Security Architecture Framework for Enterprises

Michelle Graham[1], Katrina Falkner[2], Claudia Szabo[3] and Yuval Yarom[4]

School of Computer Science, University of Adelaide, North Terrace, Adelaide, Australia
michelle.graham, katrina.falkner, claudia.szabo@adelaide.edu.au,
yval@cs.adelaide.edu.au

Abstract. Security is a complex issue for organisations, with its management now a fiduciary responsibility as well as a moral one. Without a holistic robust security structure that considers human, organisational and technical aspects to manage security, 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 at least 30 years in organisations globally. It relies on a holistic classification structure for organisational assets. Grouping security with EA promises to leverage the benefits of EA in the security domain. We conduct a review of existing security frameworks to evaluate the extent to which they employ EA. We find that while the idea of grouping security with EA is not new, there is a need for developing a comprehensive solution. We design, develop, and demonstrate a security EA framework for organisations regardless of their industry, budgetary constraints or size; and survey professionals to analyse the framework and provide feedback. The survey 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.

Keywords: design science research, information systems security policy, enterprise architecture.

1 Introduction

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 [1]. High profile American security breaches such as the Verizon breach releasing more than 14 million customer records[5], the WannaCry ransomware computer hack giving access to NSA files[6] and the iCloud

[1] https://orcid.org/0000-0001-5658-6483
[2] https://orcid.org/0000-0003-0309-4332
[3] https://orcid.org/0000-0003-2501-1155
[4] https://orcid.org/0000-0003-0401-4197
[5] http://www.zdnet.com/article/millions-verizon-customer-records-israeli-data/
[6] http://www.wired.co.uk/article/wannacry-ransomware-virus-patch

accounts extortion[7] highlight the global need for increased security resilience. These startling statistics highlight that effective security has never been more important to businesses and therefore individuals [2], however very few companies have adopted a cohesive security strategy that encompasses the protection of all assets whether they be physical, digital or cognitive [3]. The benefits of a holistic approach could be used to mitigate these risks and requires 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 [4, 5]. Enterprise Architecture (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 [6]. The development of the concept of a holistic security structure using EA would demonstrate that security is not just technical but requires a focusing on all the organisational assets of people, information, technology and processes and will provide enterprise security management guidance to contemporary digitalised organisations of the 21st Century.

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?

This paper builds on and extends our past work [7]. The main new contribution is an expanding the original four design principles to five, adding a requirement for ontological phrases and providing a broader explanation of the principles. This paper further expands the analysis of the evaluation of the artifact and revises the related works section identifying and analysing five analogous security frameworks surveys. In addition, this paper includes a more detailed explanation of the theoretical foundations including Design Science Research, philosophy approach and qualitative analysis method.

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, needs to be tested [7, 8]. We develop a novel, fully researched enterprise security architecture (ESA) framework for organisations. The framework is 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. Our 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 defense-in-depth and in the current world climate, what could be more necessary to business [5].

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

The paper is organised as follows. The background discusses the methods used and the sources consulted to meet the research goals. To describe the ESA artifact, a description of the design search (development) process and procedures that led to the artifact design principles is provided as well as a detailed description of the artifact itself. The assessment includes 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 rich data set for analysis. The explanation also demonstrates the chosen evaluations' utility, validity, quality and efficacy [9] and discusses 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. Through research, five security framework surveys were identified and analysed, a discussion of each will be provided. Finally, we conclude 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

Notwithstanding the popularity and recent adoption of EA, the majority of EA frameworks do not have a security component [8]. The Zachman ontological framework [9] is one of the most widely accepted and implemented EA frameworks, however despite Zachman's success, it does not include security in any form [10]. This lack of security has been identified by others [5] who have used Zachman to create an enterprise security architecture (ESA) [11]. 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 [9]. 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 [12]. 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. A Design Science Research (DSR) study [10, 11] suited the research due to the emphasis on the design and creation of an artifact to test a research question [12] and the research rigor the DSR methodology provided [13, 14]. 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 [15] qualitative questionnaire. We will explain the history of EA, the rationale behind the choice of DSR and how it is used in this research as well as the selection for the philosophy, approach and method.

2.1 Enterprise Architecture

The enterprise architecture (EA) domain began with Zachman's seminal work in 1987 [16]. 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, specifically focusing on the advent of computing. The theory 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.

EA frameworks fall into two categories, ontologies and prescriptive methodologies. An ontology or classification structure is a recognized vocabulary used to describe objects in a particular domain [17]. A prescriptive methodology describes how to create the artifacts and with what tools or describes which artifacts are required to be in compliance with the framework. The Zachman framework is an example of an ontology and is now the adopted vocabulary for EA. The Zachman 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.

The implementation of the Zachman 6 x 6 framework grid 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 fulfill 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 which 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. The ontology is used to organise and categorise an organisation's artifacts which are notated in the framework's grid.

2.2 Security

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 almost all departments within an organisation. The difficulty is that due to their evolution 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. The overall effect is a lack of a cohesive strategy for organisational security [18].

Looking at frameworks that address the need for enterprise-wide security, holistic frameworks for organisational security are limited. One example is governance frameworks which are defined by the IT Governance Institute [19] 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; however 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 [20]. Unfortunately it is still very common for a company to believe that organisational security is solely about virus defense 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 [21]. As Anderson [7] 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.

2.3 Design Science Research

Vaishnavi & Kuechler [22] describe the body of DSR knowledge as man-made objects – artifacts – that are designed to meet specific goals. It creates novel contributions through the design of new artifacts including the analysis of their operation using evaluation and abstraction. DSR uses design as a research method that maps functional requirements on to a fulfilling artifact. As indicated in Figure 1 there are five steps.

Awareness of the Problem – Step 1. An individual becomes aware of a problem that doesn't 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. The problem was then confirmed through a literature review of holistic security models, 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.

Suggestion – Step 2. Suggestion is the second stage and 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.

Development – Step 3. At step three the artifact is created using the design from step two however it is important to note that the emphasis is on the novelty of the design not

the creation of the artifact. Using the principles to guide the design, a security architecture framework artifact was created – a thirty-six cell security instantiation or ontology.

Evaluation – Step 4. Performance measures are placed on the artifact from the initial proposal to evaluate and at this stage, any changes are fed into the design towards a new design process. Using the design principles and security domain guidelines, the security framework was given to managers, security professionals, IT professionals and researchers, along with a questionnaire about the utility of the framework, to evaluate and provide the cyclical feedback to inform the artifact change process.

Conclusion – Step 5. This cyclical evaluation continues until a conclusion is reached – usually the end of the research cycle or the solution is considered "good enough" and the results are written up.

Our research is overlaid onto the Outputs column in Figure 1 (colored red) to demonstrate our use of the DSR methodology.

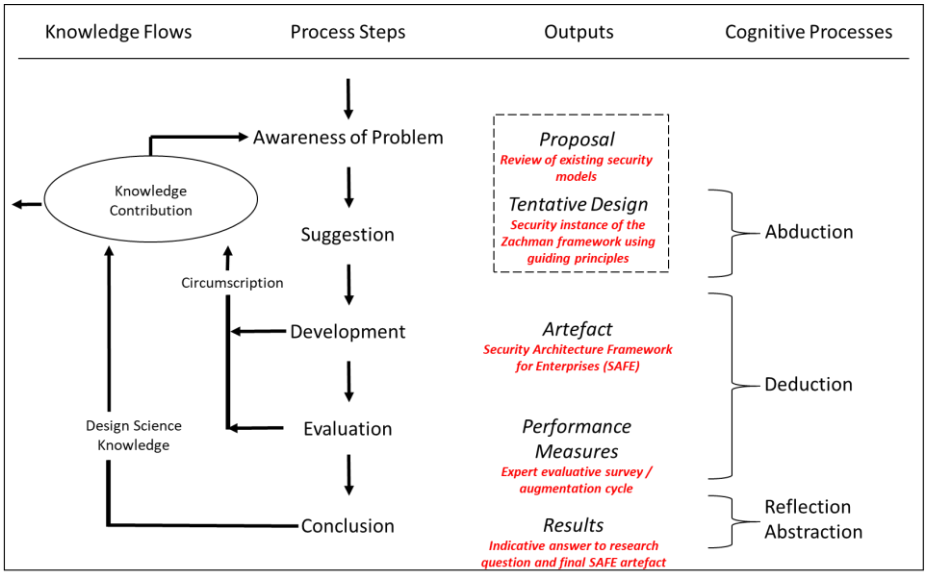

Fig. 1. SAFE Outputs in Design Science Research Cycle [22, 23]

2.4 Philosophy

The philosophy of the development of research is based on a system of beliefs and assumptions that are used at all stages of the research. 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 [24]. This research is based in the underlying assumptions of constructivism, which are often used in concert with DSR and qualitative research. This provides a basis for how knowledge is perceived and how it can be obtained [25] 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 which create new representations of reality and therefore new models using cultural tools and symbols bringing meaning and finding authentication through discussion in communities of practice [26]. 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). [27, 28]

2.5 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 develop a definitive assumption or likely conclusion [29]. Inductive reasoning was chosen for this research because of the nature of DSR and 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.

2.6 Qualitative Research Method

Grounded Theory was identified as the best suited for this research and for the qualitative data set that would be developed from the Oppenheim [15] questionnaire evaluation of the security artifact.

The Oppenheim approach was chosen because it provides clear advice on the length, clarity, grammar and specificity of the questions and attempts to avoid such bias in questions as social desirability, double barreled questions and negatively worded questions [15, 30]. The type of responses gathered from an Oppenheim also lend itself to provide effective inputs to a grounded theory qualitative analysis [31].

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 [32]. The codes are inspected for patterns and then reintegrated to form dominant thematic subjects and connections. [33, 34] 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 [35] 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 Enterprise Security Architecture Design

As described previously, 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". An analysis of 25 security frameworks, detailed in our past work [23], provided a set of five guiding design principles that would help guide an organisation towards a more secure corporate posture and concurrently support the achievement of corporate vision and strategy. The 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.

3.1 Guiding Recommendations

The following discussion explains the five design principles which have guided the development of the enterprise security architecture artifact.

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 defense-in-depth.

Framework Type (Principle 2). EA ontologies are a classification system that provides 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 doesn't 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 and uses ontological phrases and constructs.

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 [36]. 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 27000 and NIST. 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 [37]. From the analysis of the 25 frameworks, seven of the 25 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 [38], the GEAF [37], the FEAF [39] and the DoDAF [40]. 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 [18]. 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 [41].

In summary, the principles we identified provide the design foundation which supported the development of the security artifact to evaluate the design which is addressing the problem statement “will a holistic security model using EA provide security benefits in an organisation more effectively than a piecemeal approach”.

3.2 The 36 Cells of the Artifact

Using the five principles identified in Section 4.1, the framework is developed based on the Zachman framework 2013 Version 3.0 [42] 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. Also the Zachman does not have a security view which increased the novelty of our approach. All 36 cells of the Zachman framework were explored and researched to determine exactly what the purpose of the cell was. All external research available was read thoroughly to provide a clear understanding of the framework and the purpose of each cell in it. This included identifying full definitions for each cell and the outer framework terms. 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). We methodically develop all 36 cells of the security instantiation by research and analysis of the 36 Zachman cells. The outcome is the ESA framework which is an exact matching overlay of the Zachman framework as a security instantiation.

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 organisational 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 27000 and NIST

Figure 2 is an example of the four factors defined for each cell.

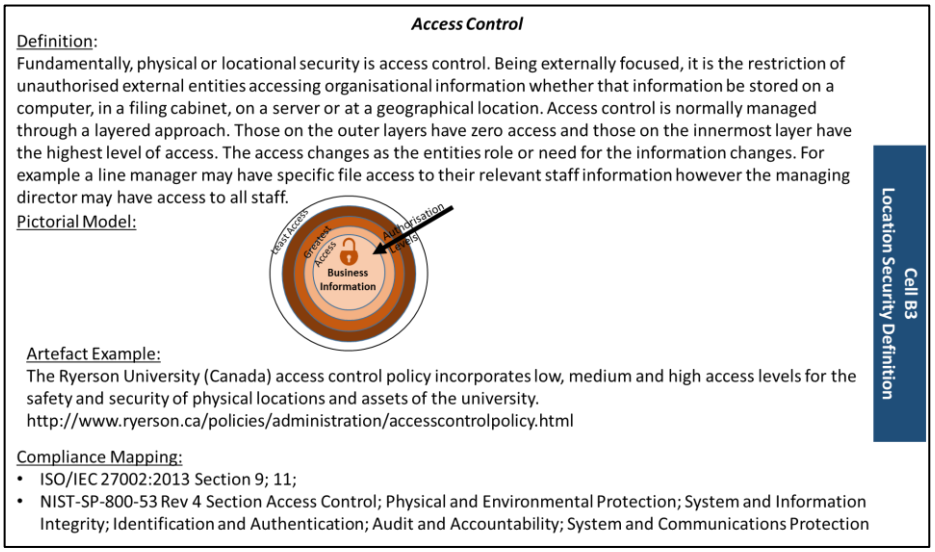

Fig. 2. Cell definition example.

3.3 The Security Architecture Framework for Enterprises Artifact

In summary, the notional artifact was completed and three layers of abstraction developed. The row / column categories, the detailed security definitions and the more detailed definitions (pictorial model, artifact example and compliance mapping) for use by organisation for understanding. The final framework is compliant with the 5 guiding design principles identified. Figure 3 is the completed Security Architecture

Framework for Enterprises (SAFE) artifact.

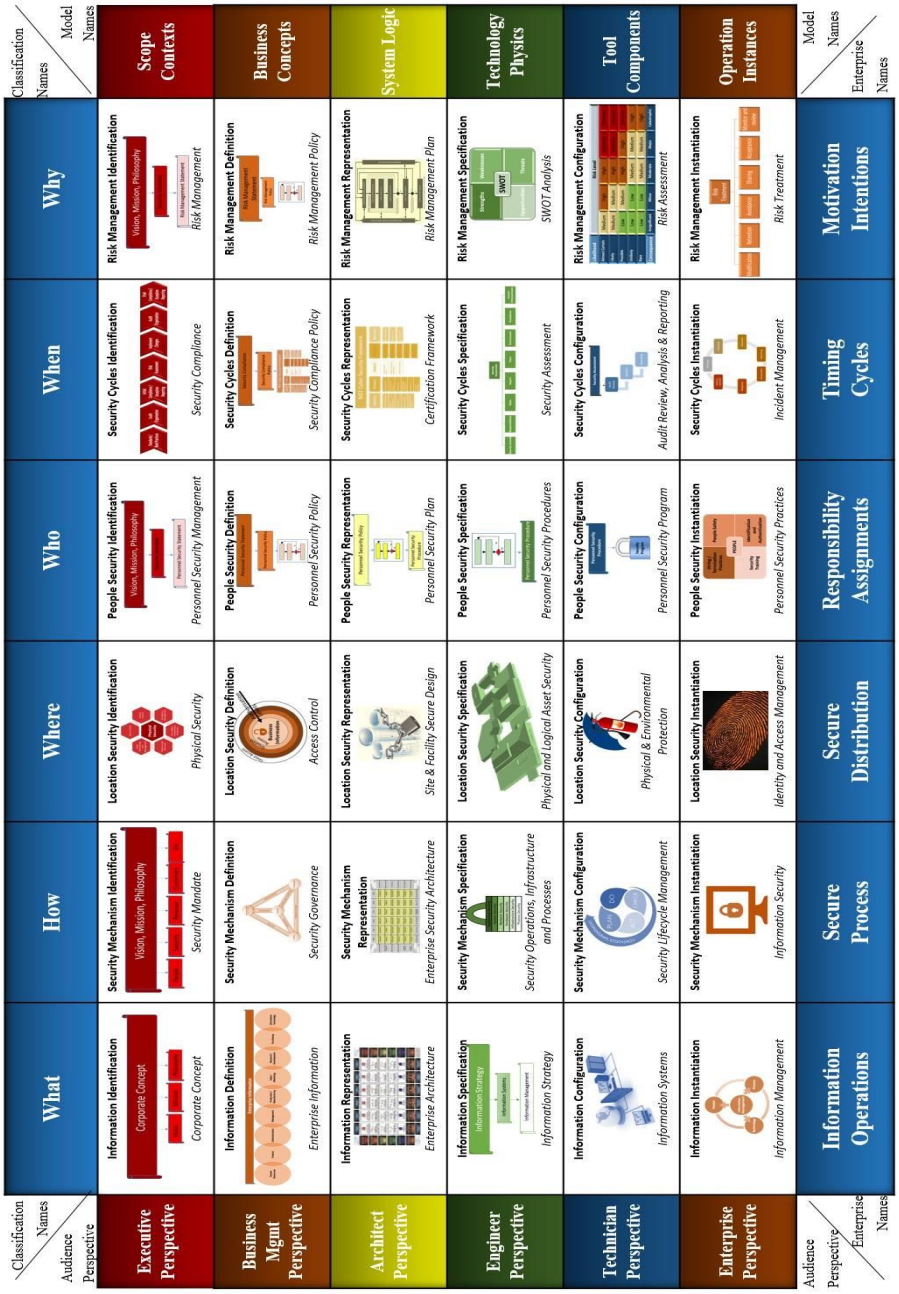

Figure 3: The Security Architecture Framework for Enterprises (SAFE) artifact **[23]**

4 Artifact Assessment

To test the artifact design described previously, an Oppenheim structured expert evaluation survey was created to ask questions of a group of participants about the efficacy, validity, utility and quality of the artifact. We received 12 responses and an inductive grounded theory qualitative analysis was completed to derive the foremost themes indicated by the participants. The themes and anecdotal results are discussed and participant quotes are included.

4.1 Expert Evaluation Survey

We shared the artifact and supporting documentation for critique, to four categories of professionals – manager, security professional, IT professional and researcher. The participants are 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 work through each cell and determine 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 we have created should functionally be able to build security into all aspects of the organisation. Theoretically a form of an organisational security ontology.

To gather the participant's inputs we designed a questionnaire using an Oppenheim [15] approach and following a successful rigorous ethical research approval process, distributed the questionnaire. The questionnaire 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.

The survey responses were collated and grounded theory was used to draw out themes, through an inductive data collection that enables the participants to tell the story. Through the cyclical nature of the grounded theory methodology, each coding phase provided richer thematic results. For example the question "Have you found the framework and background information educational?" The first coding phase saw 13 raw responses from participants. However after a second, third and fourth coding phase, which essentially distilled the responses down to the key themes, the final three thematic responses became 1) Definitions, artifacts, models and references are a very strong tool; 2) Shows the full extent of issues involved in security - risk, difficulties and complexity; 3) Security policies and practices can be used to form a cohesive framework / security program.

4.2 Participant Demography

We received 12 participant questionnaires, of which 75% of participants 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 ten years and considered themselves experts in the field. The participants came from Industry (58%), Government (33%) or the Military (8%). Table 10 provides the demographic questions and the reason they were included in the survey.

4.3 Results of Design Principles Application

The following discussion describes the participant results to the 14 questions related to the Principles. The outcome shows an effective implementation of the Principles in guiding the design of the framework and the responses indicate that the artifact provides significant organisational security benefits more effectively than a piecemeal approach which successfully answers the research question. Table 1 provides the 14 questions and the design principle(s) they are mapped to or the purpose for inclusion.

Table 1. Artifact survey questions and design principle mapping

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
Q3. Do you believe a holistic approach to security is likely to provide a more secure organisation? Why or why not?	Principle1, Principle 5
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

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
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 positive use 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 and ISO27002 (international security industry standards). Does this information give you more confidence in the framework? Is the compliance important to you?	Principle 3
Q11. Is the framework easy to understand and use? Why or why not?	Usability 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.
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.

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.

Participant comments included "ensures all aspects of security are covered and assessed", "organises the complete security function", and "focuses organisations to include security elements not traditionally addressed".

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 wouldn't. 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 ten 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 very 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.

Participant comments included "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".

Principle 3 – Compliance to security industry standard. Survey questions two, five and ten 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 27000 and NIST. 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.

Participant comments include "compliance to NIST and ISO validates the framework in terms of academic rigor", "management are more likely to accept a model based on international standards", "compliance standards build more confidence in the benefits and provenance of the framework" and "tells me that the framework is based on best practice".

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 25 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.

Participant comments include "definitions, artifacts, models and references are a very strong tool", "fantastic concept that provides a single awareness for all security" and "would be used effectively and compliment the organisations existing enterprise architecture".

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. Mapping all of an organisations security in the single model would provide a view of security that had not previously been available. The consequences of this was exciting for some 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. Also a holistic view of an organisation's security is a balanced view of security for the purposes of resources and discussions where ICT or physical security is usually the focus.

Participant comments 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".

4.4 Theoretical Significance

The kernel knowledge for this research was the domain of enterprise architecture. As described in the Literature Review, 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.

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.

5 Related Work

The earliest enterprise security architecture (ESA) frameworks were developed in 1995 [43] and the few approaches available all agree that "the problem is that no standardised, comprehensive information security architecture currently exists" [5, 18]. Our analysis of existing work identified five surveys of ESA frameworks which gives a broad domain overview of the status of Enterprise Security Architecture as a discipline. The outcome of this review also led us to the need for a new, more comprehensive security framework survey which can be found in our past work [23] and includes 25 frameworks reviewed. The surveys are discussed below.

The Shariati et al. [44] 2010 survey 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 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. In contrast, this research has reviewed 25 frameworks and provides a recommended principles-based framework for an effective security framework.

The Oda et al. review [45] 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 [46], 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 [47] is centered 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 [48] 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 [18] 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.

6 Conclusions

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 25 organisational security structures demonstrated in our past work [23], 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 25 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.

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 3) 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 review and has been completed to three layers of abstraction. 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.

To determine the effectiveness of the framework in meeting security concerns and test the efficacy within real-world organisational environments, we shared the framework and supporting documentation 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 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 such as a larger design study, a case study in an organisation or an organisational implementation study to explore further the ideas discussed in this research.

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. The success of this important security research provides an opportunity and a significant foundation for future ESA studies.

Acknowledgements

This work has been supported by an Australian Research Council Discovery Early Career Research Award (project number DE200101577).

References

1. ASD, Cyber Crime in Australia July to September 2019 (2020).
2. Patterson, T., Holistic Security: Why Doing More Can Cost You Less and Lower Your Risk. Computer Fraud & Security, 2003(6): p. 13-15.
3. Roeleven, S. and J. Broer, Why Two Thirds of Enterprise Architecture Projects Fail. ARIS Expert Paper (2010).
4. Angelo, S., Security Architecture Model Component Overview. Sans Security Essentials (2001).
5. Copeland, M., Cyber Security on Azure: An IT Professional's Guide to Microsoft Azure Security Center. (2017): Springer.
6. Gorazo, Enterprise Architecture Literature Review. (2014)
7. Anderson, R., Security engineering. 2008: John Wiley & Sons.
8. Moulton, R. and R.S. Coles, Applying information security governance. Computers & Security, 2003. 22(7): p. 580-584.
9. Gregor, S. and A.R. Hevner, Positioning and presenting design science research for maximum impact. MIS quarterly, 2013. 37(2): p. 337-355.
10. Hevner, A.R., et al., Design science in information systems research. MIS quarterly, 2004: p. 75-105.
11. Nunamaker Jr, J.F., M. Chen, and T.D. Purdin, Systems development in information systems research. Journal of management information systems, 1990. 7(3): p. 89-106.
12. Venable, J., J. Pries-Heje, and R. Baskerville, FEDS: a framework for evaluation in design science research. European Journal of Information Systems, 2016. 25(1): p. 77-89.
13. Sein, M.K., et al., Action design research. MIS quarterly, 2011: p. 37-56.
14. Peffers, K., et al. The design science research process: a model for producing and presenting information systems research. in Proceedings of the first international conference on design science research in information systems and technology (DESRIST 2006). 2006. ME Sharpe, Inc.
15. Oppenheim, A.N., Questionnaire design, interviewing and attitude measurement. 2000: Bloomsbury Publishing.
16. Zachman, J.A., A framework for information systems architecture. IBM System Journal, 1987. 26(3): p. 276-292.
17. EBI, E.B.I., Glossary. (2015)
18. Eloff, J. and M. Eloff, Information security architecture. Computer Fraud & Security, 2005. 2005(11): p. 10-16.
19. ITGI, I.G.I., Board briefing on IT governance. 2001: Information Systems Audit and Control Foundation.
20. Anderson, R., Why information security is hard-an economic perspective, in Proceedings 17th Annual Computer Security Applications Conference pp. 358-365. 2001, IEEE. p. 358-365.
21. ISACA, An Introduction to the Business Model for Information Security (2009.
22. Vaishnavi, V. and W. Kuechler, Design research in information systems (2004).

23. McClintock, M., et al. Enterprise Security Architecture: Mythology or Methodology? in International Conference on Enterprise Information Systems (2020).
24. Crotty, M., The foundations of social research: Meaning and perspective in the research process. 1998: Sage.
25. Hirschheim, R., Information systems epistemology: An historical perspective. Research methods in information systems, 1985: p. 13-35.
26. Fosnot, C.T., Constructivism: Theory, perspectives, and practice. 2013: Teachers College Press.
27. Strauss, A. and J. Corbin, Basics of qualitative research techniques. 1998: Sage publications.
28. Mills, J., A. Bonner, and K. Francis, The development of constructivist grounded theory. International journal of qualitative methods, 2006. 5(1): p. 25-35.
29. Lee, A.S. and R.L. Baskerville, Generalizing generalizability in information systems research. Information systems research, 2003. 14(3): p. 221-243.
30. Williams, M., Questionnaire design. Making sense of social research, 2003: p. 104-124.
31. Rattray, J. and M.C. Jones, Essential elements of questionnaire design and development. Journal of clinical nursing, 2007. 16(2): p. 234-243.
32. Urquhart, C., H. Lehmann, and M.D. Myers, Putting the 'theory'back into grounded theory: guidelines for grounded theory studies in information systems. Information systems journal, 2010. 20(4): p. 357-381.
33. Starks, H. and S. Brown Trinidad, Choose your method: A comparison of phenomenology, discourse analysis, and grounded theory. Qualitative health research, 2007. 17(10): p. 1372-1380.
34. Strauss, A. and J. Corbin, Grounded theory methodology. Handbook of qualitative research, 1994. 17: p. 273-85.
35. Martin, P.Y. and B.A. Turner, Grounded theory and organizational research. The journal of applied behavioral science, 1986. 22(2): p. 141-157.
36. Siponen, M. and R. Willison, Information security management standards: Problems and solutions. Information & Management, 2009. 46(5): p. 267-270.
37. Bittler, R.S. and G. Kreizman, Gartner Enterprise Architecture Process: Evolution 2005. G00130849, Gartner, Stamford, CT, 2005: p. 1-12.
38. Josey, A., TOGAF Version 9.1 Enterprise Edition: An Introduction. The Open Group, (2009).
39. USG, U.S.F.G., Introduction to the Federal Enterprise Architecture Framework V2. (2013).
40. DoD, C., DoDAF Architecture Framework Version 2.02. Website, August (2010).
41. ISO, I.S.O./I.E.C. 27000, 27001 and 27002 for information security management (2013).
42. Zachman, J.A., The framework for enterprise architecture: background, description and utility. Zachman International (1996).
43. Sherwood, J., A. Clark, and D. Lynas, Enterprise security architecture. SABSA White Paper 2009 (1995).
44. Shariati, M., F. Bahmani, and F. Shams, Enterprise information security, a review of architectures and frameworks from interoperability perspective. Procedia Computer Science, 2011. 3: p. 537-543.
45. Oda, S.M., H. Fu, and Y. Zhu. Enterprise information security architecture a review of frameworks, methodology, and case studies. in ICCSIT 2009. 2009. IEEE.
46. Zachman, J.P., The Zachman Framework Evolution (2011).

47. Veiga, A.D. and J.H. Eloff, An information security governance framework. Information Systems Management, 2007. 24(4): p. 361-372.
48. Claycomb, W. and D. Shin. Mobile-driven architecture for managing enterprise security policies. in ACMSE 2006. 2006. ACM.