Enterprise Security Architecture: Mythology or Methodology?

Michelle McClintock[a], Katrina Falkner[b], Claudia Szabo[c] and Yuval Yarom[d]
School of Computer Science, University of Adelaide, North Terrace, Adelaide, Australia

Keywords: Information Systems Security Policy, Enterprise Architecture, Design Science Research, Grounded Method, Business Process Modelling.

Abstract: Security has never been more important. However, without a holistic security structure that secures all assets of an organisation (physical, digital or cognitive), an organisation is at a critical risk. Enterprise architecture (EA) applies engineering design principles and provides a complete structure to design and build an organisation using classification schema and descriptive representations. The grouping of security with EA, through a framework with corresponding security classifications and representations, promises a complete security solution. We evaluate security frameworks and find that grouping security with EA is not new, however current solutions indicate a lack of research process in development, a disjoint focus in either technical or policy / department or project. Thus, there is a need for a holistic solution. We use a Design Science Research methodology to design, develop, and demonstrate a security EA framework that provides an organisation with a complete security solution regardless of industry, budgetary constraints, or size, and survey professionals to critically analyse the framework. The results indicate the need for a complete security structure including benefits in governance, resourcing, functional responsibilities, risk management and compliance.

1 INTRODUCTION

In less than one year, between April 2018 and March 2019, there were 964 data breach notifications made under the Australian Notifiable Data Breaches scheme by businesses, 60% of which were malicious or criminal attacks. This is a 712% increase in business notifications compared with the previous 12 months, which demonstrates the size of the security challenge.[1] These startling statistics highlight that effective security has never been more important to the Australian society (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 & Broer, 2010). Basic online security behaviours are not being practiced by Australians and small to medium business. While 73% use security software, 44% admitted to sharing passwords[2] at work. Most information security programs manage each security instance departmentally, e.g. the finance department is responsible for risk, 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 complicated and uses many different security models leading to duplication of resources, responsibility confusion and parts of the organisation being overlooked entirely (Roberti, 2001; Shariati, Bahmani, & Shams, 2011). An organisational security framework that includes all aspects of security – information, physical, technical process, people, cycles and risk – and has the flexibility of

[a] https://orcid.org/0000-0001-5658-6483
[b] https://orcid.org/0000-0003-0309-4332
[c] https://orcid.org/0000-0003-2501-1155
[d] https://orcid.org/0000-0003-0401-4197

[1] Office of the Australian Information Commissioner, Notifiable Data Breaches Scheme 12-month Insights Report, https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/ndb-scheme-12month-insights-report.pdf

[2] Last Pass 2017, *The Psychology of Passwords: Neglect is Helping Hackers Win*, available at: https://blog.lastpass.com/2018/05/psychology-of-passwords-neglect-is-helping-hackers-win.html/

McClintock, M., Falkner, K., Szabo, C. and Yarom, Y.
Enterprise Security Architecture: Mythology or Methodology?.
DOI: 10.5220/0009404406790689
In *Proceedings of the 22nd International Conference on Enterprise Information Systems (ICEIS 2020) - Volume 2*, pages 679-689
ISBN: 978-989-758-423-7

implementation to work with an organisation's budget, size and security mechanisms, could be used to mitigate these risks (Angelo, 2001).

We conduct an extensive review of existing security frameworks, 25 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 of existing security frameworks, a disjoint focus in either technical or policy, and a department or project focus for their implementation. Of those frameworks with a holistic approach, the most common framework methodology referenced was Enterprise Architecture (EA).

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, Bombosch, & Langade, 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 (Kreizman & Robertson, 2006). EA provides a methodology that reaches all parts of an organisation. 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.

An organisational security framework poses significant challenges and there is a lot of research that points to the importance and benefits of a holistic approach (R. Anderson, 2008). To test this, we use a Design Science Research study methodology to develop and evaluate a novel, fully researched enterprise security architecture (ESA) framework for organisations 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". 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.

2 LITERATURE REVIEW

We conduct a review of existing security frameworks to determine the effectiveness and we discover that coverage is not holistic, it is ineffective, and the only organisational model that is addressing whole-of-organisation approach is EA, however it is not applied effectively. As an example the most well-known and comprehensive ESA frameworks are the SABSA (Sherwood, Clark, & Lynas, 1995) and the TOGAF (Haren, 2011) however while the stated intent of the frameworks is holistic, the implementation is not. The SABSA model references the strategic mechanisms of EA, however it does not include EA in its elements and does not apply its framework to non-technical security. The focus in the implementation of security is low level technical system assets. The TOGAF is an EA framework that has created a security architecture as an optional tool. The principle of the TOGAF is to identify and implement security to only those parts of the organisation that need it rather than requiring security throughout an organisation. The implementations of the TOGAF are similar to the SABSA, both are effective technical frameworks.

To find existing security frameworks, we search Google Scholar and the ACM Digital Library database and we follow citations for articles about enterprise security architecture. Google search terms include 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'). Relevant works matching our inclusion/exclusion criteria are entered into EndNote X7.3.1 with the PDF as an attachment. The results are used for classification and analysis. The inclusion and exclusion criteria are determined based on the simplest version of an ESA framework. An ESA should have security, architecture and business as its focus. If the work is not a framework or security is not the focus, it is excluded. This is done to provide the broadest definition and therefore capture all relevant ESA frameworks developed since 1995.

From the analysis and review of all included 25 security models, we establish recommendations for guiding principles of an enterprise security

architecture. The review is guided by the following research question:

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

Through research of existing principles for the development of organisational security models, the four most referenced principles are drawn out. Our analysis shows the majority of the 25 frameworks satisfy a subset of these four identified principles and are discussed below:

1. The purpose of an effective framework should be to support the organisation's vision. Specifically, a security mechanism for all organisational assets is satisfied by six frameworks (Eloff & Eloff, 2005; Killmeyer, 2006; Organisation, 2013; Saleh & Alfantookh, 2011; Scholtz, 2006; Sherwood et al., 1995).
2. An internationally recognized standard should be used to provide a security assurance to the framework developed. From the framework reviews, the choices are ISO/IEC 27000 and NIST. 15 frameworks satisfy compliance to international security standards (J. A. Anderson & Rachamadugu, 2008; Atoum, Otoom, & Abu Ali, 2014; Bernroider, Margiol, & Taudes, 2016; Eloff & Eloff, 2005; Jeganathan, 2016; Korhonen, Yildiz, & Mykkanen, 2009; NIST;, OMB;, & FCIO, 2010; Rees, Bandyopadhyay, & Spafford, 2003; Reza Bazi, Hasanzadeh, & Moeini, 2017; Saleh & Alfantookh, 2011; Shen, Lin, & Rohm, 2009; Sun & Chen, 2008; Trcek, 2003; Wahe, 2011; Webb, Ahmad, Maynard, & Shanks, 2014).
3. The framework development should be based on EA. Use of an EA reference is indicated by eight frameworks (J. A. Anderson & Rachamadugu, 2008; Ertaul & Sudarsanam, 2005; Ho, 2002; Jeganathan, 2016; NIST; et al., 2010; Scholtz, 2006; Shen et al., 2009; Sherwood et al., 1995).
4. The development of an ESA framework should be a focus for the whole of the organisation, not just singular departments or assets. A holistic framework is demonstrated by 14 frameworks (J. A. Anderson & Rachamadugu, 2008; Atoum et al., 2014; Eloff & Eloff, 2005; Ho, 2002; Jeganathan, 2016; Killmeyer, 2006; Korhonen et al., 2009; Organisation, 2013; Posthumus & Von Solms, 2004; Scholtz, 2006; Shen et al., 2009; Sherwood et al., 1995; Wahe, 2011; Webb et al., 2014).

An important and critical issue that remains unaddressed is the development and critical review of an ESA that relies on all thoroughly researched principles. The principles we identify above 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". Table 1 is the list of frameworks we review and analyse.

Table 1: Existing security frameworks review.

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 relationships between each layer
(2002)	Ho	Security Management Framework	Theoretical
(2003)	Trcek	Information Systems Security Management Framework	Nine 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	Four Phases (Assess, Plan, Deliver, Operate)
(2004)	Posthumus, Von Solms	Information Security Governance Framework	Four Aspects (Legal, Business, Infrastructure, Standards)
(2005)	Ertaul, Sudarsanam	Enterprise Security Plan	Column 6 of Zachman (Why) replaced with "External Requirements and Constraints"

Table 1: Existing security frameworks review (cont.).

Year	Author	Framework Name	Notable Features
(2005)	Eloff, Eloff	Information Security Architecture	Five 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	Three-Layered Pyramid (Conceptual, Logical, Implementation)
(2008)	Anderson, Rachamadugu	Roadmap for Information Security Across the Enterprise	Three tiers (Profile, Plan, Protect)
(2008)	Sun, Chen	Intelligent Enterprise Information Security Architecture	Based on the seven layers of the Open Systems Interconnection (OSI) Reference Model
(2009)	Korhonen, Yildiz, Mykkanen	Service Orientated Architecture Security Governance Model	Four layers (Strategic, Tactical, Operational, Real-Time)
(2009)	Shen, Lin, Rohm	Enterprise Security Architecture Framework	Three noted dimensions - Framework, Policy and Technical
(2010)	NIST, OMB, FCIO	US Federal Enterprise Architecture Security and Privacy Policy	Three Stage Methodology - Identification, Analysis, Selection
(2011)	Saleh, Alfantookh	Information Security Risk Management Framework	Five domains (Strategy, Technology, Organization, People, Environment)
(2011)	TOGAF	Open Enterprise Security Architecture	Four dimensions (Program Management, Governance, Enterprise Architecture, Operations)
(2013)	ISO/IEC 27000	International Standard for Information Technology - Security	Fourteen 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 - four dimensions - security ambition, security process, resilience, business value
(2017)	Bazi, Hassanzadeh, Moeini	Cloud migration framework	A secure cloud computing framework using meta-synthesis - uses a seven stage maturity model

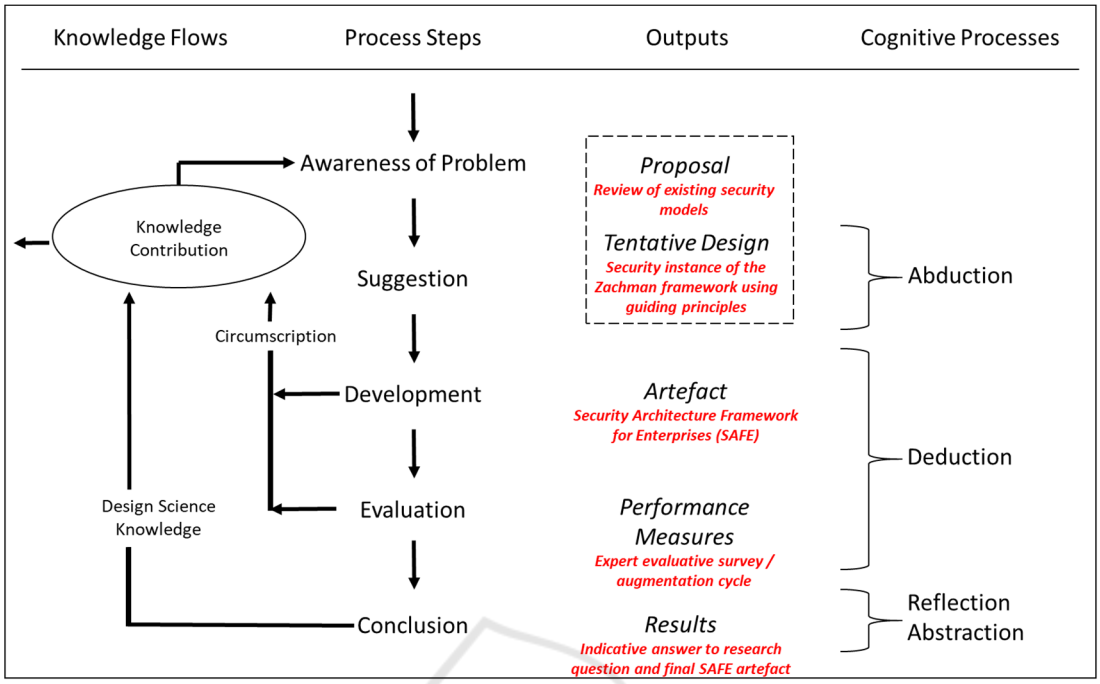

Figure 1: SAFE outputs in Design Science Research Cycle (Vaishnavi & Kuechler, 2004).

3 METHOD

A Design Science Research (DSR) study suited the research due to the emphasis on the design and creation of an artefact to test a research question (Venable, Pries-Heje, & Baskerville, 2016). The philosophy is constructivist, the approach is inductive and the choice of data analysis is qualitative using the grounded theory methodology to analyse a qualitative questionnaire.

Vaishnavi & Kuechler (2004) describe the body of DSR knowledge as man-made objects – artefacts – that are designed to meet specific goals. It creates novel contributions through the design of new artefacts 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 artefact. 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. For the purposes of this research, the kernel theory is Enterprise Architecture and the improvement of the theory is the security dimension design created strictly based on the foundational principles of Enterprise Architecture.

As indicated in Figure 1 there are five steps. We overlay our research (coloured red) onto the Outputs column to demonstrate our use of this methodology. The artefact discussed above is termed *the security architecture framework for enterprises* (or the framework) for the remainder of the paper.

4 ARTEFACT DESCRIPTION

Using the four principles identified in Section 2, the framework is developed from the Zachman framework 2013 Version 3.0 (Zachman, 1996) 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. 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. The following discussion provides an explanation of the rows and columns of the security framework.

4.1 Audience Perspectives / Stages of Reification (The Rows)

The perspectives in the Zachman framework constitute a complete way to build and view an organisation from the initial concept to the final

instantiation. Our security framework retains the rows of the Zachman framework with no changes.

Executive Perspective / Identification – The executive perspective is defined at the inception of a company, is the identification of the concept for the business and is externally focused.

Business Management Perspective / Definition – 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.

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.

Engineer Perspective / Specification – The requirements and specifications of the systems (detailed designs) of the organisation are designed at the engineering perspective.

Technician Perspective / Configuration – The technician perspective is the business component level implemented using specific tooling configurations.

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. At this stage of the framework, the artefacts are the actual organisation not the architectural abstractions like the previous five rows.

4.2 Classification Names (The Columns)

The columns of the framework are the English interrogatives and provide the detail of each row or organisational view. Where the differentiation for our security framework comes is the answer to the interrogative questions. All columns of the security framework are addressed by each having a related security question asked of the interrogative rather than the Zachman question. By doing so, the integrity of the Zachman is retained but the security instance is created. Table 2 shows the original Zachman framework interrogative definitions alongside the security framework definition.

4.3 Framework Development

Once the high-level categories are defined for each cell, the detail needs to be developed to explain what each cell actually means so the framework can be given to potential users for evaluation purposes. Figure 2 is an example of the instances of the cell definitions, we develop for all 36 cells. For all cells, a detailed research process is conducted to understand the original Zachman intent and develop authentic instances which results 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. Framework example – shows the use of the cell using a real-world example.
4. Compliance mapping to ISO 27000 and NIST.

In summary, our notional framework is completed and three layers of abstraction developed. The row / column categories, the detailed security definitions and the more detailed definitions (pictorial model, framework example and compliance mapping) for use by organisation for understanding. The final framework is compliant with the four guiding recommendations including compliant to NIST and ISO 27000 international security standards. Figure 3 is the completed Security Architecture Framework for Enterprises (SAFE).

5 EVALUATION

To test our design and evolve the conceptual framework, we share the framework and supporting documentation for critique with 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.

Table 2: Column definitions – English Interrogatives.

Interrogative	Zachman Definition	Security Framework 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.
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. Conceptual level security mechanisms are processes down to final level which are security technologies.
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.
Who – People	The responsibility assignments are allocated to the organisational stakeholders and can be internal or external.	Securing all organisational stakeholders, internal and external, through security responsibility assignment from Executive Management to Operational staff.
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.
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.

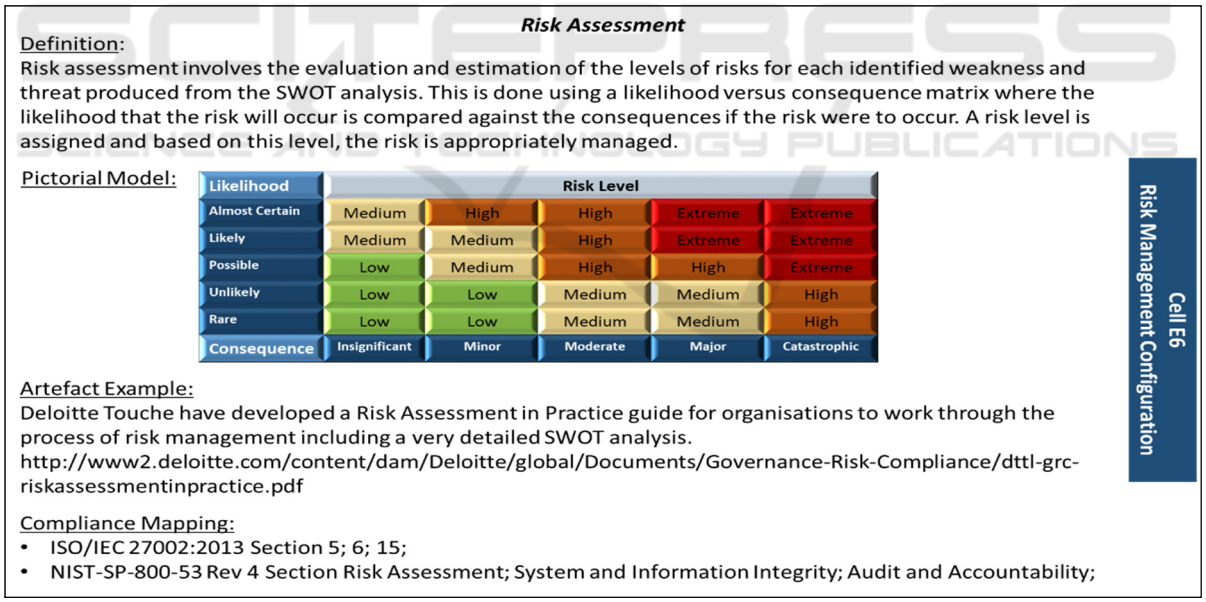

Figure 2: Cell E6 Risk Management Configuration (Risk Assessment).

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 design a questionnaire using an Oppenheim (2000) approach made up of five demographic questions – including security industry experience, job category, years of expertise; and 14 questions aimed at drawing out

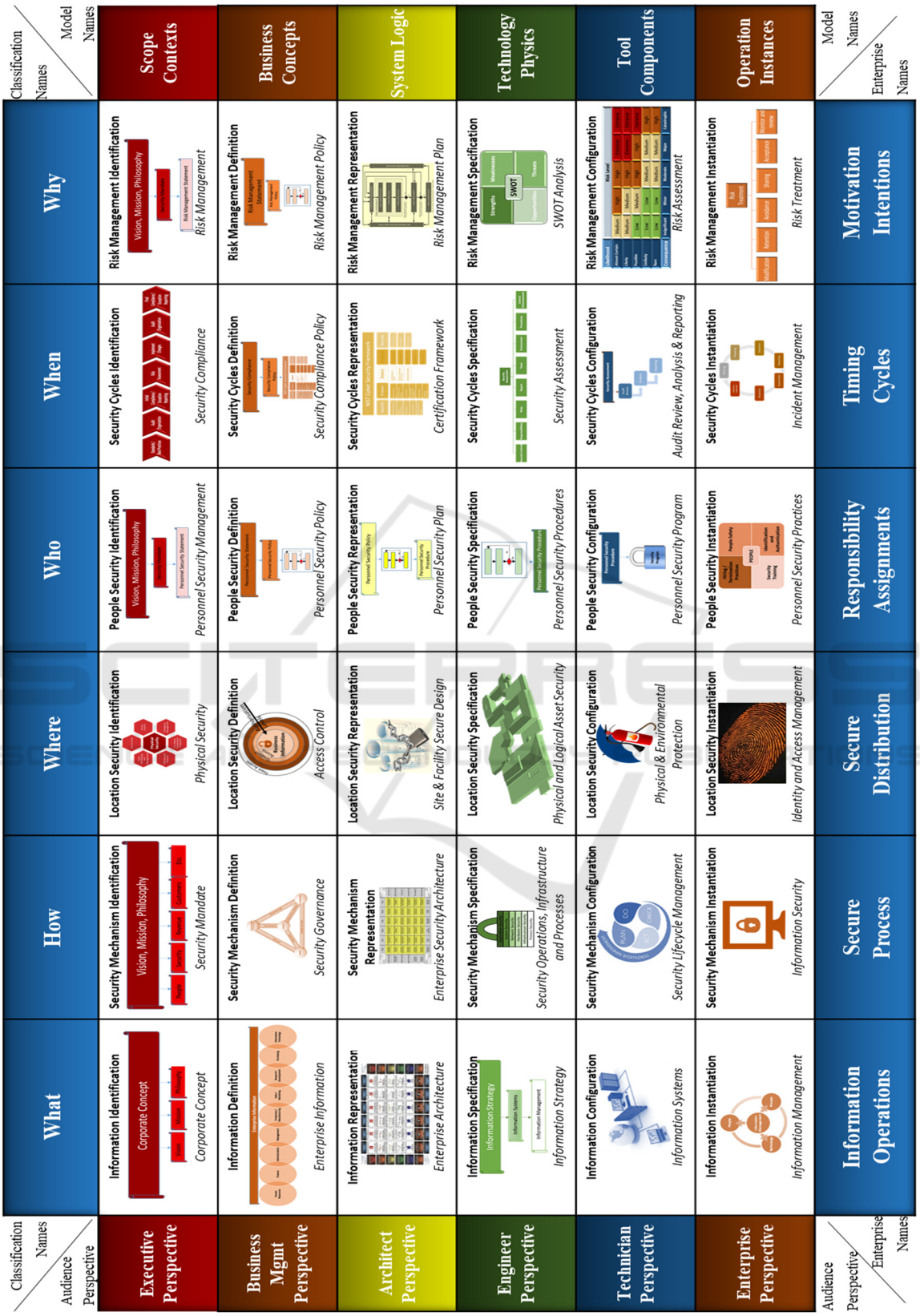

Figure 3: The Security Architecture Framework for Enterprise (SAFE).

selected aspects of the initial research question. Examples of the questions include:

- Do you believe a holistic approach to security is likely to provide a more secure organisation?
- What are the problems or challenges of the framework for an organisation using it?
- Does it help to have the categories broken down into organisational levels (rows)?

We use the inductive grounded theory method to analyse the results from our questionnaire about our framework. Grounded theory is a methodology by which qualitative analysis is iterative – the data (meaningful concepts from the text) are collected and separated from the conversation and each data unit is assigned codes. The codes are inspected for patterns and then reintegrated to form dominant thematic subjects and connections. (Starks & Brown Trinidad, 2007; Strauss & Corbin, 1994). Through the cyclical nature of the grounded theory methodology, each coding phase provides richer thematic results which are discussed below.

6 DISCUSSION

6.1 Demographic Results

We received 12 returned questionnaires, of which 75% of participants are employed by a large company (200+ employees), 17% are from a small (1–19 employees) and 8% from a medium (20–199 employees). 42% have security industry experience and 75% have been in their current role for more than ten years and consider themselves experts in the field. The participants come from Industry (58%), Government (33%) or the Military (8%) in roles such as management, security professionals, information technology professionals and researchers.

6.2 Framework Results

The questionnaire responses provide overall thematic characterisations of the framework and therefore indicative answers to the research question. The following discussion describes the overarching themes indicated though the qualitative analysis process and direct quotes from participants.

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 up 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 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 to 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 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 that although were not thematic are 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. Overall the feedback is supportive and comments from the participants include “definitions, artefacts, 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”.

7 CONCLUSIONS

In security, the whole is clearly greater than the sum of its parts and security has never been more important. The development of the concept 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 and processes, which will provide enterprise security management guidance to contemporary digitalised organisations of the 21st Century. The benefits of a holistic approach require all aspects of security to be considered and implemented based on the budget, size and mechanisms of the organisation, and provides a reduction in responsibility confusion and appropriate resourcing. We conducted a review of 25 security frameworks to determine if a fully researched and holistic security methodology would better provide security benefits to organisations than a piecemeal approach. The review indicated that there were very few frameworks that met the holistic test and therefore the research question could not be answered without a new framework being created. From the review, we took recommendations to guide the framework development – inclusion of all security mechanisms, compliant to international security standards, using EA as the foundation and organisationally holistic in its implementation.

We develop the Security Architecture Framework for Enterprises (SAFE) using the Design Science Research method. The framework is based on the John Zachman 2013 Version 3.0 and its layers of abstraction were developed with supporting documentation. The completed framework (Figure 3) is a 6 x 6 framework and each cell was defined using 1) a detailed explanation, 2) pictorial model, 3) framework example in the real world and 4) compliance mapping to ISO 27000 and NIST.

To determine the effectiveness of our framework in meeting security concerns, we shared the framework and supporting documentation with industry professionals using a questionnaire to evaluate. Our analysis of the questionnaire responses identified that the evaluation of the security framework indicates a positive correlation for the improvement of organisational security if a holistic design approach was applied.

To mature and evolve the design concept further there would be benefit from future work such as a larger design study, a user manual, a case study in a company or an organisational implementation study.

REFERENCES

Anderson, J. A., & Rachamadugu, V. (2008). *Managing security and privacy integration across enterprise business process and infrastructure.* Paper presented at the IEEE SCC.

Anderson, R. (2008). *Security engineering*: John Wiley & Sons.

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

Atoum, I., Otoom, A., & Abu Ali, A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security, 22*(3), 251-264.

Bente, S., Bombosch, U., & Langade, S. (2012). *Collaborative enterprise architecture: enriching EA with lean, agile, and enterprise 2.0 practices*: Newnes.

Bernroider, E. W., Margiol, S., & Taudes, A. (2016). *Towards a General Information Security Management Assessment Framework to Compare Cyber-Security of Critical Infrastructure Organizations.* Paper presented at the 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.

DiMase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions, 35*(2), 291-300.

Eloff, J., & Eloff, M. (2005). Information security architecture. *Computer Fraud & Security, 2005*(11), 10-16.

Ertaul, L., & Sudarsanam, R. (2005). *Security planning using Zachman framework for enterprises* Paper presented at the EURO mGOV 2005

Gorazo. (2014). Enterprise Architecture Literature Review.
Haren, V. (2011). *TOGAF Version 9.1*: Van Haren Publishing.
Ho, L. (2002). Security Management Framework: A New Approach based on John Zachman's Framework for Enterprise Architecture.
Jeganathan, S. (2016). Enterprise Security Architecure.
Killmeyer, J. (2006). *Information security architecture: an integrated approach to security in the organization*: CRC Press.
Korhonen, J. J., Yildiz, M., & Mykkanen, J. (2009). *Governance of information security elements in service-oriented enterprise architecture.* Paper presented at the ISPAN 2009.
Kreizman, G., & Robertson, B. (2006). Integrating Security Into the Enterprise Architecture Framework. In: Stamford CT: Gartner Inc.(G00137069).
Luhach, A. K., & 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), 395.
NIST, OMB, & FCIO. (2010). Federal Enterprise Architecture Security and Privacy Profile V3.
Oppenheim, A. N. (2000). *Questionnaire design, interviewing and attitude measurement*: Bloomsbury Publishing.
International Standards Organisation, (2013). I.S.O./I.E.C. 27000, 27001 and 27002 for information security management.
Patterson, T. (2003). Holistic Security: Why Doing More Can Cost You Less and Lower Your Risk. *Computer Fraud & Security*(6), 13-15.
Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security, 23*(8), 638-646.
Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES: a policy framework for information security. *Communications of the ACM, 46*(7), 101-106.
Reza Bazi, H., Hasanzadeh, A., & 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., & Broer, J. (2010). Why Two Thirds of Enterprise Architecture Projects Fail. *ARIS Expert Paper*.
Saleh, M. S., & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied computing and informatics, 9*(2), 107-118.
Sandhu, R. (2000). *Engineering authority and trust in cyberspace: The OM-AM and RBAC way.* Paper presented at the ACM RBAC 2000.
Scholtz, T. (2006). Structure and Content of an Enterprise Information Security Architecture. *Gartner Inc*.
Shariati, M., Bahmani, F., & Shams, F. (2011). Enterprise information security, a review of architectures and frameworks from interoperability perspective. *Procedia Computer Science, 3*, 537-543.
Shen, Y. T., Lin, F., & Rohm, T. (2009). A Framework for Enterprise Security Architecture and Its Application in Information Security Incident Management. *Communications of the IIMA, 9*(4), 8-20.
Sherwood, J., Clark, A., & Lynas, D. (1995). Enterprise security architecture. *SABSA White Paper2009*.
Starks, H., & Brown Trinidad, S. (2007). Choose your method: A comparison of phenomenology, discourse analysis, and grounded theory. *Qualitative health research, 17*(10), 1372-1380.
Strauss, A., & Corbin, J. (1994). Grounded theory methodology. *Handbook of qualitative research, 17*, 273-285.
Sun, J., & Chen, Y. (2008). *Intelligent Enterprise Information Security Architecture Based on Service Oriented Architecture.* Paper presented at the FITME 2008.
Trcek, D. (2003). An integral framework for information systems security management. *Computers & Security, 22*(4), 337-360.
Vaishnavi, V., & Kuechler, W. (2004). Design research in information systems.
Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: a framework for evaluation in design science research. *European Journal of Information Systems, 25*(1), 77-89.
Wahe, S. (2011). Open Enterprise Security Architecture - A Framework and Template for Policy-Driven Security.
Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security, 44*, 1-15.
Zachman, J. A. (1996). The framework for enterprise architecture: background, description and utility. *Zachman International*.