for Small and Medium Sized E-Commerce Based on Soa," *Journal of Theoretical and Applied Information Technology* (82:3), p. 395.

Malhotra, Y. 2000. "Knowledge Management for E-Business Performance: Advancing Information Strategy to "Internet Time"," *Information Strategy: The Executive's Journal* (16:4), pp. 5-16.

Martin, P. Y., and Turner, B. A. 1986. "Grounded Theory and Organizational Research," *The journal of applied behavioral science* (22:2), pp. 141-157.

Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E., and Wieringa, R. 2019. "An Integrated Conceptual Model for Information System Security Risk Management Supported by Enterprise Architecture Management," *Software & Systems Modeling* (18:3), pp. 2285-2312.

McClintock, M., Falkner, K., Szabo, C., and Yarom, Y. 2020. "Enterprise Security Architecture: Mythology or Methodology?," *International Conference on Enterprise Information Systems*, pp. 679-689.

McCrie, R. 2015. *Security Operations Management*. Butterworth-Heinemann.

Mentz, J. C., Kotzé, P., and van der Merwe, A. 2014. "Propositions That Describe the Intended Meaning of Enterprise Architecture," *Proceedings of the Southern African Institute for*

Computer Scientist and Information Technologists Annual Conference 2014 on SAICSIT 2014 Empowered by Technology: ACM, p. 304.

Merleau-Ponty, M. 1996. *Phenomenology of Perception*. Motilal Banarsidass Publishe.

Metzger, S., Hommel, W., and Reiser, H. 2011. "Integrated Security Incident Management--Concepts and Real-World Experiences," *2011 Sixth International Conference on IT Security Incident Management and IT Forensics*: IEEE, pp. 107-121.

Meyer, M., Helfert, M., and O'Brien, C. 2011. "An Analysis of Enterprise Architecture Maturity Frameworks," in *Perspectives in Business Informatics Research*. Springer, pp. 167-177.

Mills, J., Bonner, A., and Francis, K. 2006. "The Development of Constructivist Grounded Theory," *International journal of qualitative methods* (5:1), pp. 25-35.

Moen, R., and Norman, C. 2006. "Evolution of the Pdca Cycle." Citeseer.

Moulton, R., and Coles, R. S. 2003. "Applying Information Security Governance," *Computers & Security* (22:7), pp. 580-584.

Mykhashchuk, M., Buckl, S., Dierl, T., and Schweda, C. M. 2011. "Charting the Landscape of Enterprise Architecture Management," *WI 2012*, pp. 570-577.

NIST. 2010. "Federal Enterprise Architecture Security and Privacy Profile V3,").

NIST. 2013. "Security and Privacy Controls for Federal Information Systems and Organizations (Sp-800-53 Rev 4)," *National Institute of Standards and Technology Special Publication* (800), p. 53.

NIST. 2014. "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," National Institute of Standards and Technology.

Nunamaker Jr, J. F., Chen, M., and Purdin, T. D. 1990. "Systems Development in Information Systems Research," *Journal of management information systems* (7:3), pp. 89-106.

OAIC. 2019. "Notifiable Data Breaches Scheme 12-Month Insights Report."

Oda, S. M., Fu, H., and Zhu, Y. 2009. "Enterprise Information Security Architecture a Review of Frameworks, Methodology, and Case Studies," *ICCSIT 2009*: IEEE, pp. 333-337.

Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T., and Kagaya, T. 2009. "Information Security Governance Framework," *WISG '09*: ACM, pp. 1-6.

Oppenheim, A. N. 1992. "Questionnaire Design," *Interviewing and Attitude measurement* (24).

Oppenheim, A. N. 2000. *Questionnaire Design, Interviewing and Attitude Measurement*. Bloomsbury Publishing.

Orman, H. 2003. "The Morris Worm: A Fifteen-Year Perspective," *IEEE Security & Privacy* (1:5), pp. 35-43.

Orna, E. 2017. *Information Strategy in Practice*. Routledge.

Panchenko, V., Zamula, A., Kavun, S., and Mikheev, I. 2018. "Intelligent Management of the Enterprise Personnel Security System," *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*: IEEE, pp. 469-474.

Pather, S., and Remenyi, D. 2005. "Some of the Philosophical Issues Underpinning Research in Information Systems-from Positivism to Critical Realism: Reviewed Article," *South African Computer Journal* (2005:35), pp. 76-83.

Patterson, T. 2003. "Holistic Security: Why Doing More Can Cost You Less and Lower Your Risk," *Computer Fraud & Security*:6), pp. 13-15.

Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., and Bragge, J. 2006. "The Design Science Research Process: A Model for Producing and Presenting Information Systems Research," *Proceedings of the first international conference on design science research in information systems and technology (DESRIST 2006)*: ME Sharpe, Inc., pp. 83-106.

Peltier, T. R. 2013. *Information Security Fundamentals*. CRC press.

Peltier, T. R. 2016. *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. CRC Press.

Plachkinova, M., and Maurer, C. 2019. "Security Breach at Target," *Journal of Information Systems Education* (29:1), p. 7.

Posthumus, S., and Von Solms, R. 2004. "A Framework for the Governance of Information Security," *Computers & Security* (23:8), pp. 638-646.

Prajogo, D., Toy, J., Bhattacharya, A., Oke, A., and Cheng, T. 2018. "The Relationships between Information Management, Process Management and Operational Performance: Internal and External Contexts," *International Journal of Production Economics* (199), pp. 95-103.

Purdy, G. 2010. "Iso 31000: 2009—Setting a New Standard for Risk Management," *Risk Analysis: An International Journal* (30:6), pp. 881-886.

Rahi, S. 2017. "Research Design and Methods: A Systematic Review of Research Paradigms, Sampling Issues and Instruments Development," *International Journal of Economics & Management Sciences* (6:2), pp. 1-5.

Rees, J., Bandyopadhyay, S., and Spafford, E. H. 2003. "Pfires: A Policy Framework for Information Security," *Communications of the ACM* (46:7), pp. 101-106.

Reza Bazi, H., Hasanzadeh, A., and Moeini, A. 2017. "A Comprehensive Framework for Cloud Computing Migration Using Meta-Synthesis Approach," *Journal of Systems and Software*).

Roberti, M. 2001. "Building an Enterprise Security Architecture," *Retrieved September* (10).

Roeleven, S., and Broer, J. 2010. "Why Two Thirds of Enterprise Architecture Projects Fail," *ARIS Expert Paper*).

Rowley, J. 2012. "Conducting Research Interviews," *Management research review*).

Safa, N. S., Von Solms, R., and Furnell, S. 2016. "Information Security Policy Compliance Model in Organizations," *computers & security* (56), pp. 70-82.

Saint-Louis, P., and Lapalme, J. 2016. "Investigation of the Lack of Common Understanding in the Discipline of Enterprise Architecture: A Systematic Mapping Study," *2016 IEEE 20th International Enterprise Distributed Object Computing Workshop (EDOCW)*: IEEE, pp. 1-9.

Saleh, M. S., and Alfantookh, A. 2011. "A New Comprehensive Framework for Enterprise Information Security Risk Management," *Applied computing and informatics* (9:2), pp. 107-118.

Sandhu, R. 2000. "Engineering Authority and Trust in Cyberspace: The Om-Am and Rbac Way," *ACM RBAC 2000*: ACM, pp. 111-119.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., and Youman, C. E. 1996. "Role-Based Access Control Models," *Computer* (29:2), pp. 38-47.

Sandhu, R. S., and Samarati, P. 1994. "Access Control: Principle and Practice," *IEEE communications magazine* (32:9), pp. 40-48.

Scholtz, T. 2006. "Structure and Content of an Enterprise Information Security Architecture," *Gartner Inc*).

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., and Lindgren, R. 2011. "Action Design Research," *MIS quarterly*), pp. 37-56.

Sessions, R. 2007. "Comparison of the Top Four Enterprise Architecture Methodologies,").

Shackleford, D. 2016. "Sans 2016 Security Analytics Survey," *SANS Institute, Swansea*).

Shariati, M., Bahmani, F., and Shams, F. 2011. "Enterprise Information Security, a Review of Architectures and Frameworks from Interoperability Perspective," *Procedia Computer Science* (3), pp. 537-543.

Shen, Y. T., Lin, F., and Rohm, T. 2009. "A Framework for Enterprise Security Architecture and Its Application in Information Security Incident Management," *Communications of the IIMA* (9:4), pp. 8-20.

Sherwood, J., Clark, A., and Lynas, D. 1995. "Enterprise Security Architecture," *SABSA White Paper2009*).

Siponen, M., Pahnila, S., and Mahmood, M. A. 2010. "Compliance with Information Security Policies: An Empirical Investigation," *Computer* (43:2), pp. 64-71.

Siponen, M., and Willison, R. 2009. "Information Security Management Standards: Problems and Solutions," *Information & Management* (46:5), pp. 267-270.

Snedaker, S. 2013. *Business Continuity and Disaster Recovery Planning for It Professionals*. Newnes.

Stanton, R. 2005. "Beyond Disaster Recovery: The Benefits of Business Continuity," *Computer Fraud & Security* (2005:7), pp. 18-19.

Starks, H., and Brown Trinidad, S. 2007. "Choose Your Method: A Comparison of Phenomenology, Discourse Analysis, and Grounded Theory," *Qualitative health research* (17:10), pp. 1372-1380.

Stoneburner, G. 2001. *Underlying Technical Models for Information Technology Security: Recommendation of the National Institute of Standards and Technology*. US Department of Commerce.

Strauss, A., and Corbin, J. 1994. "Grounded Theory Methodology," *Handbook of qualitative research* (17), pp. 273-285.

Strauss, A., and Corbin, J. 1998. *Basics of Qualitative Research Techniques*. Sage publications.

Sun, J., and Chen, Y. 2008. "Intelligent Enterprise Information Security Architecture Based on Service Oriented Architecture," *FITME 2008*: IEEE, pp. 196-200.

Susman, G. I., and Evered, R. D. 1978. "An Assessment of the Scientific Merits of Action Research," *Administrative science quarterly*), pp. 582-603.

Tamm, T., Seddon, P. B., Shanks, G., and Reynolds, P. 2011. "How Does Enterprise Architecture Add Value to Organisations," *Communications of the Association for Information Systems* (28:1), pp. 141-168.

Theoharidou, M., and Gritzalis, D. 2007. "Common Body of Knowledge for Information Security," *Security & Privacy, IEEE* (5:2), pp. 64-67.

Tøndel, I. A., Line, M. B., and Jaatun, M. G. 2014. "Information Security Incident Management: Current Practice as Reported in the Literature," *Computers & Security* (45), pp. 42-57.

Trcek, D. 2003. "An Integral Framework for Information Systems Security Management," *Computers & Security* (22:4), pp. 337-360.

U.S.Government. 2013. "Federal Enterprise Architecture Framework Version 2,").

Urquhart, C., Lehmann, H., and Myers, M. D. 2010. "Putting the 'Theory'back into Grounded Theory: Guidelines for Grounded Theory Studies in Information Systems," *Information systems journal* (20:4), pp. 357-381.

Vaishnavi, V., and Kuechler, W. 2004. "Design Research in Information Systems,").

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:3-4), pp. 190-198.

Veiga, A. D., and Eloff, J. H. 2007. "An Information Security Governance Framework," *Information Systems Management* (24:4), pp. 361-372.

Venable, J. 2006. "A Framework for Design Science Research Activities," *Emerging Trends and Challenges in Information Technology Management: Proceedings of the 2006 Information Resource Management Association Conference*: Idea Group Publishing, pp. 184-187.

Venable, J., Pries-Heje, J., and Baskerville, R. 2016. "Feds: A Framework for Evaluation in Design Science Research," *European Journal of Information Systems* (25:1), pp. 77-89.

von Solms, B. 2005. "Information Security Governance: Cobit or Iso 17799 or Both?," *Computers & Security* (24:2), pp. 99-104.

Wahe, S. 2011. "Open Enterprise Security Architecture - a Framework and Template for Policy-Driven Security,").

Walsham, G. 1995. "The Emergence of Interpretivism in Is Research," *Information systems research* (6:4), pp. 376-394.

Webb, J., Ahmad, A., Maynard, S. B., and Shanks, G. 2014. "A Situation Awareness Model for Information Security Risk Management," *Computers & security* (44), pp. 1-15.

Whitman, M., and Mattord, H. 2011. *Principles of Information Security*. Cengage Learning.

Williams, M. 2003. "Questionnaire Design," *Making sense of social research*), pp. 104-124.

Wilson, M., and Hash, J. 2003. "Building an Information Technology Security Awareness and Training Program," *NIST Special publication* (800:50), pp. 1-39.

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

Zachman, J. A. 2001. "Security and the 'Zachman Framework'," *Enterprise Architecture Resources*).

Zachman, J. A. 2008. "The Enterprise Ontology,").

Zachman, J. A. 2015. "A Historical Look at Enterprise Architecture with John Zachman,").

Zachman, J. A. 2016. "The Framework for Enterprise Architecture: Background, Description and Utility by John A," *Zachman, published by Zachman Institute for Framework Advancement (ZIFA) Document ID*), pp. 810-231.

Zachman, J. P. 2011. "The Zachman Framework Evolution,").

Zafar, H. 2013. "Human Resource Information Systems: Information Security Concerns for Organizations," *Human Resource Management Review* (23:1), pp. 105-113.

Zio, E. 2018. "The Future of Risk Assessment," *Reliability Engineering & System Safety* (177), pp. 176-190.