UNIVERSITY OF SOUTHAMPTON

FACULTY OF PHYSICAL SCIENCES AND ENGINEERING

Electronics and Computer Science

The Viable System Model for Information Security Governance

by

Ezzat Hamed Alqurashi

Thesis for the degree of Doctor of Philosophy in Computer Science

June 2015

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF PHYSICAL SCIENCES AND ENGINEERING

Electronics and Computer Science

Doctor of Philosophy

The Viable System Model for Information Security Governance

Ezzat Hamed Alqurashi

Information security governance (ISG) has emerged as a new information security (IS) discipline and is considered one of the critical areas of research for enhancing the viability of organisations. This research proposes a viable system model (VSM) for ISG (VSMISG) and investigates its effects. The investigation involves studying the effects of the VSMISG in small, medium and large organisations facing low, medium and high security threat intensity over different time scales. This study also analyses the costs and benefits of changing from the baseline ISG model to the VSMISG.

From reviewing the literature, the VSM was identified and redefined for the context of ISG. A preliminary study was conducted to confirm the appropriateness of the VSM for ISG. This employed a questionnaire survey of eleven highly experienced IS experts and the inter-rater agreement among them was analysed. The time taken by the governance level of IS to identify strategic security crises (SSC) that affect organisations' viability was used for the investigation in the baseline ISG model and the VSMISG. Conceptual models were designed and simulation models developed using the discrete-event simulation approach for representing the baseline ISG model and the VSMISG. The IS incident management guidance embodied in the international standard BS ISO/IEC 27035 was adopted to represent the IS operations part in the baseline ISG model and the VSMISG. The chi-square and autocorrelation tests were used to test the random number generator of the Simul8 simulation software.

This research presents a VSM for ISG whose components are rated as 'important' and 'very important' and there was fair agreement among the experts on this rating. Using the VSMISG in small, medium, and large organisation leads to swifter identification of SSC than under the baseline ISG model, enhancing organisations' viability. Small organisations take the longest time to identify SSC, especially when the security threat intensity is high, while large organisations take the least time in all cases. The benefits of changing from the baseline ISG to the VSMISG outweigh the costs, and they are expected to be seen from early in the first year of implementation.

The VSM for ISG proves its vital role in enhancing viability at all organisation sizes. Decision makers in small organisations need to increase the number of IS staff to cut the time taken to identify SSC in order to enhance their viability. Implementing the VSMISG saves organisations a tremendous amount of money.

Contents

List of Tables

List of Figures

Declaration

I, Ezzat Alqurashi, declare that this thesis entitled 'The Viable System Model for Information Security Governance' and the work presented in it are my own and has been generated by me as the result of my own original research. I confirm that:

1. This work was done wholly or mainly while in candidature for a research degree at this University;

2. Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;

3. Where I have consulted the published work of others, this is always clearly attributed;

4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;

5. I have acknowledged all main sources of help;

6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;

7. Part of this work has been published as:

> Alqurashi, E., Wills, G., & Gilbert, L. (2013). A viable system model for information security governance: Establishing a baseline of the current information security operations system. In *Security and Privacy Protection in Information Processing Systems* (pp. 245–256). Springer: Berlin Heidelberg.

Signed:

Date:

Acknowledgements

I am so grateful to Allah for the guidance, good health and wellbeing necessary to complete this work.

I am also grateful to my father (may Allah bless his soul) and my mother for helping and supporting me in shaping and undertaking my postgraduate studies, and for their prayers and encouragement.

I would like also to extend my gratitude to my loving family, with special thanks to my wife and my children for their understanding and support through all the stages of this research, for travelling with me far away from home, and for creating the settled atmosphere that I enjoy.

I wish to express my sincere thanks to my supervisors, Gary Wills and Lester Gilbert, for their help and wonderful supervision. Their valuable ideas, guidance and discussions were the drivers and motivations behind the completion of this work.

I place on record my gratitude to the Saudi Ministry of Education for granting me both the scholarship and the opportunity to pursue my PhD study.

Definitions and Abbreviations

BS ISO/IEC	British Standards- International Organisation for Standardisation and the International Electrotechnical Commission
CBA	Cost–Benefit Analysis
CEO	Chief Executive Officer
CGTF	Corporate Governance Task Force
CIO	Chief Information Officer
ERGO	Ethics and Research Governance Online
IRR	Internal Rate of Return
IS	Information Security
ISG	Information Security Governance
ISIRT	Information Security Incident Response Team
ISM	Information Security Management
IT	Information Technology
ITGI	Information Technology Governance Institute
NPV	Net Present Value
PDF	Probability Density Function
PoC	Point of Contact
RNG	Random Number Generator
SSC	Strategic Security Crises
VSM	Viable System Model
VSMISG	Viable System Model for Information Security Governance

Note	
We	For ease of expression and for directness, I use “we” extensively. Nowhere does this device imply joint or co-authority

Chapter 1 Introduction

Information security (IS) has evolved in step with the increasing complexity of its diverse environments. During the past decade, Information Security Governance (ISG) has emerged as a new information security discipline in response to new laws and regulations aiming to counter evolving security challenges (von Solms 2006). Boards of directors and executive management have become accountable for the effectiveness of the internal controls of their corporation's information security. Adopting a framework is considered an essential starting point in securing information systems, complying with regulations, and increasing the efficiency of business processes (Entrust 2004). Therefore, corporations and organisations need a framework to govern their information security (Corporate Governance Task Force 2004; Entrust 2004; Posthumus & von Solms 2004).

Against this background, a number of researchers and organisations have proposed various ISG frameworks and models. The Corporate Governance Task Force (2004) has provided guidance in the development and implementation of an organisational ISG structure including recommendations for the responsibilities of members of organisations. Posthumus and von Solms (2004) have defined two structure levels—information security governance and information security management—for dealing with business information risk at a corporate governance level. Von Solms and von Solms (2006) have proposed an ISG model based on the principle of Direct Control Cycle over three levels of structure: governance; management; and operation. The Information Technology Governance Institute (ITGI 2006) has provided guidance for boards of directors and executives on the development and maintenance of information security programmes. Da Veiga and Eloff (2007) have identified a list of information security components mapped to three levels of structure: strategic; managerial and operational; and technical, in order to approach ISG from a holistic perspective. Recently, Ohki et al. (2009) have identified functions and interfaces of ISG between stakeholders, auditors, executives and managers.

The organisational information security is relatively new and under-researched domain. Nonetheless, it may be considered as one of the critical areas of research necessary for maintaining organisations' viability (Kotulic & Clark 2004). Vinnakota (2011) stated that there is a growing emphasis on the need for systemic models of ISG

to deal with the dynamic nature of today's changes and organisational complexity. According to Gokhale and Banks (2002), the Viable System Model (VSM) provides a promising route for exploration to counter the increasing level of threat and meet the need for rapid response at the organisational level.

Although much work has been undertaken to date, more studies are needed to provide a systematic ISG model that enhances organisational viability. According to Corporate Governance Task Force (2004), irrespective of size or form, organisations use internal controls to manage and direct. The effects of the ISG model that enhance organisational viability need to be investigated at different organisation sizes and levels of security threat intensity over different time scales to ensure performance consistency. The purpose of this research is to provide a systematic ISG model that enhances organisational viability, to investigate its effects at different organisation sizes, levels of security threat intensity and over different time scales, and to analyse it financially.

1.1 Research Questions

To fulfil the purposes of this research, we defined the research questions as follows:

RQ1 What are the components of ISG that enhance organisational viability?

Current ISG frameworks and models identify many ISG components to ensure better management of organisational internal controls and performance. However, none of these studies identify ISG components specifically to enhance an organisation's viability. Identifying the viability components of information security governance plays a vital role in ensuring organisational survival. This research question aims to identify the viability components of ISG that ensure not only the effectiveness of internal controls but the viability of organisations. Chapter 3 provides a VSM for ISG (abbreviated to VSMISG), identifying the components that enhance an organisation's viability and answer this research question:

RQ2 What is the importance of the VSM's systems and principles to ISG?

This research question aims to determine the importance of the VSM components to the ISG. Determining the importance of the viability components to ISG confirms the

appropriateness of using these components in the ISG domain and allows further studies and investigations of these components to take place.

RQ3 To what extent do information security experts agree on the importance of the VSM's principles and systems to ISG?

This research question aims to determine the degree of agreement among the evaluators (IS experts) on the importance of the VSM's components to ISG. Determining the extent of agreement shows whether there is consensus or variation. Consensus among IS experts would suggest a high level of trust in determining the importance of the VSM's components to ISG; that is, not randomly identified.

RQ4 Does the VSMISG have significant effects on the time taken to identify strategic security crises that affect organisational viability?

In current ISG practice, Strategic Security Crises (SSC) that affect organisational viability and that require immediate response from the governance level of IS are reported through routine communication channels, causing delay in dealing with emergency situations. The aim of this research question is to investigate the effects of the VSMISG on the time to identify SSC. Reducing the time to identify SSC leads to faster response and an enhancement of the viability of the organisation.

RQ5 Are the effects of the VSMISG related to organisation size?

The VSMISG may have different effects on different-sized organisations. The aim of this research question is to investigate the effects of the VSMISG on a small, medium and large organisation. This is to examine whether the effects of the VSMISG depends on the size of the organisation.

RQ6 Are the effects of the VSMISG related to the intensity of security threat?

The VSMISG may have different effects according to changes in the intensity of security threat. The aim of this research question is to investigate the effects of the VSMISG when facing low, medium and high security threat intensities to examine whether the effects of the VSMISG depends on the intensity.

RQ7 Are the effects of the VSMISG related to different time scales?

The VSMISG may have different effects according to changes in the time taken to deal with SSC. The aim of this research question is to investigate the effects of the VSMISG at different time scales to examine whether these depend on changes in time scales.

RQ8 Is using the VSMISG more beneficial than using the current ISG model?

Current ISG models report SSC to the governance level of IS through routine communication channels, causing delays that may have a severe impact on organisational economics. This research question aims to investigate the economic aspects of using the VSMISG. The answer shows the costs and benefits of the VSMISG and baseline ISG model and whether changing from the baseline ISG model to the VSMISG is beneficial.

1.2 Contributions

This thesis provides a viable system model for information security governance and investigates its effects in a small, medium and large organisation, at low, medium and high threat intensities over different time scales. In more detail, the state of the art will be extended by the key contributions of this research over its methodology and findings as follows:

1- We provide a viable system model for information security governance based on the redefined principles and systems of the viable system model.

2- We confirm the importance of the viable system model for information security governance by surveying the opinions of IS experts.

3- We provide an original development of the BS ISO/IEC 27035 standard by designing three information security management systems on top of the information security operations system, namely the control, planning and policy systems, to yield the VSMISG.

4- We investigate the effects of the VSMISG in a small, medium and large organisation under, low, medium and high security threat intensities, and in different time scales, fixed and variable.

5- We investigate the costs and benefits of using the current ISG model versus the VSMISG.

1.3 Structure of the Thesis

This thesis is divided into eight chapters. A description of the content of each chapter is given as follows.

Chapter 2 describes the current trends in information security governance, reviews the current information security governance frameworks and models, and identifies the ISG components. It ends by summarising the current ISG components in the literature.

Chapter 3 introduces the theory of the viable system model, which will serve as the theoretical underpinning of the study. It then redefines the viability components of the VSM for information security governance and provides a viable system model for information security governance (VSMISG). It then goes on to confirm the appropriateness of the VSM for ISG by surveying the opinions of IS experts and determining the level of agreement among them. The chapter ends by determining that emergency direct reporting is the viability component by which the effects of the VSMISG will be investigated in this study.

Chapter 4 presents the research methods for constructing the environment for investigating the effects of the VSMISG in a small, medium and large organisation, at low, medium and high threat intensities, and in different time scales. It presents the design of the baseline ISG and the VSMISG conceptual models. It then presents the developments and the validation of the baseline ISG and VSMISG simulation models, going on to test the random number generator of the simulation software used for the investigation to ensure its randomness.

Chapter 5 details the experiment design and the methodology for investigating the effects of the VSMISG. It then presents the results of the experiment and its analysis.

Chapter 6 investigates the economic aspects of using the baseline ISG model and the VSMISG. It defines and calculates the costs and benefits for each model and

analyses them. It ends by presenting the results that determine the costs and benefits of changing from the baseline ISG model to the VSMISG.

Chapter 7 discusses the findings of the research. It discusses the results of determining the importance of the VSMISG and the results of the inter-rater agreement analysis among the IS experts. It then discusses the results of investigating the effects of the VSMISG. It goes on to discuss the results of the cost–benefit analysis of the baseline ISG and VSMISG models. It ends by identifying the main limitations of the study.

Chapter 8 summarises the work conducted in this research. It presents the research findings centred on the research questions and defines a number of interesting future works. The chapter concludes by shedding light on the key outcomes of this research.

Chapter 2. Review of Information Security Governance: Realisation and Development

A literature review has three important purposes (Weissberg & Buker 1990): the first is to establish the background of the researcher's study; the second is to identify the important studies in related areas; and the third is to establish the position of the study by linking it to relevant research and expanding it by extending the state of the art in a particular domain.

ISG literature shows that there are two trends in this area, as follows:

1. The realisation of ISG
2. The implementation of ISG.

ISG is the link between information security and corporate governance, showing the benefits and needs, and its application is the introduction of various types of frameworks and models.

2.1 Realisation of Information Security Governance

Information security is a multi-dimensional discipline that needs an appropriate level of management to direct and control every department and person in the organisation. So far it has only been tackled technologically, as it has been considered a technical issue and, therefore, has been the responsibility of IT departments (Business Software Alliance 2003; von Solms 2001). However, the relevant challenges cannot be dealt with by relying only on Chief Information Officers (CIOs) (Mears & von Solms 2004; CGTF 2004).

Although often viewed as a technical issue, information security is also a governance challenge that involves risk management, reporting and accountability (CGTF 2004; ITGI 2006; Entrust 2004). According to Posthumus and von Solms (2004), it should be a priority for executives, including the Board and the CEO, and therefore be the responsibility of corporate governance. They highlighted the need to integrate it into corporate governance through the development of ISG framework (Posthumus & von Solms 2004).

To achieve effectiveness and sustainability in today's complex, interconnected world, security of information assets must be addressed at the highest levels of the organisation, not regarded as a technical specialty and relegated to IT departments. Effective security requires the active involvement of executives to assess emerging threats and the organisation's response (ITGI 2006); indeed, several sources such as Corporate Governance Task Force (CGTF) (2004), Entrust (2004), Business Software Alliance (2003), Posthumus and von Solms (2004) and von Solms (2006) assert that information security management should be directed and controlled by the executive management and board of directors. The CGTF calls on organisations to generate awareness of the need to treat information security as governance issue and then to make it a priority (CGTF 2004). The governance of information security domain is a relatively new and under-researched area, yet it may become one of the most critical areas of research for enhancing organisations' viability (Kotulic & Clark 2004).

Executive management and boards began to realise that ISG was becoming their direct responsibility and that serious personal consequences, specifically legal, could arise from ignoring it (von Solms & von Solms 2005). Relevant aspects include accountability to shareholders, compliance with legal requirements, planning security policies effectively, spearheading security awareness and education, defining roles and responsibilities within the organisational structure, contingency planning and instituting of best practice standards (Mears & von Solms 2004).

ISG has become an important business responsibility, and the issue of accountability has risen to board level. According to the CGTF, 'Corporate Governance consists of the set of policies and internal controls by which organisations, irrespective of size or form, are directed and managed. Information security governance is a subset of organisations' overall governance program'. ISG is an essential component of a successful organisational management and is the responsibility of the board of directors and senior executives (CGTF 2004; ITGI 2006; von Solms 2006).

2.2 Information Security Governance: Frameworks and Models

A number of ISG frameworks and models have been introduced in the literature defining many aspects, structures, components, roles and responsibilities, and principles of ISG. This section provides a brief description of the current ISG frameworks and models.

2.2.1 ISG framework by Corporate Governance Task Force

The CGTF was formed in 2003 to develop a governance framework to drive the implementation of effective information security programmes. It defined a framework covering the following areas:

- Roles and responsibilities of the board of directors/trustees
- Roles and responsibilities of the senior executives
- Roles and responsibilities of the executive team members
- Roles and responsibilities of senior managers
- Responsibilities of all employees and users
- Organisational unit security programmes
- Organisational unit reporting
- Information security programme evaluation.

The framework makes recommendations for members' roles and responsibilities at all organisational levels. It specifies that each organisational unit should develop and evaluate its own security programme and report on its effectiveness to top management (CGTF 2004).

2.2.2 Governance and Management Strategy

Posthumus and von Solms (2004) propose a framework comprising two levels: ISG and Information Security Management (ISM). The ISG side, including the board of directors and executive management, directs the organisation by formulating the strategy, mission, vision and policy of information security. It controls information security efforts by requiring periodic reports from various department heads to show the

effectiveness of their security plans. The ISM side is concerned with how to meet the security requirements with assistance of conventional security codes of practice such as BS 7799 (1999). The framework identifies internal and external factors that may have an impact on information security such as business issues, IT infrastructure, standards, best practices, and legal and regulatory matters.

2.2.3 ISG Framework Based on a Holistic Perspective

Da Veiga and Eloff (2007) introduced a framework based on the evaluation of four approaches to define a holistic perspective toward ISG. There are three levels of management in the framework: strategic; managerial and operational; and technical. Each features one or more of the six categories of common components identified in these approaches, with a number of information security components:

- Strategic
  - Leadership and governance
- Managerial and operational
  - Security management and organisation
  - Security policies
  - Security programme management
  - User security management
- Technical
  - Technology protection and operations.

The framework includes change management, as this influences the six identified categories.

Figure 2-1 shows the information security governance framework from a holistic perspective.

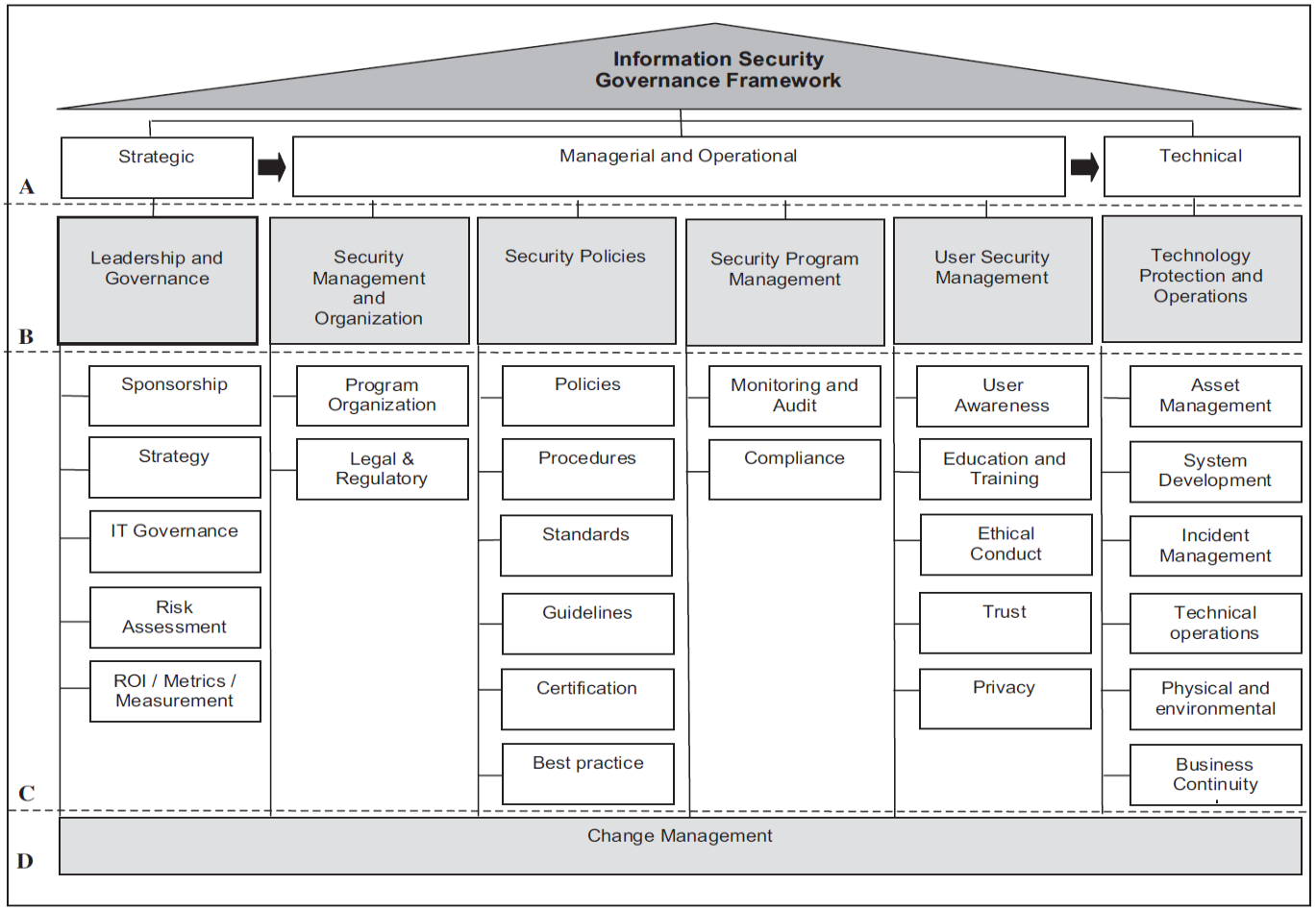


Figure 2-1: Information security governance framework, based on a holistic view (from Da Veiga & Eloff 2007)

2.2.4 Guidance for Boards of Directors and Executive Management

The Information Technology Governance Institute (ITGI 2006) proposed a framework to guide the development and maintenance of a comprehensive information security programme. This identifies eight points for achieving effective ISG:

1. Organisational security structure
2. Business and IT security strategy
3. Risk management methodology
4. Information value security strategy
5. Security policies
6. Security standards
7. Monitoring processes
8. Continuous evaluation process.

2.2.5 ISG Based on Direct-Control Cycle

Von Solms and von Solms (2006) proposed a model based on two principles for governing information security. The first identifies three actions: direct; execute; and control. The second identifies three management levels: strategic; tactical; and operational. The strategic level starts the direct process by defining the importance of protecting the information assets in its vision. The tactical level should align to the strategic vision of information security by formulating appropriate information security policies, organisation standards and procedures. The operational level defines administrative guidelines and procedures. Figure 2-2 shows the information security governance model based on the direct-control cycle.

The control process depends on the characteristic of ‘measurability’, that is, no statement of information security policies or strategic directives should be formulated unless measurable. The operational level collects measurement data electronically from the log files of various resources, then reports them to the tactical level. Other data that cannot be collected electronically are collected through questionnaires, interviews and inspections. The tactical level then integrates all the received data to determine the level of compliance against the defined policies, standards and procedures, then the strategic

level receives compliance reports on relevant directives that need to reflect relevant risks.

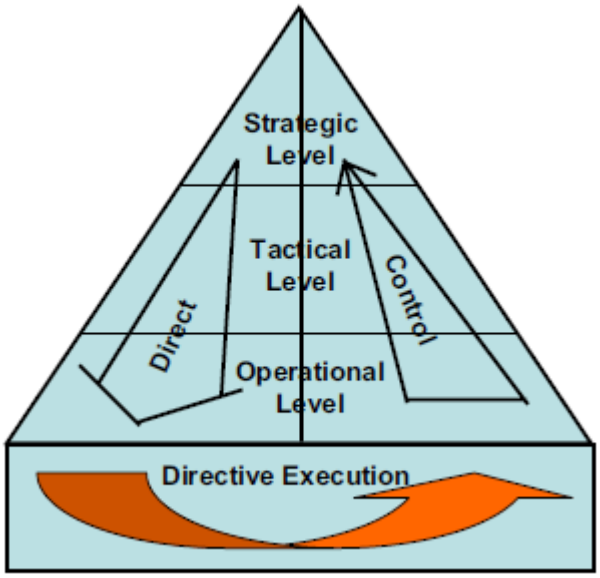


Figure 2-2: Information security governance based on direct-control cycle (from von Solms & von Solms 2006)

2.2.6 ISG Functions and Interfaces

Ohki et al. (2009) introduced a framework identifying five ISG functions: direct; monitor; evaluate; report; and oversee. It identifies four interfaces between stakeholders, auditors, executives and managers. Executives perform the first four functions, while auditors have oversight. Executives direct the management of information security, monitor information security management practice and security incidents, evaluate results against defined goals, and report security issues and activities to stakeholders. Auditors oversee executives' activities relating to information security. Figure 2-3 shows the functions and interfaces of information security governance framework.

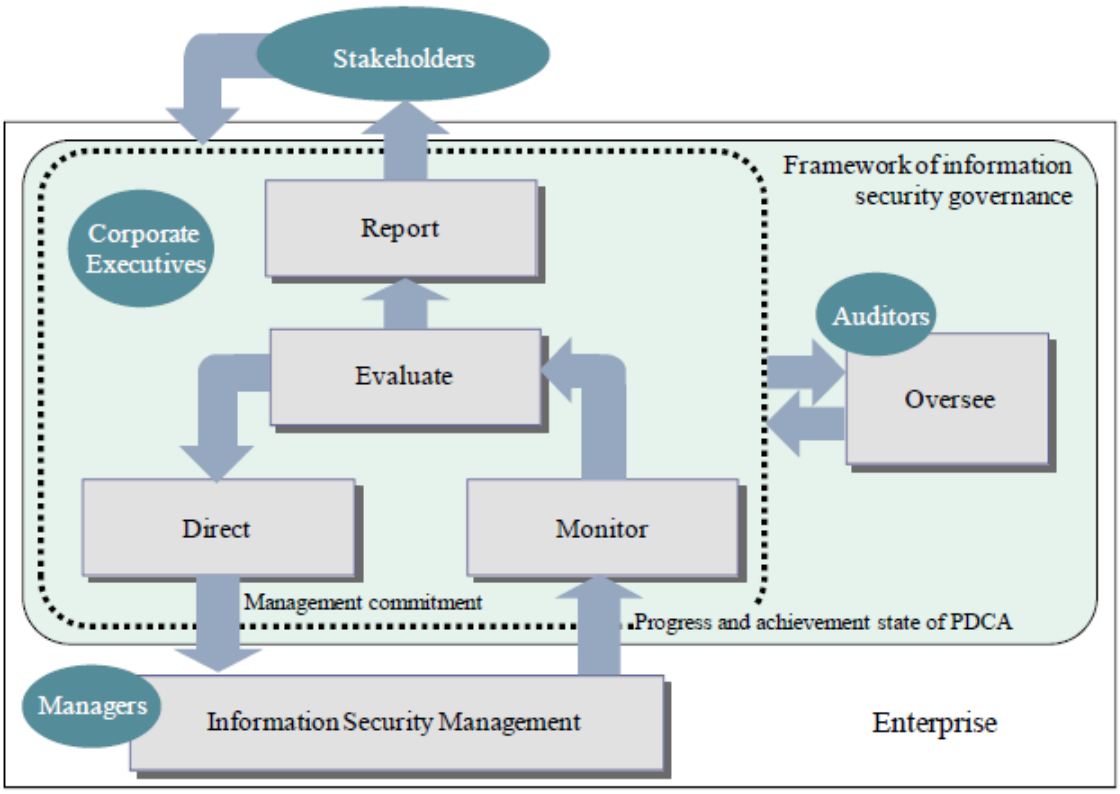


Figure 2-3: ISG functions and interfaces (from Ohki et al. 2009)

2.3 Summary

This chapter reviewed the literature and provided a description of the current state of the art of ISG frameworks and models. It showed how the ISG started and developed. Current frameworks and models cover a broad range of ISG components and aspects including roles and responsibilities, reporting, information security organisation structure and programmes, resources, principles, functions and other components. Table 2-1 illustrates the current ISG components.

Despite considerable work on identifying various ISG components and aspects, little work has been undertaken to define the ISG components that enhance an organisation's viability. There is a need to do so.

Table 2-1: Components of current ISG frameworks and models, from literature review

Source	Components of ISG frameworks and models
Corporate Governance Task Force (CGTF), 2003	• The roles and responsibilities of board of directors, trustees, senior executives, executive team members, senior managers, employees and users • Organisational unit security programme • Organisational unit reporting, and • Information security program evaluation.
Posthumus & von Solms, 2004	• Information security governance: board of directors and executive management, strategy, mission, vision, policy, and evaluation • Information security management: information security standard BS 7799 (1999) • Internal and external factors: business issues, IT infrastructure, standards, best practices, and legal and regulatory matters.
Information Technology Governance Institute (ITGI), 2006	• Organisational security structure, business and IT security strategy, risk management methodology, information value security strategy, policies, standards, monitoring processes and continuous evaluation process.
von Solms & von Solms, 2006	• Information security structure: strategic (vision), tactical (policies, standards and procedures) and operational (administrative guidelines and procedures), • Information security governance principles: direct, control, execute, and reporting.
Da Veiga & Eloff, 2007	• Leadership and governance: sponsorship, strategy, IT governance, risk assessment and ROI/metrics/ measurements • Security management and organisation: programme organisation, legal and regulatory • Security policies: policies, procedures, standards, guidelines, certification and best practice • Security programme management: monitoring and audit, and compliance • User security management: user awareness, education and training, ethical conduct, trust and privacy • Technology protection and operations: asset management; system development; incident management; technical operations; physical and environmental; and business continuity.
Ohki et al., 2009	• Information security governance functions: direct; monitor; evaluate; report; and oversee • Interfaces: stakeholders; auditors; executives; and managers.

Chapter 3. Viable System Model for Information Security Governance

A number of ISG frameworks and models were presented in the literature review identifying ISG components. However, there was little literature on those that enhance organisation viability. Therefore, one of the main objectives of this study is to explore the domain of information security governance and to identify components that work together to do so.

This chapter introduces the Viable System Model (VSM), redefined as VSM for Information Security Governance (ISG). VSM consists of principles and systems working together to enhance organisation viability. It describes them and reviews their appropriateness by means of a rating by eleven information security experts on their importance to ISG. The level of agreement among these experts is revealed on the importance of the VSM systems, principles, and systems and principles (combined) for ISG, before the chapter concludes by identifying the focus of this research.

By the end of this chapter, the following research questions will be answered:

RQ1 *What are the components of ISG that enhance organisational viability?*

RQ2 *What is the importance of the principles and systems of the viable system model to information security governance?*

RQ3 *To what extent do information security experts agree on the importance of the viability system model's principles, systems, and principles and systems (combined)?*

3.1 Viable System Model

Stafford Beer introduced the VSM as a blueprint for designing the communication and control aspects of viable systems. Beer described it in *Brain of the Firm* (1972), then developed it in *The Heart of Enterprise* (1979) and *Diagnosing the System for Organisations* (1985). The VSM is a model from cybernetics for an organisational structure based on that of the human nervous system (Beer 1981) and concepts that contribute to systems viability. Beer's model of viable organisations includes

governance functions and roles such as creating identity, defining values and purpose, setting direction, steering and providing resources (Davies 2002).

Cybernetics is fundamental to the operation of control systems. It looks at how information is communicated between the environment and a machine or organism, or between component parts. In computers, any program that changes its behaviour in response to new data might be called cybernetic. Cybernetics is relevant to a variety of fields in computer science that involve machine learning or reasoning (Henderson 2003).

The background of the VSM consists of common concepts between artificial intelligence, a branch of computer science, and cybernetics such as control, feedback, environment and communication. As governance and cybernetics both concern 'control' (Lewis & Millar 2009), redefining the VSM developed within the field of cybernetics for information security governance may prove a useful contribution to the field of ISG.

Beer (1985) claimed that an organisation can be viable, that is, will survive and be effective, if constructed according to five main management systems, referred to as S1 to S5: operations; coordination; control; planning (intelligence); and policy. In this report, these will be referred to as #1 to #5 when referencing ISG. Beer identified a function of the control system as monitoring the performance of the operations system: compliance monitoring. The systems are interconnected by communication channels or information flows.

In addition, Beer argued that an organisation will survive if based on five principles: autonomy; emergency direct reporting; recursion; requisite variety; and viability. Figure 3-1 shows the VSM of these five systems, a function, and the environments with which it interacts. These are explained in the following sections.

.

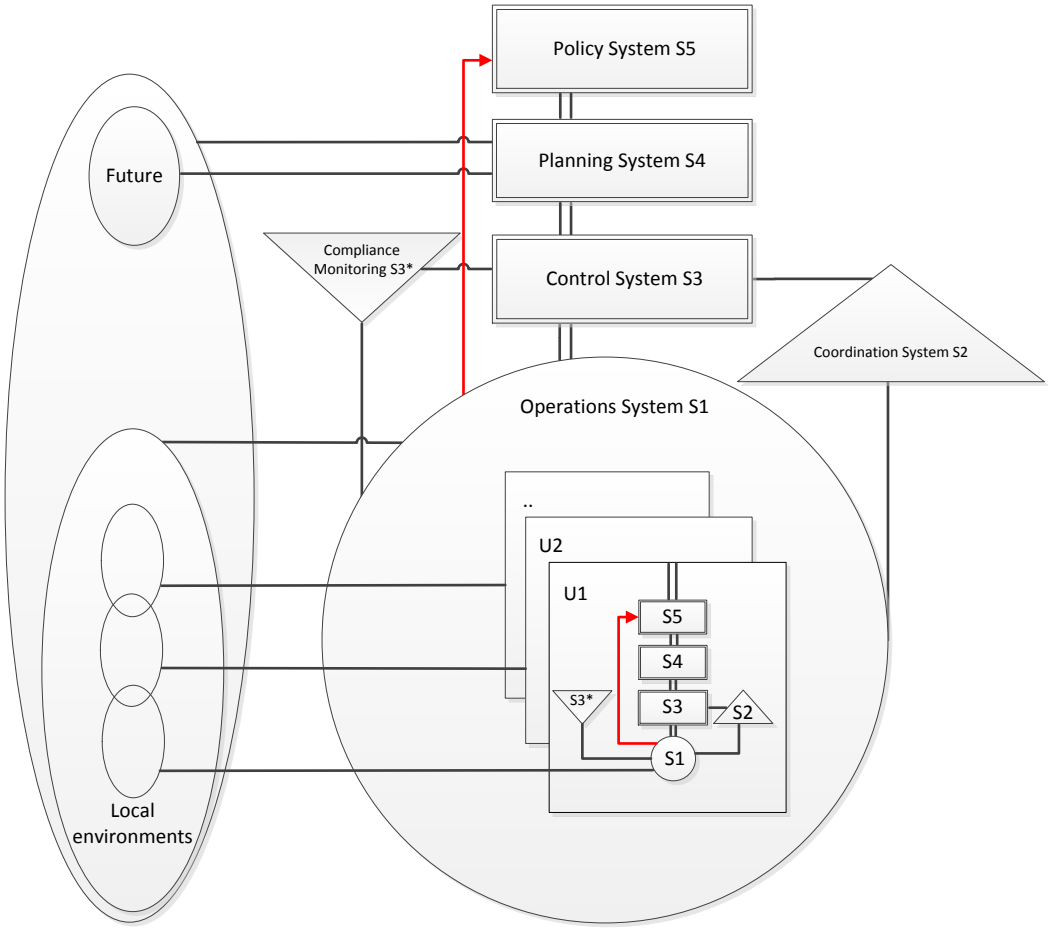


Figure 3-1: VSM

3.2 A Viable System Model for Information Security Governance

This section proposes an ISG model based on the VSM, as shown in Figure 3-2. The proposed VSMISG consists of five viable systems and a function, based on five principles. The following sections describe the design process and the components of the VSMISG.

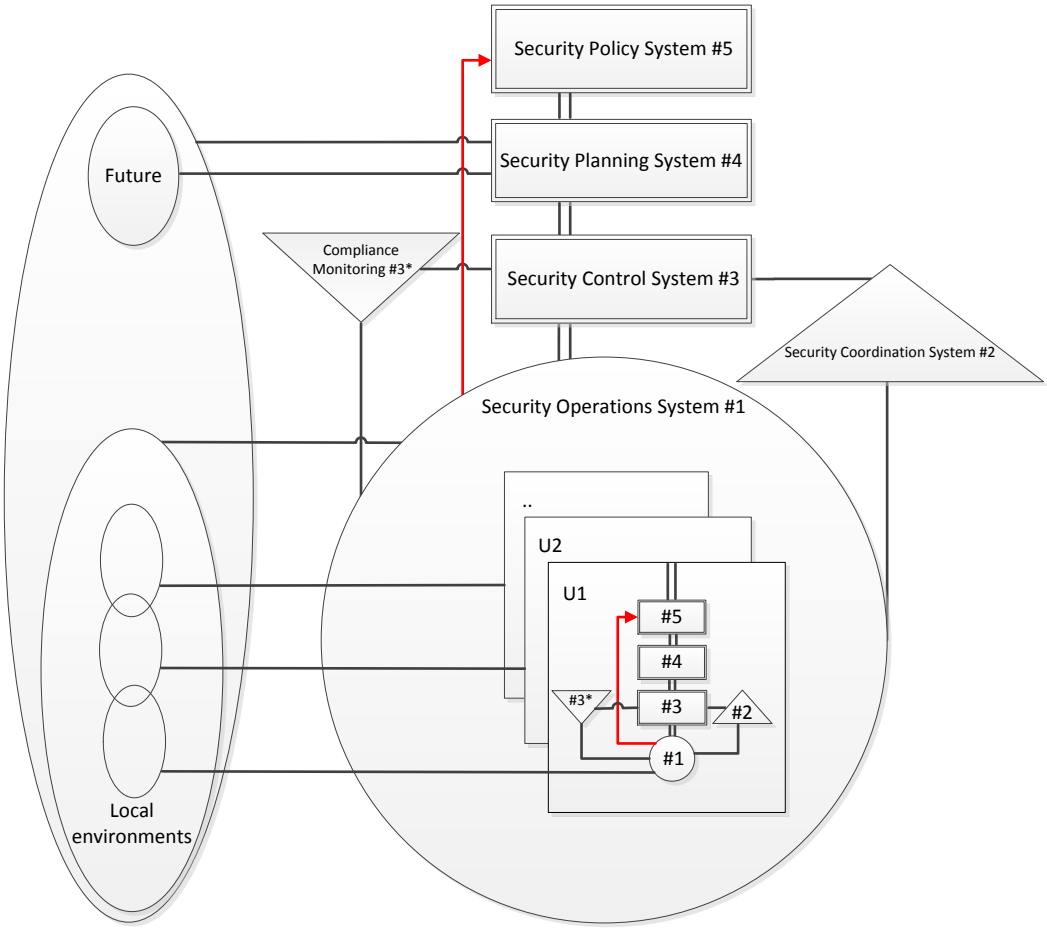


Figure 3-2: VSMISG

3.2.1 Design of the Viable System Model for Information Security Governance

The main goal of the VSMISG is to identify the components of information security governance that enhance an organisation's viability. The components were found by reviewing VSM theory and redefining it for the purpose of ISG. Figure 3-3 illustrates the design process of the VSMISG. It started by reviewing the current literature on ISG frameworks and models and identifying the current components. The viability components of the viable system model (VSM) were next identified, then the components redefined for ISG. After that, a survey was conducted to confirm the appropriateness of the VSM for ISG, yielding the VSMISG shown in Figure 3-2.

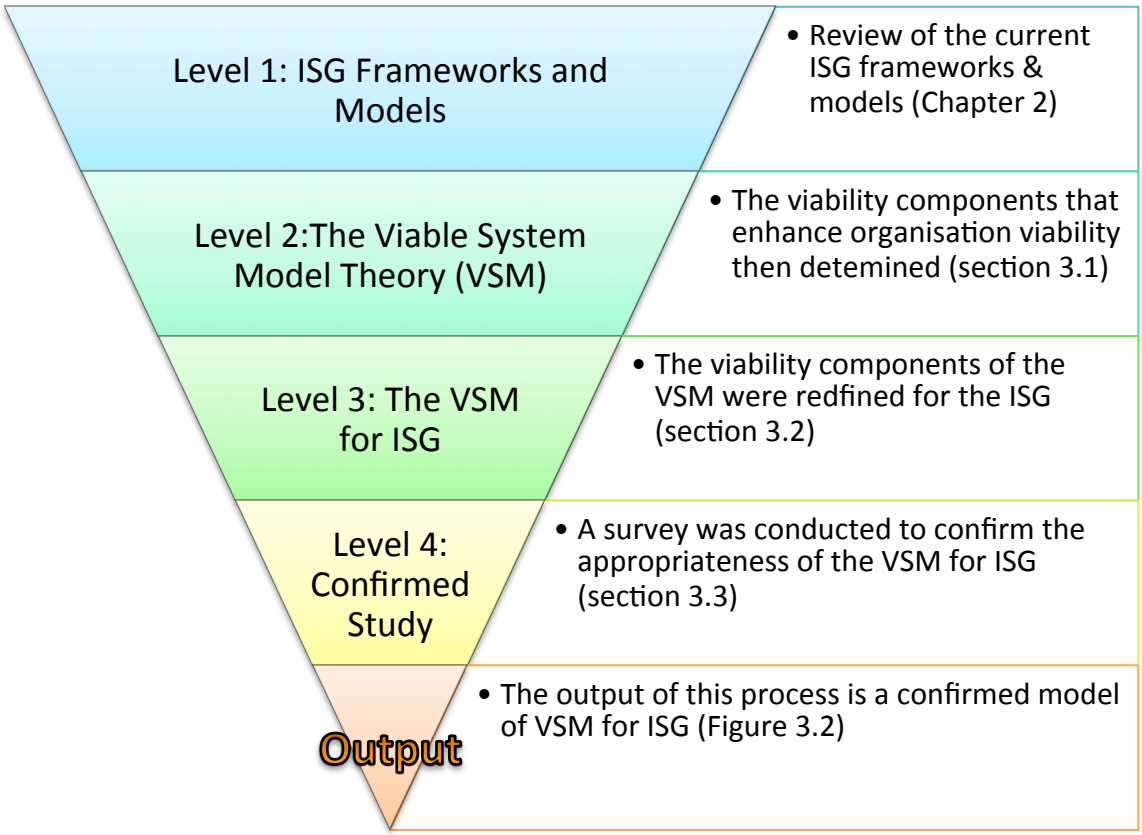


Figure 3-3: Design process of VSMISG

3.2.2 Viable System Model for Information Security Governance Systems

The VSMISG consists of five viable systems and a function, grouped into the three categories described in the next sections.

3.2.2.1 Security operations system #1 and Coordination system #2

Information security operations system #1 is where the organisation works daily to protect its information. It continually deals with and controls dynamic changes in various information security environments. To be able to cope with these changes, it needs to make decisions without delay and must depend on other systems to keep its decisions to a minimum. It must be autonomous to respond effectively and to control its relevant security environments, yet being autonomous does not mean complete separation from the organisational security system; rather, working within an accountability framework.

Information security coordination system #2 coordinates the units (U1, U2 etc) of Operations system #1 to resolve possible conflict and ensure stability and harmony. It dampens uncontrolled oscillations between the units of Operations system #1. Coordination system #2 consists of the information security systems necessary for decentralised decision making (Skyttner 2005) on which the autonomy of Operations system #1 is based.

3.2.2.2 Security control system #3 and Compliance monitoring function #3*

Information security operations system #1 includes one or more specialised units that deal with and control the dynamic changes in its information security environments. To do that, the specialised units require various resources and sometimes these requirements conflict. Information security control system #3 provides the required resources in a way that enables the units of the Security operations system #1 to accomplish their objectives. Security control system #3 is concerned with the 'inside and now' world of organisations. It regulates the current information security activities and requirements of Security operations system #1 for consistence with defined future requirements.

Security control system #3 ensures through the Compliance monitoring function #3* that current information security activities of the Security operations system #1 comply with defined information security policies and that the current activities of Coordination system #2 ensures a proper coordination between the units of Security operations system #1. The security control system translates the information security strategic plan into security policies that the security operations system must adhere to.

3.2.2.3 Security Planning System #4 and Policy System #5

Information security planning (intelligence) system #4, which represents the ISG part in organisations, is responsible for the research and development of a strategic information security plan. Security planning system #4 is concerned with the 'outside and future' world of the organisation system. It models and monitors the security system and relevant strategic security environments, and makes predictions on future trends in information security environments. According to Richelson (1995), the main activities of Planning systems #4 are to collect, process, analyse and produce, and distribute information.

Various information security environments such as risks, competition, clients, regulations, standards and partners exist at the boundary of the organisational security system. Security planning system #4 needs to interact with and adapt to dynamic changes in these environments. It directs the organisational security system toward achieving the goals of information security and securely to position the organisation system. It collects the necessary information about relevant strategic security environments and analyses them to formulate a suitable information security plan with defined requirements. Security control system #3 must implement this plan and maintain cohesion inside the organisation system.

Information security policy system #5 sets the general information security policy and defines the information security identity of the organisation system, which is based on defined purposes. Security policy system #5 establishes the basis for the development of information security guidelines and makes final decisions regarding long-term information security directions.

3.2.3 VSMISG Principles

The VSMISG is based on five principles: autonomy; emergency direct reporting; recursion; requisite variety; and viability. We describe these principles in the following sections (Beer 1981; Lewis 1997; Schwaninger 2006).

3.2.3.1 Autonomy

Control and organisational intelligence are not limited to the head of the organisation. Rather, they are distributed throughout the primary organisational levels (Espejo 2004). Autonomy is necessary for responding to changes in security environments in order to minimise vulnerability (Lewis 1997). The adaptation to dynamic changes in diverse information security environments demands that organisations are autonomous. This means that individuals need to possess the authority and knowledge to be able to take immediate action, if necessary. Autonomy does not mean separation, but the freedom to act with a clear accountability. Autonomous information security operations deploy resources with minimal reference to senior managers, enabling quick adaptation to dynamic changes in related environments. The large ellipse on the left in Figure 3-2 represents the security environment in which the organisation is embedded. Security operations system #1 has its own security environments within organisational security.

In fact, each unit in Security operations system #1 has its own security environment that it needs to deal and cope with it in the operations environment.

3.2.3.2 Emergency direct reporting

Effective defence must involve continuous monitoring and intelligence to ensure dynamic response to information security threats (Hutchinson & Warren 2002). Information security events are communicated between the information security systems through reliable communication channels. The communication channels connect all the information security systems and functions, as well as linking an organisation with its diverse information security environments. For instance, when the Information security operations system #1 cannot cope with changes in its related security environments, it will seek the intervention of the Information security control system #3 through the communication channels between them. If no proper response is received within a defined timeframe, then Security operations system #1 will directly report the situation to the Information security policy system #5 to intervene immediately through exceptionally designed communication channels between Security operations system #1 and Security policy system #5, indicated by red lines in Figure 3-2. Security policy system #5 must eventually receive the urgent information and send 'alarm signals' from the lower systems (Skyttner 2005).

The presence of effective communication channels and the proper design of information flow and reliable information systems are the essential elements behind the emergency direct reporting principle (Espejo 2003).

3.2.3.3 Recursion

Viable systems are recursive; that is, a viable system contains and is contained in a viable system (Beer 1979). For example, the information security operations system and its units are viable systems in their own right, and the operations system is embedded within an organisation that is also a viable system. Furthermore, the organisation is embedded within an industry that is likewise. The recursion principle is depicted in Figure 3-2 by the viable systems inside the units (U1, U2 etc) that are contained in Security operations system #1. The recursion principle enables organisations to cope with the complexity within their diverse information security environments by creating as many levels of controlling systems as required.

3.2.3.4 Requisite variety

For a system to become or remain viable, a system or organisation must attain requisite variety in its operating environment; it must preserve the capacity to adapt to different states and dynamic changes (Brocklesby & Cummings 1996).

In order for Security operations system #1 to cope with dynamic changes in its security environments, it must possess the necessary capabilities to control the changes in these environments. And in order for Security control system #3 to absorb the changes of Security operations system #1, it must be able to contain its changes. Security planning system #4 must possess the necessary ability to absorb strategic changes in its security environment, depicted by the large ellipse in Figure 3-2. The capabilities of the controlling system must absorb the uncertainties of the controlled system to maintain the balance of the whole system (Skyttner 2005).

3.2.3.5 Viability

A viable system is defined as one able to maintain a separate existence by surviving on its own (Beer 1979). However, survival should not be understood as being able merely to exist. Coping with dynamic changes in diverse information security environments can only be maintained by learning, adapting and growing (Beer 1984). It is a key principle in arranging and managing the structure of organisational security systems in such a way that they merge with defined security systems and interrelationships. The clear definitions of the security systems, their internal sub-systems, and their intra- and interrelationships are essential to organisational viability.

3.2.4 Expert Review of the VSM for ISG

In previous sections, we proposed an ISG model based on the VSM that defined the components for enhancing organisation viability. The VSMISG is intended to improve the practice of ISG by contributing an organisation's viability. Therefore, the appropriateness of using the VSM and the importance of its components for ISG were reviewed by eleven information security academics and practitioners. This section assesses their degree of agreement on the importance of the VSM components for ISG. The review used a quantitative method, a questionnaire, to collect the responses through

face to face interviews. This is one of researchers' most widely used data collection techniques (Gray 2009).

The following sections cover the ethical approval for this study, the questionnaire design, descriptions of participants and the results.

3.2.5 Ethical Approval

This study was approved by the Ethics and Research Governance Online (ERGO) committee at the University of Southampton, reference number 2500 (Appendix A). While the questionnaire did not gather personal information and participants were completely anonymous, the data were dealt with confidentially, used only for the research purposes and deleted after analysis.

3.2.6 Participants

The target participants for this study were academics specialised or their research interests fall in information security, and practitioners with knowledge and experience about information security operations and management. Five of the participants were information security practitioners and six were academics. They all worked for a public educational organisation at the time of this study. It is difficult to access participants from other organisations relating for example to business or health due to the sensitivity of their work nature. The ease of access to participants from educational organisation helped in conducting this study.

3.2.7 Questionnaire Design

The main purpose of the questionnaire (Appendix B) was to assess the importance of using the VSM for ISG. This assessment was required to determine the importance of VSM systems and principles by gathering participants' opinions.

The questionnaire was divided into two parts:

1. The assessment of the VSM systems for ISG
2. The assessment of the VSM principles for ISG.

In the first part of the questionnaire, each VSM system was described and the experts requested to rate the importance of the systems for ISG on this basis. Table 3-1 provides these descriptions of VSM systems for ISG.

Table 3-1: Descriptions of ISG viable systems

Information security policy system: Sets the general security policy and defines the security identity of the organisation, establishing the basis for the development of security guidelines, and making final decisions regarding long-term security directions.
Information security planning system: Strategically assesses and manages the organisation security environments (e.g. risks, regulations, competition, environmental factors, partners, and technology changes) by formulating suitable strategic centralised security objectives and plans, with which other functional decentralised security objectives and plans should be consistent.
Information security control system: Formulates operational security policies based on the security strategic plan and provides the necessary resources to parts of the security operations system to enable them to achieve objectives matching the defined operation security policies.
Compliance monitoring function: Ensures that the activities of the information security operations system comply with defined security policies, and that the activities of the security coordination system ensure proper coordination between the various parts of the information security operations system.
Information security coordination system: Coordinates the parts of the security operations system and resolves their conflicting operations security policies to ensure stabilisation and harmonisation in the information security operations system. It consists of the necessary resources for making autonomous decisions.
Information security operations system: Deals with various information security environments such as vulnerabilities, best practices, policies, and standards to cope with dynamic security changes in these environments in order to protect the operations of the organisation.

In the second part of the questionnaire, the VSM principles for ISG were described and the experts were requested to rate them. Table 3-2 shows the descriptions of the VSM principles for ISG.

Table 3-2: Descriptions of the VSM principles for ISG

Requisite variety: Enables the information security systems to have the required capability to control changes in their information security environment and those in the other information security systems they need to control.
Recursion: Enables a security system to encapsulate itself within another in order to cope with the embedded complexity in relevant security environments; that is, solving the complexity of a security system leads to solving the complexity of the whole.
Viability: Enables an organisation to arrange and manage its information security structure based on clear definitions of the roles and responsibilities of its information security systems, to control dynamic changes in its security environments toward organisation viability.
Emergency direct reporting: Enables information security systems to communicate, escalate and translate security events into an understandable format for making necessary decisions or taking required action. Critical warning signals may be routed directly to the information security policy system for it to react immediately.
Autonomy: Enables information security systems to make independent decisions to control the dynamic changes in their information security environments.

According to Matell and Jacoby (1971), Likert scales provide two types of information: the direction and the intensity of a participant attitudinal composition. In

this study we used a five-point Likert scale: very important (5); important (4); neutral (3); not important (2); and not relevant (1).

3.2.8 Data Analysis

Descriptive statistics, including minimum and mean (Saunders et al. 2009), were used to describe and compare variables numerically and were calculated on the rated viability components of the VSMISG. This was undertaken to provide a broad overview of trends in the perceived importance of VSMISG.

Kendall's W is used to assess the extent of inter-rater agreement among raters (Siegel & Castellan Jr 1988). It may vary between 0, 'no agreement' to 1, 'complete agreement' (Kendall 1948). In this study, Kendall's W was used to assess the inter-rater agreement on rating the importance of the following components for ISG:

1. VSM systems
2. VSM principles
3. VSM systems and principles (combined).

We calculated three values of Kendall's W for the inter-rater agreement among experts on the importance of the VSM systems, VSM principles, and the VSM systems and principles (combined) for ISG. This was to investigate whether the experts had different attitudes about the VSM systems and principles as separate parts and as a whole. IBM's SPSS software[1] was used to calculate the mean, minimum and Kendall's W.

3.3 Results of Assessing Importance of VSM for ISG

This section presents an assessment of the importance of the VSM for ISG. This includes both the results of assessing the importance of VSM systems, and the VSM principles for ISG.

[1] www.ibm.com/software/uk/analytics/spss
[2] http://www.gartner.com/it-glossary/smbs-small-and-midsize-businesses

3.3.1 VSM Systems for ISG

This part of the questionnaire aimed to determine the importance of the VSM systems for ISG. Table 3-3 shows the minimum and average ratings of the systems. The minimum ratings were in the range 2–5, while the average ratings were in the range 3.7–4.9.

Table 3-3: Descriptive statistics of the VSM systems for ISG

VSM system	Minimum	Average
Policy system	4	4.9
Planning system	4	4.7
Control system	3	4.4
Compliance monitoring function (part of control system)	3	4.4
Coordination system	2	3.7
Operations system	3	4.4

The average ratings of the experts on the importance of the VSM systems for ISG can be seen in Figure 3-4. It can be seen that almost all ratings of the VSM systems varied between 'important' and 'very important'.

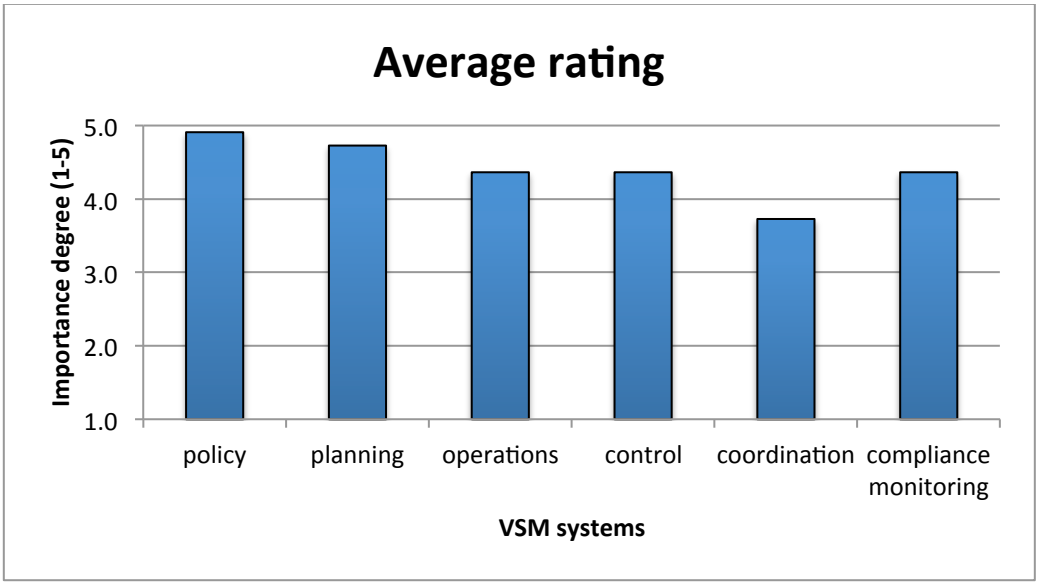


Figure 3-4: The average ratings of the importance of VSM systems

3.3.2 VSM Principles for ISG

This part of the questionnaire aimed to determine the importance of the VSM principles for ISG. Table 3-3 shows the minimum and average of the rated principles. The minimum ratings were in the range 2–4, while the average ratings were in the range 3.9–4.5.

Table 3-4: Descriptive statistics of VSM principles for ISG

VSM principle	Minimum	Average
Viability	4	4.2
Emergency direct reporting	3	3.9
Requisite variety	2	4.2
Autonomy	3	4.4
Recursion	4	4.5

The ratings of the experts on the importance of the VSM principles for ISG can be seen in Figure 3-5. It can be seen that almost all ratings of the VSM principles varied between 'important' and 'very important'.

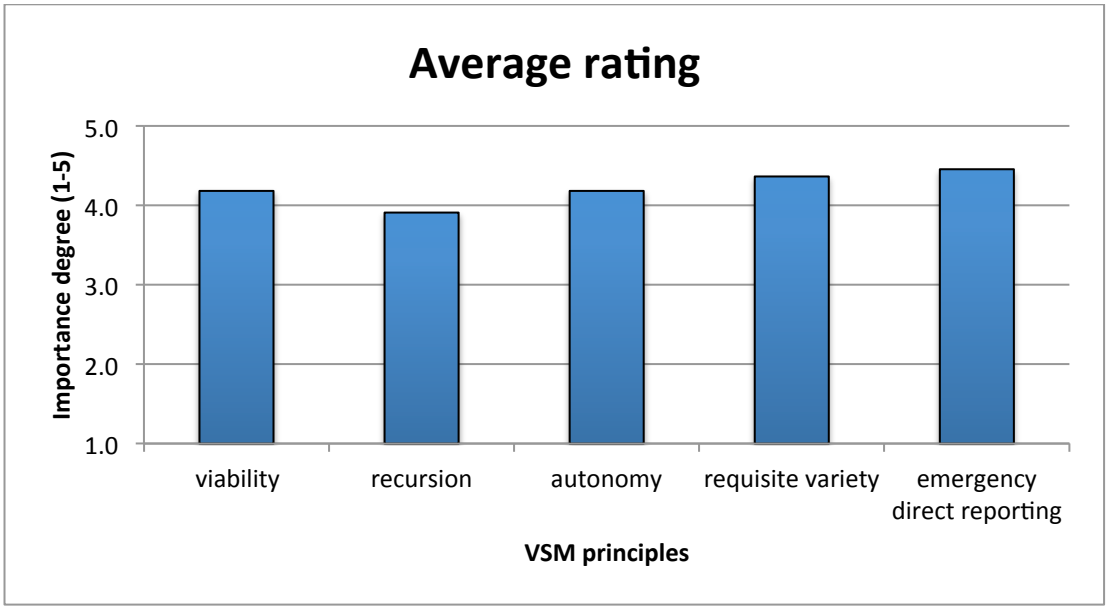


Figure 3-5: The average ratings of the importance of VSM principles

The ratings of the experts on the importance of the VSM systems and principles combined can be seen in Figure 3-6. It can be seen that almost all ratings of the VSM systems and principles varied between 'important' and 'very important'.

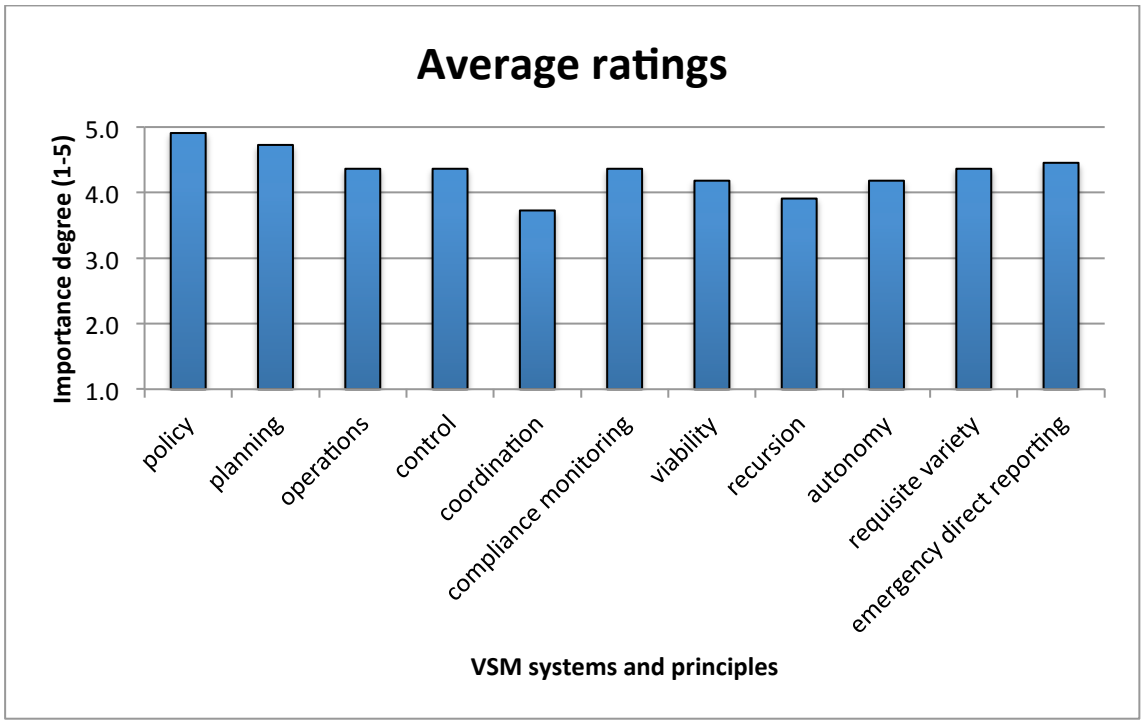


Figure 3-6: Experts' ratings on importance of VSM systems and principles combined

3.3.3 Inter-rater Agreement among Experts (Systems)

The results of assessing the inter-rater agreement among experts on the importance of the VSM systems for ISG were analysed by using the Kendall's W. Table 3-5 shows the results of their inter-rater agreement on the importance of the VSM systems for ISG.

Table 3-5: Extent of inter-rater agreement on importance of the VSM systems for ISG.

N	6
Kendall's W	.285
df	10
Sig.	.072

The Kendall's W results in Table 3-5 show that there was a little agreement among the experts on rating the importance of the VSM systems for ISG, and the result was not significant.

3.3.4 Inter-rater Agreement among Experts (Principles)

The results of assessing the inter-rater agreement among the experts on the importance of the VSM principles for ISG were analysed. Table 3-6 shows the results of the agreement on the importance of the VSMISG principles.

Table 3-6: Extent of inter-rater agreement on the importance of VSMISG principles

N	5
Kendall's W	.341
df	10
Sig.	.073

Kendall's W results in Table 3-6 shows there was a little agreement among experts on rating the importance of the VSMISG principles but better than their agreement on the importance of the systems, and the result was not significant.

3.3.5 Inter-rater Agreement among Experts (Systems and Principles)

Having assessed the degree of inter-rater agreement of experts on the importance of the VSMISG systems and principles separately, we assessed overall inter-rater agreement.

Table 3-7: Extent of inter-rater agreement on importance of the VSMISG systems and principles as a whole

N	11
Kendall's W	.200
Df	10
Sig.	.015

Kendall's W results in Table 3-7 show that there was a little agreement among the experts on rating the importance of the VSMISG systems and principles as whole, and the result was significant.

3.4 From VSMISG to Emergency Direct Reporting

In Chapter 2 we reviewed the literature, and identified the current ISG frameworks and models. Although many ISG components were identified that relate to ISG principles, structure, risk management strategies, plans, processes and others, information security governance has no direct means of becoming aware of information security threats affecting organisational viability in order to be able to respond in a timely manner. Boards of directors and executive management are held accountable for their organisational information security, yet this accountability is meaningless if they do not have the capability directly to identify strategic security incidents that affect their organisation's viability.

In the reviewed literature in Chapter 2, reporting was identified as an important component of ISG (CGTF 2004; ITGI 2006; Entrust 2004), and organisational unit reporting (CGTF 2004). According to the Federal Financial Institutions Examination Council (2004), a board of directors is responsible for overseeing an organisational information security programme through a number of methods, including receiving reports on the effectiveness of management's response. This type of reporting follows conventional routes of communication between information security staff and departments through existing channels. It is not adequate to deal with emergency situations that impact on an organisation's viability and demand direct reporting to the strategic or governance level, as it takes too long before the ISG level is aware of the situation.

According to Gokhale and Banks (2002), VSM for ISG enhances organisational security, fostering viability. Information security governance based on the VSM has the ability directly to make the security governance level aware of current strategic security threats affecting organisational viability through emergency direct reporting. This way of reporting to the governance level is a useful method to embed in an organisation's information security structure. The authors propose that security threats affecting an organisation's viability are reported to the ISG level through emergency security

reporting, besides other alerts. They argue that modern organisations require automatic security monitoring methods capable of overriding conventional communication channels in the event of threats to an organisation's viability in an emergency. In a timely manner, organisations must be capable of reporting and controlling dynamic changes in information security environments, including the security threat environment. Emergency direct reporting leads to more effective security governance (Ross & Weill 2004; Brown & Nasuti 2005), while routine (hierarchical) reporting introduces delay since it spans several layers (Bender 2010; Howes 2004).

The argument of Gokhale and Banks (2002) inspired this research and was its motivation. Consequently, the focus of this study is emergency direct reporting, one of the internal controls that can be used for organisational governance. According to CGTF (2004), irrespective of size or form, all organisations use internal controls to manage and direct. This statement helped to focus this research on investigating the effects of VSMISG, incorporating emergency direct reporting for different sizes of organisations, security threat intensities and times.

Ryan (2009) concluded that the level of crisis preparedness is related to the size of the organisation. Large organisations are expected to exert more diligence in protecting organisational assets (Baker & Wallace 2007), while in small organisations the processing of security threats that affect organisation viability is delayed as the necessary resources are busy (Savarimuthu et al. 2004). Small organisations are generally human resource poor, thus it is large organisations with their greater human resources that are generally more successful in terms of information security (Yang et al. 2005; Chang & Ho 2006). Kankanhalli et al. (2003) and Hoffer and Straub. (1989) conclude that large organisations invest more heavily in information security in terms of available human resources.

Using the VSMISG provides a number of benefits such as aware organisation awareness (Beer 1984; Gokhale & Banks 2002), responsive organisation (Espejo 2003; Hutchinson & Warren 2002; Gokhale & Banks 2002; Davies 2002; Lewis & Millar 2009), viable organisation (Gmür et al. 2010; Hoverstadt & Bowling 2002; Gokhale & Banks 2002) and cost-effective organisation (IT Governance Institute 2005; Lewis & Millar 2009). According to the IT Governance Institute (2005) and Lewis and Millar (2009), implementing the VSMISG is more profitable than the baseline ISG model.

3.5 Summary

This chapter introduced VSM theory, redefined for the ISG context. It proposed VSM for ISG, referred to as VSMISG, and described its principles and systems. In doing so, the following research question was answered:

RQ1 What are the components of ISG that enhance organisational viability?

Eleven information security experts rated the importance of the VSM systems and principles to ISG. The results showed that they recognised them as either 'important' or 'very important' to ISG. This answered the following research question:

RQ2 What is the importance of the VSM' systems and principles for ISG?

The degree of agreement among the information security experts was assessed regarding the importance of the VSM systems and principles to ISG. There was a little agreement among the experts on rating the importance of the VSM's principles, systems, and principles and systems combined. This answered the following research question:

RQ3 To what extent do information security experts agree on rating the importance of the VSM's principles, systems, and principles and systems (combined) to ISG?

This chapter ended by determining that the focus of the study was to be on investigating the effects of the VSMISG, incorporating emergency direct reporting in various sizes of organisation, security threat intensities and time scales.

Chapter 4. Information Security Governance Models Design and Development – Baseline and VSMISG

In previous chapters we saw how VSM theory was adopted and redefined for the purpose, then reviewed the importance of the VSMISG to information security governance.

One of the viable system principles introduced in Chapter 3 was emergency direct reporting between information security operations and policy systems. To study the impact of emergency direct reporting between them requires two ISG models, one to represent the baseline ISG model and the other the VSMISG incorporating emergency direct reporting. These were designed and their simulation models developed. In addition, the randomness of the Simul8 Random Number Generator (RNG) was tested to ensure that it generated random numbers before using it to simulate both models, as described in the next chapter.

The baseline ISG and VSMISG models consist of two parts, the first representing the information security operations system and the second the information security control, planning and policy systems. By model, we mean the structure of the simulation system and, by system, we mean the constituent information security systems within it. The baseline ISG model has five information security systems and the VSMISG has five viable information security systems. These are numbered following Beer's notation as follows:

- Information security operations system #1
- Information security control system #3
- Information security planning system #4
- Information security policy system #5.

Information security co-ordination system #2 and the Compliance monitoring function were not needed in this study.

4.1 Simulation Method

A simulation is a representation of the operation of a real world system or process (Banks 1999). Simulating a system and testing hypotheses about it are undertaken by means of modelling (Sokolowski & Banks 2009) to enable the study of how a system changes over time and how components interact with each other (Carson 2005).

The aim of simulation is to construct a model that draws conclusions and provides insight into the behaviour of real world entities or phenomena (Preece et al. 2005), gaining a better understanding and identifying improvements to the system or process under study (Pidd 2003). We have access to few real world systems or processes, yet through simulation we can imitate the behaviour of many more with a certain degree of accuracy by developing models. When simulation models are developed and validated, they can be used to investigate different situations and scenarios.

Advances in simulation methodologies and the availability of various simulation languages with huge capabilities at affordable cost has made simulation one of the most widespread methods in systems analysis and operations research. Environmental, informational, and organisational variations are observed in order to note the effect on the model's behaviour (Banks et al. 1999). This allows investigation of the effects of change on organisational attributes.

Simulation plays an important role in security evaluation. It may be used in areas including the assessment of how security measures impact on system performance (Nicol 2005). Simulation was used in this research to investigate the impact of changes in organisation size, threat intensity and simulation time on reporting times.

4.1.1 Discrete-Event Simulation

There are several types of simulation such as discrete-event, continuous, combined discrete-continuous, Monte Carlo and spreadsheet simulations. According to Law and Kelton (2006), '*Discrete-event simulation concerns the modelling of a system as it evolves over time by a representation in which the state variables change instantaneously at discrete points in time*'.

Information security events take place and enter the information security governance model at discrete points in time. Change in such events causes change in the

state of the system, so this study opted for the discrete-event type to simulate ISG models.

4.1.2 Software simulation package

Today, visualised interactive simulations are widely used by academics and practitioners. This type of simulation provides a number of benefits, identified by (Robinson 2003) as:

- Greater understanding of the model
- Easier model verification and validation
- Interactive experimentation
- Improved understanding of the results
- Improved communication of the model and its findings to all parties
- Potential for using simulation in group problem solving.

The simulation software package used for the ISG models was the discrete event simulator SIMUL8. This permits the creation of flexible and robust simulations, and is widely used in industries and academia (Concannon et al. 1995) to create a visual model of the system under study by drawing animated objects directly on a display. All inputs, queues, routing arrows, activities and outputs of the models were thus visualised. The University of Southampton provided access and support to SIMUL8 as a licensed software simulation package for researchers.

4.2 Baseline Model for Information Security Governance

Demonstrating the effect of the direct reporting between the information security operations and policy systems necessitated the construction of two models. One represented the current situation, as the baseline of information security governance model, while the other represented viable information security governance.

In the following sections the design of the conceptual and simulation models of the baseline model is described.

4.2.1 Conceptual Model Design

In this section the focus is on representing the conceptual ISG model. The design of the conceptual ISG model includes all the inputs, outputs and activities involved. The first part of the model represents the current information security operations system, while the second represents the others: control, planning, and policy.

The International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) published an information security incident management model, as embodied in BS ISO/IEC 27035 (2011). The standard is intended to simulate information security incident management for large and medium-sized organisations.

For the current information security operations system we adopted the operational side of the information security incident management model embodied in the international standard BS ISO/IEC 27035. We adopted this standard because it is an international and well-known standard reflecting best practice in information security incident management. For simplicity, since they were not needed in this research, four activities of this standard were excluded: detection, digital evidence collection, communication and later response. The other activities that are required for this study for representing the information security operations system are shown in Figure 4-1.

The second part of the model represents one of the contributions of this research, as original development of the ISO standard was achieved by designing three information security management systems, namely control, planning, and policy.

Figure 4-1 shows the activities, inputs and outputs of the model, comprising four information security systems: operations, control, planning and policy. It involves 15 activities distributed between the security systems. The solid black dot in the conceptual model represents the initial point of receiving the different types of information security events, while the arrow shows the direction of flow. The solid black dot in a circle represents final activity, while final flow is represented by an X in a circle. Activities are represented by rounded rectangles and diamond shapes represent decisions, notation derived from the UML diagram convention for the start and end of an activity (Fowler 2003).

The next section explains the information security operations system that comprise the first part of the model, the current information security operations system that serves as the baseline.

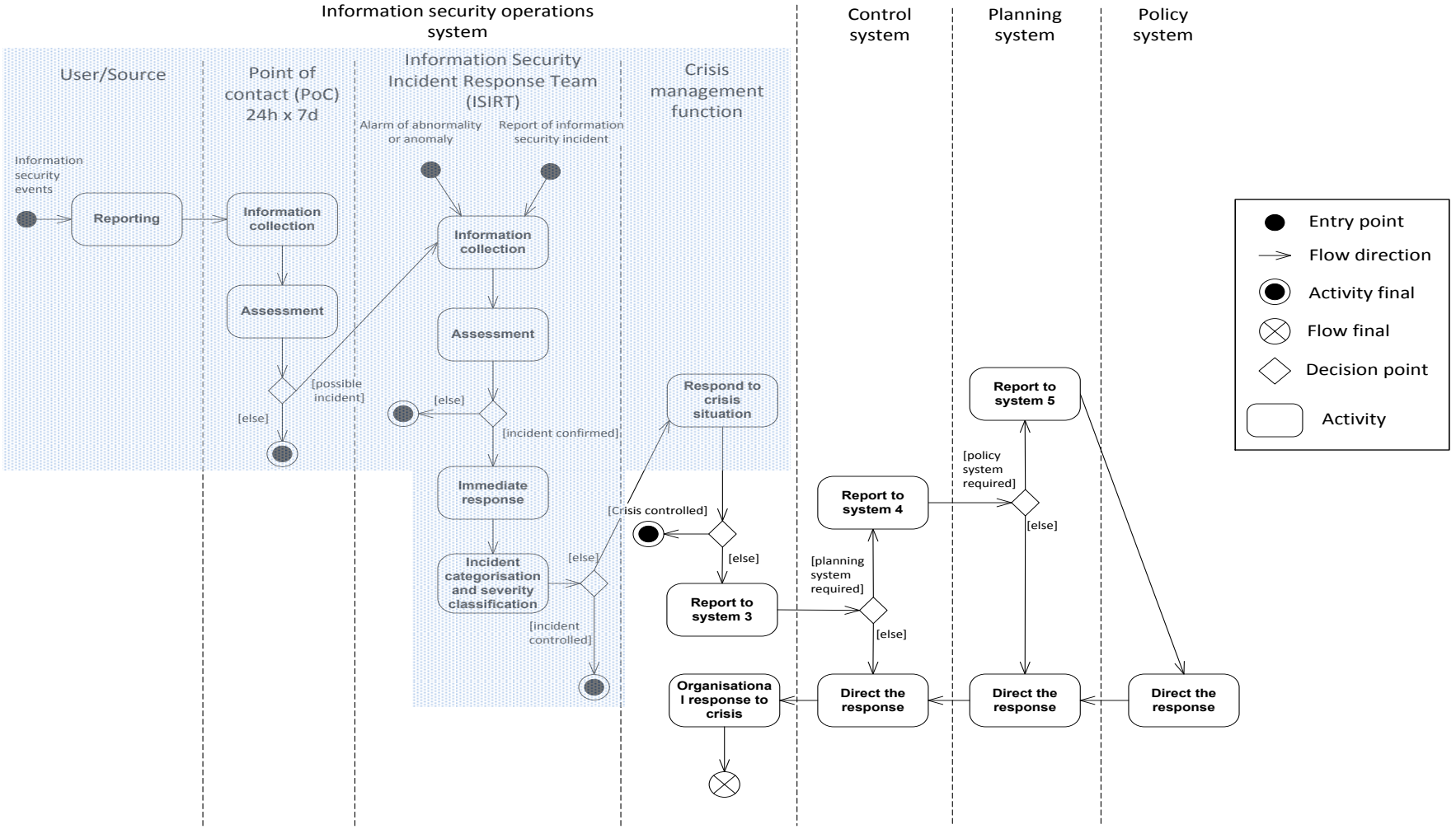


Figure 4-1: Conceptual baseline ISG model (highlighted activities adopted from BS ISO/IEC 27035: 2011)

4.2.1.1 Information security operations system

The information security operations system comprises four entities: the user/source, the Point of Contact (PoC), the Information Security Incident Response Team (ISIRT) and the crisis management function. The inputs into the model are information security events, which can be false positives, incidents or crises. Information security crises are processed by all information security systems. Some may be controlled by the operations system and others by the control system, while others require intervention by the planning system or immediate attention and response from the policy system.

Users or sources such as detection and monitoring systems report information security events. The PoC team starts collecting the required information relating to the reported event, then assesses it before deciding whether it is a false positive or indeed a possible incident.

In the ISIRT information collection activity, the ISIRT collects the required information relating to a possible incident received from the PoC, also reports of information security incidents and alarms about abnormalities or anomalies. Next, the ISIRT assesses these to decide if they are false positives or confirmed incidents.

In immediate response activity, the ISIRT provides a response to a confirmed incident straightaway. In incident categorisation and severity classification activity, incidents are mapped to relevant categories and the severity of its impact on the organisation is determined. Response to a crisis situation is activated when the ISIRT reports that an information security incident is not under control and needs to be dealt with as a crisis.

The activities of the model described so far are those adopted to represent only the information security operations system. To represent the other systems—information security control, planning and policy systems—more activities had to be designed, considered to be a contribution of this research.

4.2.1.2 Information security control, planning, and policy systems

A decision point was added to the model after the response to a crisis situation to check whether the crisis is controlled. If not, then the crisis management function reports the situation to the control system, then the control system decides whether the received

situation requires intervention by the planning system. If it does, the control system reports the situation to the planning system; if not, the control system directs the response and the crisis management function responds to the crisis.

When the planning system receives a reported situation from the control system, it decides whether the received situation requires the attention of the policy system. If it does, the planning system reports the situation to the policy system, which directs the response to the crisis; if not, the planning system directs the response.

The response to a crisis is directed by the system appropriate for the required intervention; the policy system directs the response of the planning system, the planning system directs the response of the control system and the control system directs the response of the operations system. After providing the organisational response to crisis, the flow ends.

4.2.2 Simul8 Simulation Model Development

Identifying the behaviour of the ISG baseline model necessitated the design of a simulation model that corresponds to the conceptual model. The simulation model could then be used to emulate the behaviour of all the ISG systems. Determining the behaviour of the baseline model established the foundation for demonstrating the effect of the direct reporting between the information security operations and policy systems.

Figure 4-2 shows the baseline ISG simulation model, comprising four systems: information security operations; control; planning; and policy systems. Table 4-1 describes the Simul8 objects.

Table 4-1: Description of Simul8 objects

Object	Description
Work entry point 	The point where work items enter the simulation
Queue 	The storage bin where information security events wait until the required resource(s) in a work centre become available
Resource 	Human resources such as information security technicians, analysts, engineers, managers required for processing security events in work centres
Work centre 	Where resource(s) process information security events
Route arrow 	The path that information security events take, travelling between the work centres of a simulation
Work exit point 	The point where information security events leave the simulation when work is completed as closed false positives, incidents or crises
Decision point 	At this point, human resources decide what to do with information security event

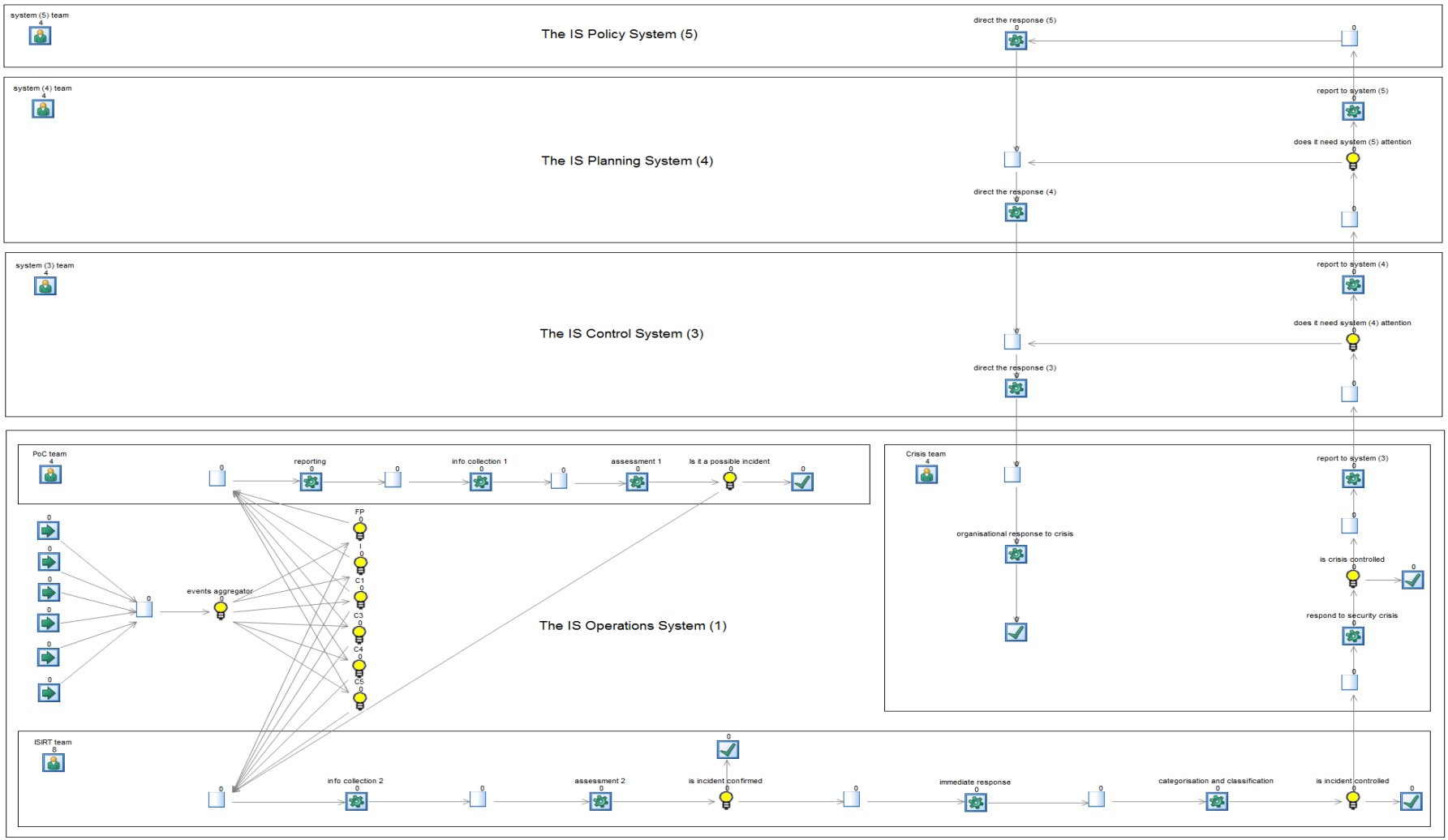


Figure 4-2: Simulation model for baseline ISG

4.2.2.1 Information security operations system

In section 4.2.1.1, we described the information security operations system conceptually. In this section, we detail the simulation of the information security operations system, showing the parameters and settings used. The information security events entering the simulation model were categorised into three streams: false positives; incidents; and crises to be processed by System #1.

Besides these, three crisis streams were added: crises to be processed by System #3; crises to be processed by System #4; and crises to be processed by System #5. The additional streams were required for the investigation of the impact of direct reporting between Information security operation System #1 and Policy system #5. The list below shows these streams:

1. False positives
2. Information security incidents
3. Crises processed by System #1
4. Crises processed by System #3
5. Crises processed by System #4
6. Crises processed by System #5.

Figure 4-3 shows the six visualised streams. All six streams were aggregated and labelled – the events aggregator was used for this purpose. Each stream was assigned a unique label: FP for false positive; I for incident; C1 for crises processed by Operations system #1; C3 for crises processed by Control system #3; C4 for crises processed by Planning system #4; and C5 for crises processed by Policy system #5. We did not use the C2 label, since the Information security coordination system (2) was excluded from this study, as mentioned above.

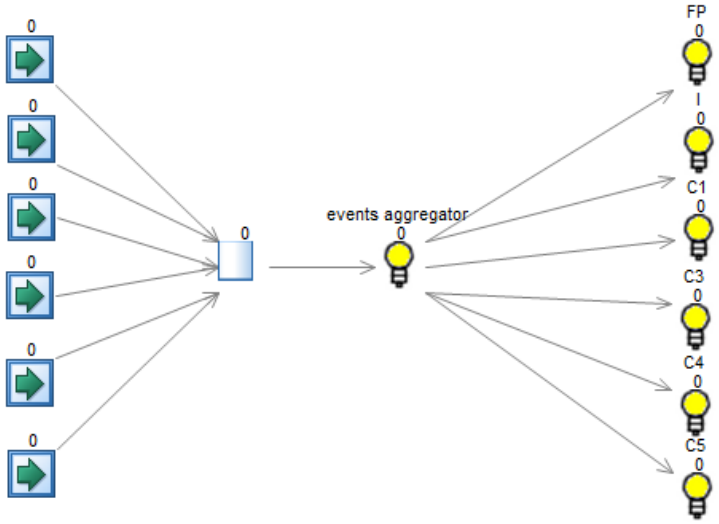


Figure 4-3: Simulation inputs and their distributor

The routing of the streams within the simulation was based on labelling, to facilitate the tracking of different types of events within the simulation and to distinguish the data for better data collection and analysis. For each type of stream, 57 per cent was routed to the PoC team and 43 per cent to the ISIRT team. Six distributors, represented by yellow light bulbs, were used for this routing purpose, as depicted on the right of Figure 4-3.

The simulation of the information security operations System #1 involved ten activities processed by three teams: the Point of Contact (PoC), the Information Security Immediate Response Team (ISIRT) and the crisis team.

The PoC team processed three of the ten activities. These were reporting, information collection 1 and assessment 1, as depicted in Figure 4-4.

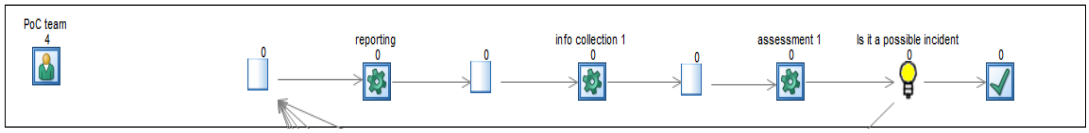


Figure 4-4: Activities processed by the PoC team

The ISIRT team processed four activities: information collection 2, assessment 2, immediate response, and categorisation and classification, as shown in Figure 4-5.

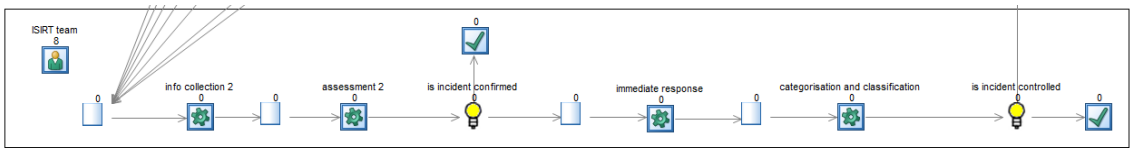


Figure 4-5: Activities processed by the ISIRT team

The crisis team processed three activities: response to security crisis, report to System #3 and organisational response to crisis. Figure 4-6 depicts these activities.

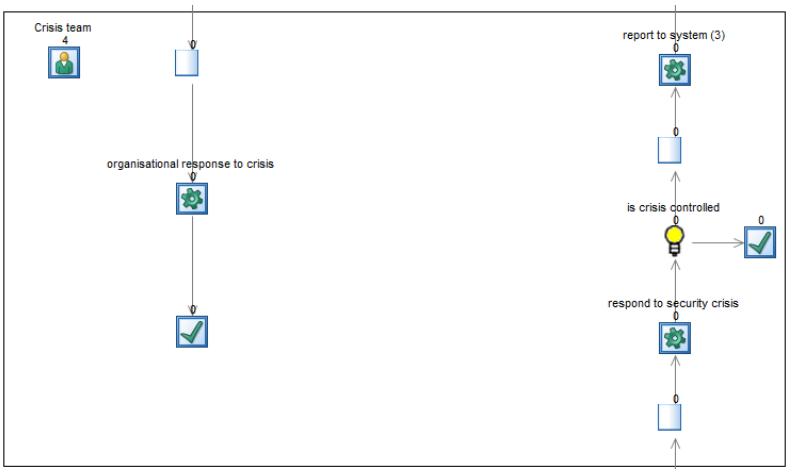


Figure 4-6: Activities processed by the crisis team

Having designed the first part of the baseline simulation model, the second part was designed as described in the following section.

4.2.2.2 Information security control, planning, and policy systems

The team for Information security control system #3 processed two activities. One was reporting to Planning system #4 and the other activity was directing Response #3 of the crisis team in System #1. Figure 4-7 illustrates the activities processed by Information security control system #3.

Figure 4-7: Activities processed by Control system #3

The team for the information security planning System #4 processed two activities. One was reporting to the policy System #5 and the other directing Response #4 of the control system. Figure 4-8 illustrated the activities processed by Information security planning system #4.

Figure 4-8: Activities processed by Planning system #4

The team for the information security policy System #5 processed one activity, that of directing the Response #5 of the planning system. Figure 4-9 illustrates the activity processed by the information security policy System #5.

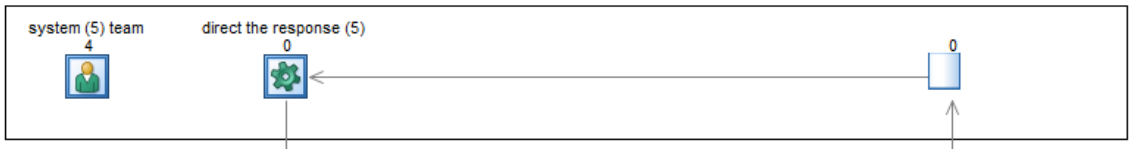


Figure 4-9: Activity processed by Policy system #5

4.2.3 Data

The data used in this research came from a case study conducted by HP Laboratories (2012). The study identified the types of statistical distributions and parameters used in its simulation of an information security operations system. The data can be categorised into two: information security events as input data; and activities data.

4.2.3.1 Information security events

Statistical distributions are the Probability Density Functions (PDF) used to generate sequences of random numbers (Robinson 2003). Different statistical distributions produce different random number sequences.

An entry point has a mean value of the arrival rate. This value defines the mean time of the arrival of information security events. The information security events that entered the simulations were randomly generated using Poisson statistical distribution. This required the specification of the mean inter-arrival time. It was assumed that the Poisson distribution was the appropriate distribution to describe random arrival rates over a period of time for simulation models (Black 2009).

The HP case study identified three types of streams and their parameters. These streams were false positives, incidents and crises processed by Information security operations system #1. Table 4-2 shows the stream type, number of occurrences per year and the statistical distribution defined in the simulation, based on the HP case study.

Table 4-2: Stream types and parameters based on HP case study

Input	Parameter	Occurrences/year (2880 hrs)	Statistical distribution
False positives	1.2	2481	Poisson
Incidents	0.27	10756	
Crises to be processed by System #1	3	942	
Total		**14179**	

Not all the required data were provided by the HP case study, as this covered only Information security operations system #1. Where needed, additional data were derived as indicated in the following discussion, usually for Control system #3, Planning system #4 and Policy system #5.

The proportions of the additional streams introduced in section 4.2.2.1 were defined by using 80 per cent and 20 per cent, following the Pareto rule, which can be used for making estimates (Ultsch et al. 2005); 20 per cent of the crises processed by System #1 were reported to System #3, and 80 per cent comprised closed crises. The same percentages were used with System #3 and System #4; that is, 20 per cent of the crises processed by System #3 were reported to System #4 and 80 per cent comprised closed crises. Finally, System #4 reported 20 per cent to System #5 and 80 per cent comprised closed crises.

Table 4-3 shows the additional stream types, number of occurrences per year and statistical distribution defined in the simulation.

Table 4-3: Additional stream types and parameters

Input	Parameter	Occurrences/year (2880 hrs)	Statistical distribution
Crises to be processed by System #3	20	144	Poisson
Crises to be processed by System #4	120	23	
Crises to be processed by System #5	240	11	
Total		**178**	

4.2.3.2 **Activities data**

A uniform distribution was assumed for the processing time for events in the models' activities. The processing times were randomly generated between lower and upper bounds. The data from the HP case study were used to define the parameters of the

simulation activities. We set the processing times of the direct the response activities of System #3, #4, and #5 and the organisational response to crisis activity at one to two hours. Table 4-4 shows the models' activities and their parameters based on the HP case study.

The number of people allocated to each security team matched the performance of the baseline model in the HP case study. Table 4-5 shows the size of each security team.

Table 4-4: Model activities and parameters, based on the HP case study

Model activities	Parameter	Statistical distribution
Reporting	0.25–1	Uniform
Info collection 1	8–80	
Assessment 1	1–16	
Info collection 2	8–24	
Assessment 2	4–16	
Immediate response	1–4	
Incident categorisation and classification	1–2	
Respond to security crises	1–2	
Report to system #3	16–24	
Report to system #4	16–40	
Report to system #5	16–40	
Direct response #5	1–2	
Direct response #4	1–2	
Direct response #3	1–2	
Organisational response to crises	1–2	

Table 4-5: Number of people in each security team

Team	People allocated to team
PoC	144
ISIRT	122
Crisis	6
System #3	1
System #4	1
System #5	1
Total	**275**

4.2.4 Model Validation

The baseline simulation system underwent a validation process to ensure that the baseline Information security operations system #1 represented the actual operation of the HP case study with sufficient accuracy. Validation is the process by which it is ensured that the simulation system represents the real world (Robinson 2003). It deals with the assessment of behavioural or representational accuracy of the simulation system (Balci 2003) and focuses on building a sound model, increasing confidence in the baseline model by attempting to confirm that it is an accurate representation of the real system (Banks et al. 1999). Hence, only a valid model can address the question: Does the computer model represent the real system with sufficient accuracy?

A number of validation techniques and their suitability for different situations have been introduced and discussed, as in the work of Balci (2003), Fenz and Ekelhart (2011), Sargent (1998) and Robinson (1997), and a taxonomy of the validation techniques may be found in Balci (1994). We used black-box validation, as it is one of the techniques used to determine that the overall model represents the real world with a certain degree of accuracy (Robinson 1997). Black-box validation has some limitations that are as follow (Khan 2012):

- Testing every input streams is unrealistic because it would take a long time
- Limited coverage as limited number of test scenarios can be performed
- Hard to design test cases without clear specifications

Other validation methods such as white-box can be used to validate models. It is used to determine that the internal structure of the model represent the real world. This type of validation has some limitations as follow (Engel 2010):

- Must have skills in the subject matter domains
- It is very expensive
- Must have specific knowledge about internal structure of the model under study
- Limitations to make exhaustive tests

In the following section, we define the performance metrics used to compare the baseline ISG model and the HP model.

4.2.4.1 Performance metrics

We used four performance metrics to compare the performance of the baseline model to the real information security operations model. These metrics were as follows:

1. Time taken to identify information security incidents
2. Time taken to identify information security crises
3. Number of reported security crises per year
4. Number of events processed per year.

Time Taken to Identify Information Security Incidents

The time taken to identify an information security incident was taken as the time from the event entering the simulation system to the ISIRT team confirming that it is indeed an incident. As in the HP case study, information security incidents were taken as those identified as such in less than 10 days (80 hours).

We ran the baseline simulation system for a simulated period of six months, representing the simulation time used in HP's system for reporting performance metrics. Figure 4-10 shows the distribution of time taken to identify information security incidents in the baseline simulation system. We can see that the ISIRT team in the baseline simulation system identified information security incidents in less than 80 hours (10 days). This matched the time to identify information security incidents as reported by HP case study.

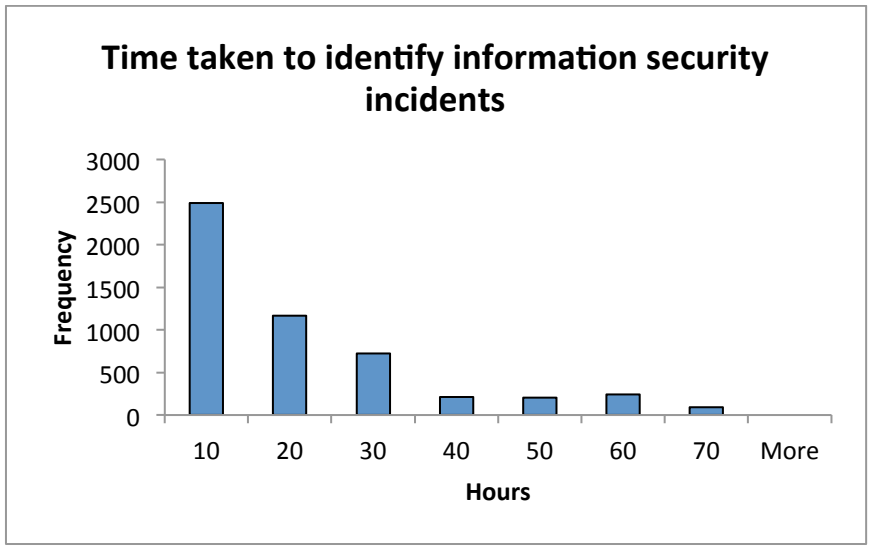


Figure 4-10: Distribution of time taken to identify information security incidents

Time Taken to Identify Information Security Crises

The time taken to identify information security crises is the time taken from events entering the baseline simulation system to the ISIRT team reporting them to the crisis management function as uncontrolled and, again as in the HP study, is here taken as less than 10 days (80 hours). Figure 4-11 shows the distribution of time taken to identify information security crises in the baseline system.

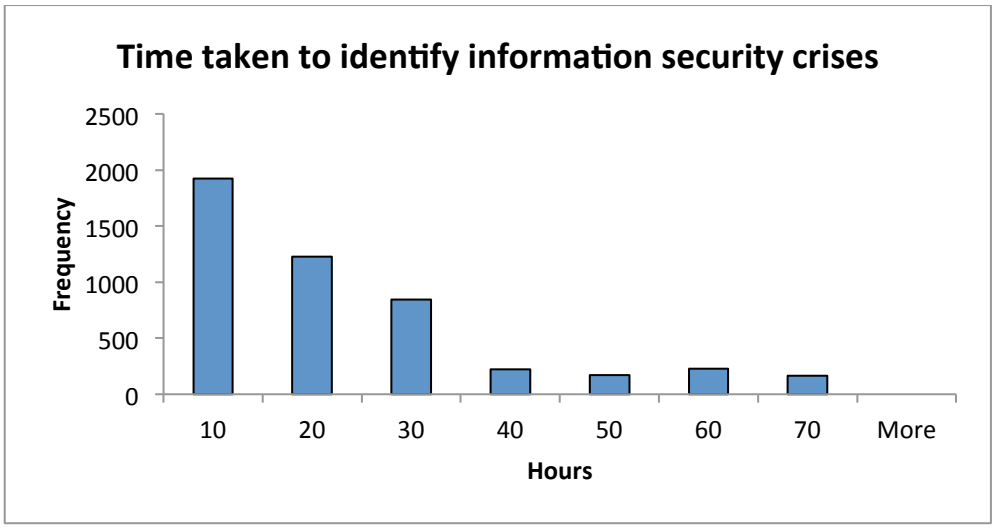


Figure 4-11: Distribution of time taken to identify information security crises

Number of Reported Security Crises per Year

In the HP case study, the ISIRT team reported about 900 information security crises per year, while in the baseline model the ISIRT team reported 1074 crises per year. The difference is owing to variation in the simulation system structure of the real and baseline systems. In the HP system, the ISIRT team decided at the same point whether an event was an incident or a crisis, whereas in the baseline system the ISIRT team first decided if an event was an incident then, after being processed by two activities, 'immediate response' and 'incident categorisation and classification', whether an incident became a crisis.

Since the time taken to identify an information security incident and crisis were therefore equal in the HP system, we accelerated the processing of security incidents in the two activities in the baseline simulation system so that the time taken to identify security crises was similar to that to identify security incidents. As a result, the number of reported security crises per year in the baseline system became greater than the

number of reported security crises in the HP system, but this is had no effect on the results.

Number of Events Processed per Year

Different types of events entered the system, to be later identified as false positives, security incidents and crises. The number of events that HP's system processed was about 12,000 per year, while the number of events that the baseline system processed per year was 12,005. This means that the real and baseline systems processed almost the same number of information security events, indicating a similar intensity of security threat.

4.3 Viable System Model for Information Security Governance (VSMISG)

In section 4.2 we described the design of the baseline model for information security governance systems. In this section we describe the design of the viable system model for information security governance (VSMISG).

In the baseline model, the information security crises that required the immediate attention of the policy system were reported in a structured way through control and planning systems; there was no direct communication between the information security operations and the policy systems. In this section, we overcome this limitation by enabling the information security operations system to communicate directly with the policy system if immediate attention of the policy system is required.

In following sections, we describe the design of the conceptual viable system model, followed by the design of the simulation model.

4.3.1 Conceptual Model Design

In this section, the focus is on representing the conceptual model of the viable system for information security governance. Figure 4-12 shows the conceptual viable system model for information security governance, divided into two parts as with the baseline model: the information security operations system and the information security control, planning and policy systems.

4.3.1.1 Information security operations system

The conceptual viable system model of the information security operations system is the same as that of the conceptual baseline model, as explained in section 4.2.1. The only change made was the addition of a direct reporting channel between the information security operations and policy systems. Figure 4-12 shows the direct reporting channel between the operations and policy systems.

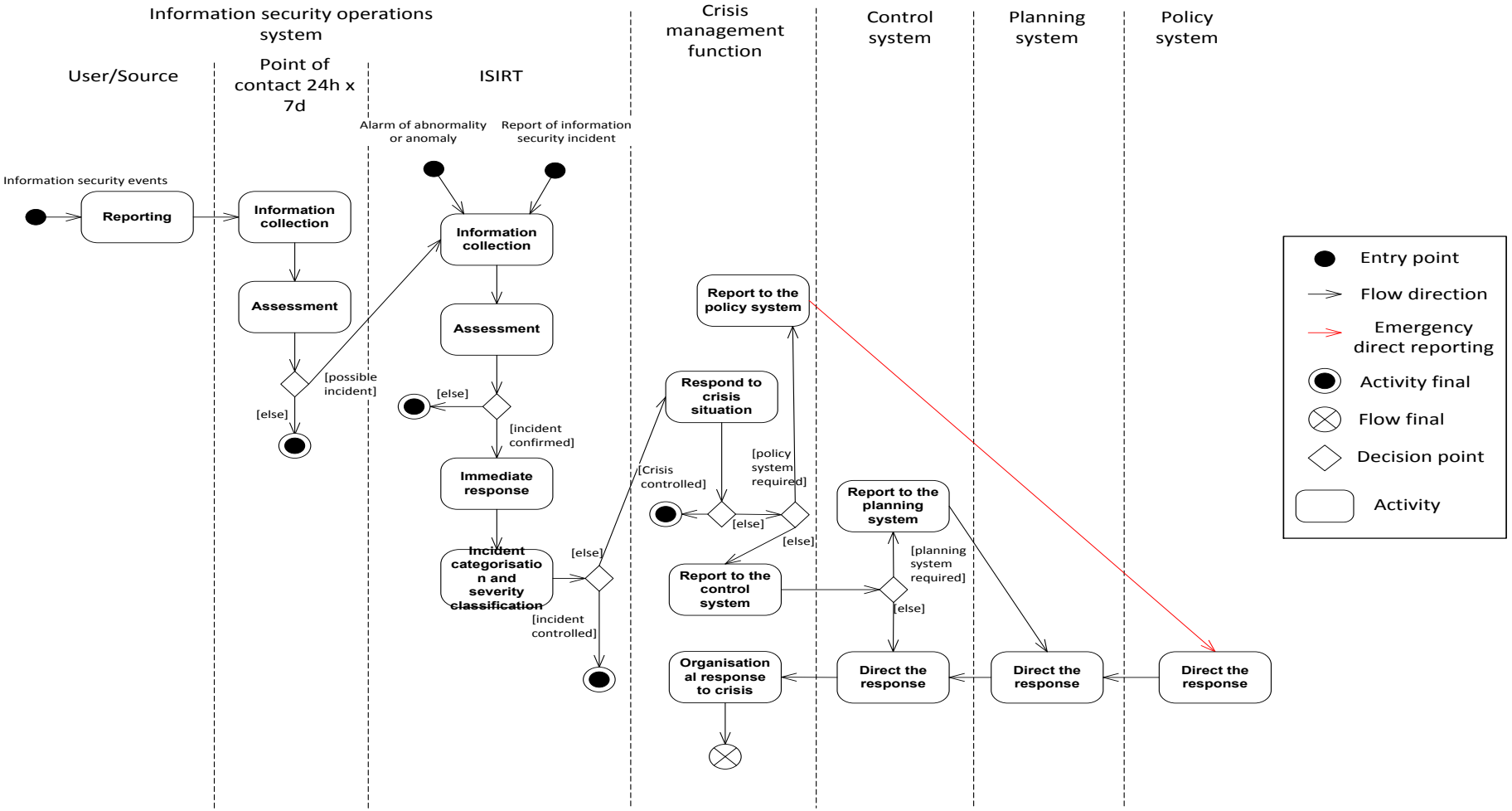


Figure 4-12: Conceptual viable system model for ISG

The direct reporting channel enables the information security policy system immediately to wake up from sleep to direct the response to critical security situation threatening the continuity of organisation (Gokhale & Banks 2002). The information security policy system monitors the current critical security situation from an early stage and responds in a timely manner.

In the baseline model, the crisis management function in the information security operations system checks whether the crisis is controlled after responding to it; if it is not controlled, then the security situation that requires the immediate attention of the policy system is reported through the control and planning systems. In the viable system model, however, the security situation that requires the immediate attention of the policy system is directly reported to the policy system, bypassing the security systems in the middle: the control and planning systems.

In the viable system model of information security governance, the crisis management function was enabled to report directly to the information security policy system in the event of an emergency by adding new a decision point and activity. The new decision point comes after checking whether the crisis is controlled. It assesses whether direct reporting to the policy system is required in an uncontrolled crisis. If so, the new activity 'report to the policy system' is activated; if not, normal communication as in the baseline model is adopted.

4.3.1.2 Information security control, planning and policy systems

The conceptual viable model of information security control, planning and policy systems is the same as that of the baseline conceptual model. The only change made was the removal of the usual reporting channel between the information security planning and policy systems, because it was no longer required after establishing direct reporting between the operations and policy systems. Other routine communications channels between the planning and policy systems were not designed for this model as they were beyond the scope of this study.

4.3.2 Simul8 Simulation Model Development

The simulation of the viable information security governance system revealed the behaviour of the system after adding a direct reporting channel between the information

security operations and policy systems. We established the simulation environment to demonstrate the effect of direct reporting between the operations and policy systems. Figure 4-13 depicts the simulation of the viable information security governance system.

4.3.2.1 Information security operations system

The simulation of the viable information security operations system is the same as that of the baseline ISG simulation model. The only change made was the addition of a direct reporting channel between the information security operations and policy systems. Figure 4-13 shows the direct reporting channel between the information security operations and policy systems.

4.3.2.2 Information security control, planning and policy systems

The simulation of the viable information security control, planning and policy systems is the same as that for the baseline simulation model. The only change made was the removal of the regular reporting channel between the information security planning and policy systems. The information security planning system directs the response of the control system and is not required to report to the policy system. The objective was to study the behaviour of the system under investigation with the effect of the direct reporting channel between the operations and policy systems in the absence of another reporting channel.

We used the statistical distribution approach to generate random numbers. In the next section, we define the statistical distributions used for the simulation.

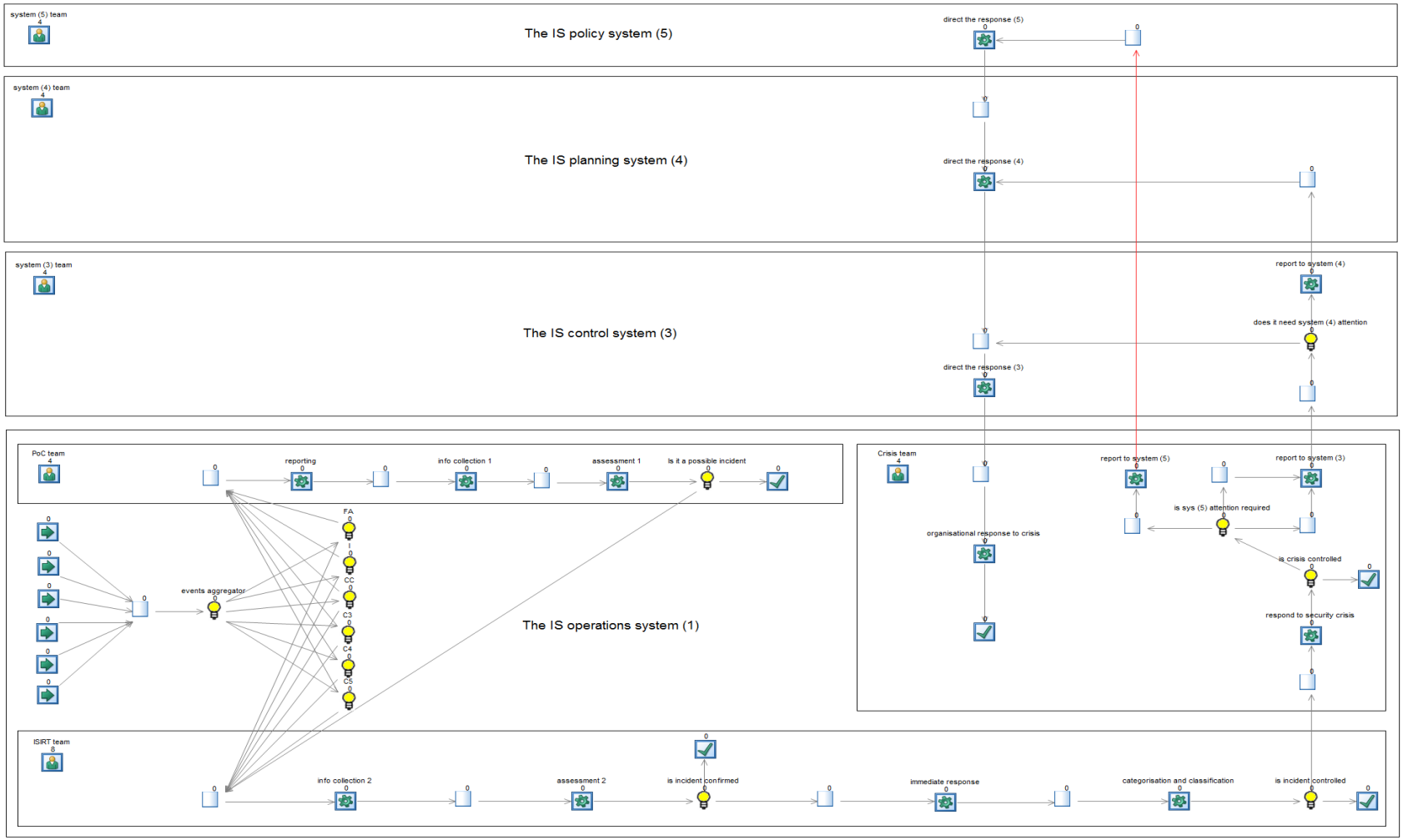


Figure 4-13: Simulation model for VSMISG

4.4 Random Number Generator

Random Number Generators (RNGs) are computer programs to produce sequences of numbers that seem to be generated randomly from a specific probability distribution. These numbers are sometimes called pseudorandom numbers, to indicate that they are not actually random.

RNGs are an essential component of all types of computer applications such as secure communications, simulation of stochastic systems and computer games (L'Ecuyer & Simard 2007). The quality measures for an RNG depend on the application; low memory usage, high speed and good statistical properties are the required attributes in computer simulations (L'Ecuyer & Simard 2013).

L'Ecuyer developed a number of RNGs in his studies, one of which was chosen to be among the ten landmark papers published in the proceedings of the Winter Simulation Conference. The Simul8 simulation software package used in our study implemented L'Ecuyer's RNG. Other popular commercial simulation software packages such as Arena, Automod, SAS and Witness also employ L'Ecuyer's RNGs (Grassmann et al. 2008).

The randomness of the streams generated by simulation software packages needs to be checked (Robinson 2003), as sometimes a poor RNG results in totally meaningless (L'Ecuyer 1998) or misleading outcomes (L'Ecuyer 1990). Therefore, before using the simulation software in our study we tested its RNG to make sure that the generated streams met the appropriate criteria of randomness.

4.4.1 Testing the Random Number Generator

There are many different tests to check the randomness properties of RNGs. Marsaglia provided a battery of statistical tests to assess these (Marsaglia 1996), the best-known of which is DIEHARD (L'Ecuyer & Simard 2007). Knuth described standard tests applied to RNGs (Soto 1999; Knuth 1998), while the National Institute for Standard and Technologies (NIST) published a statistical test suite for RNGs (Rukhin et al. 2010).

In this section, we specify the statistical tests used to check the randomness properties of the RNG and describe the testing process of the Simul8 RNG, followed by the results.

4.4.2 Chi-square Goodness of Fit

The Chi-square goodness of fit test was used to check the uniformity of the RNG. It is perhaps the best known statistical hypothesis test and it is a basic method used in connection with other tests (Knuth 1998). It measures how far the observed counts of the generated numbers vary from the expected counts (Moore & Notz 2006). The formula for the statistic is:

$$\chi^2 = \sum \frac{(observed\ count - expected\ count)^2}{expected\ count}$$

The Chi-square test requires that the observations or participants are independent, randomly selected and organised into categories. In the case of large sample sizes, the Chi-square possesses power by which it distinguishes between good and poor fitting models (Kenny & McCoach 2003).

A major limitation of the Chi-square test is that, although it deals with the statistical significance of observed cell frequencies, it does not provide information about the degree of association among the subjects in the cells (Hansjuergens 1986). For our study, we did not investigate the degree of association as this was irrelevant to its purpose.

In the following sections we use Chi-square to test the two statistical distributions of Simul8's RNG: uniform and Poisson.

4.4.2.1 Uniform distribution

We tested a null hypothesis that the sample being tested has uniform distribution. The null hypothesis represents no statistically significant difference between uniform distribution and distribution of the sample generated by Simul8's RNG. The alternative hypothesis was defined as there being a significant difference between uniform distribution and the sample distribution.

The data were categorised into ten intervals of length 0.1 and values of between zero and 1. The degree of freedom (df) was 9, the number of intervals -1.

The effect size is used to measure the influence level of a treatment effect (Lipsey & Wilson 1993). Cohen defined three levels of effect size; he set a small value at 0.1, a medium value at 0.3 and a large value at 0.5 for the Goodness of Fit statistical test (Cohen 1987). We used the small value as we were interested in detecting small but meaningful differences between the observed and expected data (Park 2010).

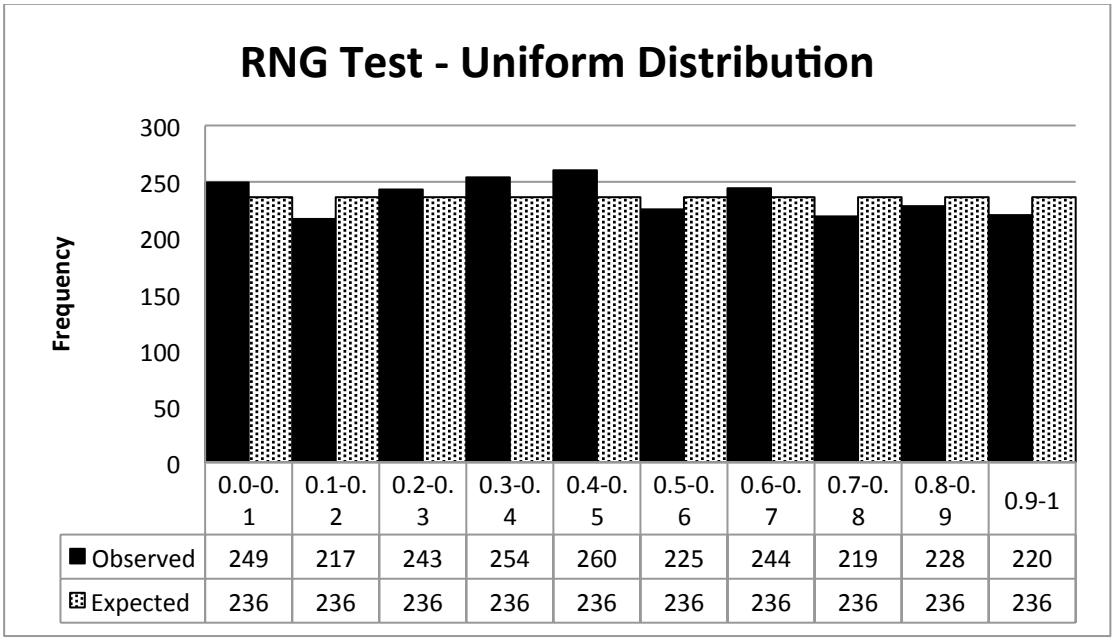
A Type I error, alpha (α) is when a true null hypothesis is rejected. In this test, a Type I error occurs when we reject the null hypothesis of equal intervals, when in fact they are equal. Based on judgement, the value of 0.05 has been defined for alpha. There is nothing technically significant about the determination of the alpha value (Cunningham & McCrum-Gardner 2007). The judgment of defining the value of alpha should consider the acceptable risk of a Type I error that can be taken in the experimental study (Bartlett et al. 2001). The power is the probability of correctly rejecting a false null hypothesis. It is equal to one minus Beta. Beta is the probability of a Type II error, one which occurs when a false null hypothesis is not rejected (Vanvoorhis & Morgan 2007). Using judgement, the value of 0.05 was defined for Beta. In this uniform distribution test, a Type II occurs when we fail to reject the null hypothesis of equal intervals when in fact they are different.

We defined the parameters by which we computed the required sample size by using GPower software, based on the settings specified in Table 4-6. GPower is one of the best known freeware software packages used to compute required sample size (Sheskin 2004). The required sample size calculated by using GPower was 2359.

Table 4-6: Parameter values for computing sample size

Test	*Goodness of fit*
Effect size	0.5
α error probability	0.05
β error probability	0.05
Power (1-β error probability)	0.95
df	9

Figure 4-14 shows the uniform distribution frequency of the RNG. Black bars depict the observed frequency of uniform distribution of the RNG, while shaded bars show the expected distribution. The expected frequency for each interval is 236. There was some variation in the uniformity of the RNG, but this was not significant, according to the result of the Chi-square test.



	0.0-0.1	0.1-0.2	0.2-0.3	0.3-0.4	0.4-0.5	0.5-0.6	0.6-0.7	0.7-0.8	0.8-0.9	0.9-1
Observed	249	217	243	254	260	225	244	219	228	220
Expected	236	236	236	236	236	236	236	236	236	236

Figure 4-14: Observed and expected Poisson frequency distributions

Table 4-7 shows the test's statistics and p-values. Since the p-value = 0.381 > 0.05, the null hypothesis was not rejected. At the $\alpha = 0.05$ level of significance, there was not enough evidence to reject the null hypothesis. Thus, the uniformity of the RNG fitted the theoretical uniform distribution.

Table 4-7: Chi-square statistic and p-value of Uniform distribution test

Chi-square	9.635
df	9
p-value	0.381

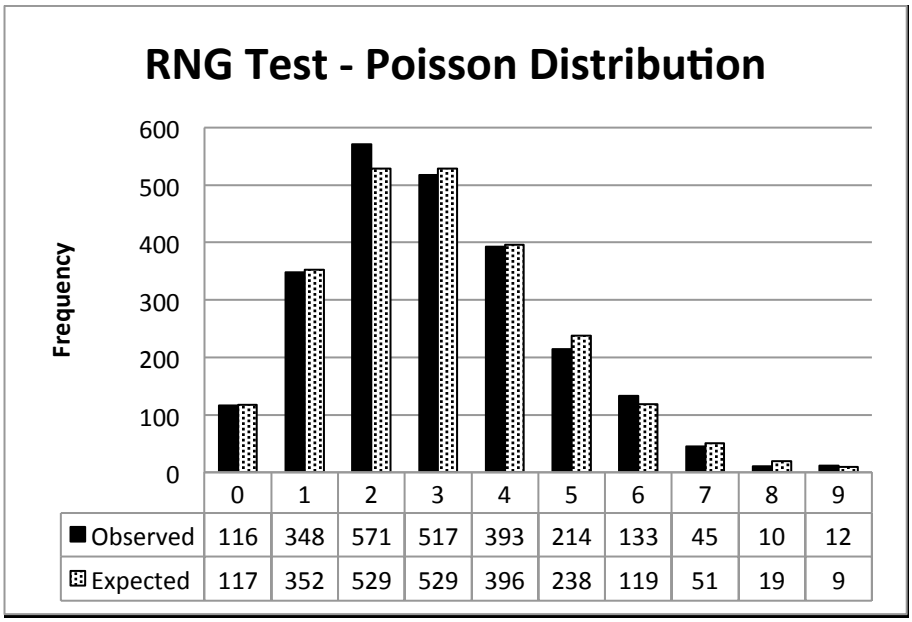
4.4.2.2 **Poisson distribution**

We tested a null hypothesis that the sample being tested followed the Poisson distribution. The null hypothesis represented no significant difference between the Poisson distribution and distribution of the sample generated by Simul8's RNG. An

alternative hypothesis was defined as there being significant difference between the Poisson distribution and the sample distribution.

The data were categorised into ten intervals of length 1, starting from zero. The key parameter to fit a Poisson distribution is the mean value, which was 3 in this test. We used two parameters to calculate the expected frequency of the Poisson distribution: the probability of the Poisson distribution for each interval and the sample size. The expected frequency for Interval 3 was given by multiplying the probability of this interval, 0.2241, by 2359, the sample size. The Excel functions POISSON.DIST and CHISQ.TEST were used to calculate the probabilities for all the intervals and to calculate the P-value, respectively.

Figure 4-15 shows the Poisson distribution frequency of the RNG. Black bars indicate the observed frequency of the Poisson distribution of the RNG, while shaded bars indicate the expected distribution. There was some variation between the observed and expected Poisson distribution, but this is not statistically significant, according to the result of the Chi-square test.



	0	1	2	3	4	5	6	7	8	9
Observed	116	348	571	517	393	214	133	45	10	12
Expected	117	352	529	529	396	238	119	51	19	9

Figure 4-15: Observed and expected Poisson frequency distributions

Table 4-8 shows the test statistics and p-value. Since the p-value = 0.126 > 0.05, the null hypothesis was not rejected. At the $\alpha = 0.05$ level of statistical significance, there was not enough evidence to conclude that the observed Poisson frequency distribution does not fit the expected Poisson distribution. The RNG generates random numbers, according to the theoretical Poisson distribution.

Table 4-8: Chi-square statistic and pvalue of Poisson distribution test

Chi-square	13.886
df	9
p-value	0.126

4.4.3 Autocorrelation

In the previous section we showed that the uniform and Poisson distributions of the Simul8's RNG passed the Chi-square test at the specified significance level. In this section, we use the autocorrelation test, also known as serial correlation, to test if there is similarity between observations with itself. The autocorrelation test was used to detect repetition or periodicity in adjacent observations (Sheskin 2004). Observed numbers are compared to subsequent numbers according to some shifts in time known as lags. For instance, the autocorrelation at Lag 2 tests whether Observations 1 and 3, 2 and 4,… 10 and 12, and so on are correlated.

Since we determined the significance level as 0.05, we expected to see five significant autocorrelations in a hundred, so we specified the number of lags likewise as one hundred.

The same data for the Chi-square tests above were used in the autocorrelation test. We employed the StatPro add-in within Microsoft Excel software to calculate the standard error and the autocorrelation test. An autocorrelation value may vary between -1 and 1, negative autocorrelations being indicated by -1 and perfect positive autocorrelation by 1. There is no autocorrelation when the value is zero. The observations are considered random when their autocorrelations are near zero, and they are considered non-random when there is one or more significant autocorrelation, depending on the significance level (Sheskin 2004).

4.4.3.1 Uniform distribution

We used the autocorrelation test to assess the uniform distribution of the Simul8's RNG to detect similarity in adjacent random numbers. Table 4-9 shows the significant values detected by autocorrelation. The autocorrelation value is considered significant when it is equal or greater than double the size of the standard error reported by the StatPro add-

in within Microsoft Excel. At Lags 22, 35, 37 and 39, the autocorrelation values were greater than double the size of the standard error, thus they were considered significant.

Table 4-9: Significance values of the uniform distribution autocorrelation test

Lag	Autocorrelation	StErr
22	0.0494	0.0206
35	0.0477	0.0206
37	0.0414	0.0206
39	0.0491	0.0206

Figure 4-16 displays the autocorrelations of the RNG uniform distribution. The dotted lines represent the confidence bounds at the 95 per cent significance level. We can see four significant autocorrelations, shown in red, among the one hundred observations shown in blue. The number of the significant autocorrelations was as expected and we concluded that the Simul8's RNG randomly generated uniform distribution.

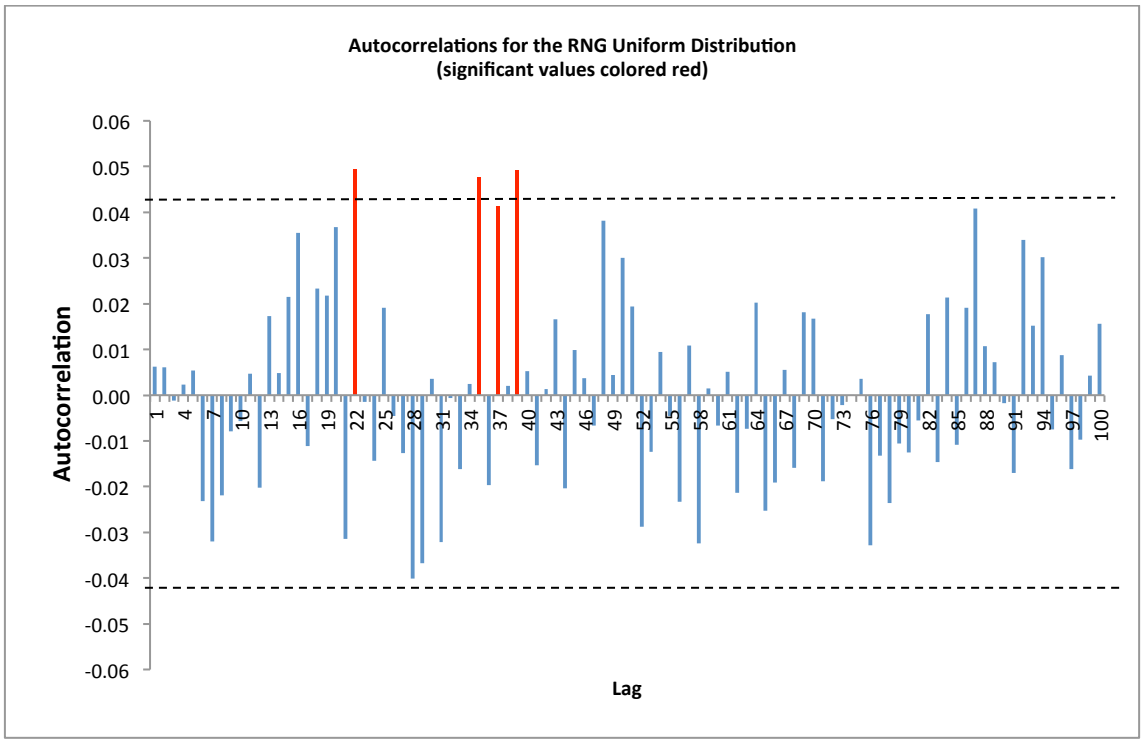


Figure 4-16: Autocorrelations of the RNG Uniform distribution

4.4.3.2 **Poisson distribution**

The autocorrelation test was used to test the Poisson distribution of the Simul8's RNG. Table 4-10 shows the significant values detected by the autocorrelation test. At Lags 4, 12, 45, 86 and 98, the autocorrelation values were greater than double the size of the standard errors, thus they were considered significant.

Table 4-10: Significance values of Poisson distribution Autocorrelation test

Lag	Autocorrelation	StErr
4	0.0453	0.0206
12	-0.0530	0.0206
45	0.0703	0.0206
86	0.0453	0.0206
98	-0.0484	0.0206

Figure 4-16 displays the autocorrelations of the RNG Poisson distribution. We can see five significant autocorrelations, shown in red, among the one hundred observations shown in blue. The number of the significant autocorrelations is five, as expected, and we concluded that the Simul8's RNG randomly generated Poisson distribution.

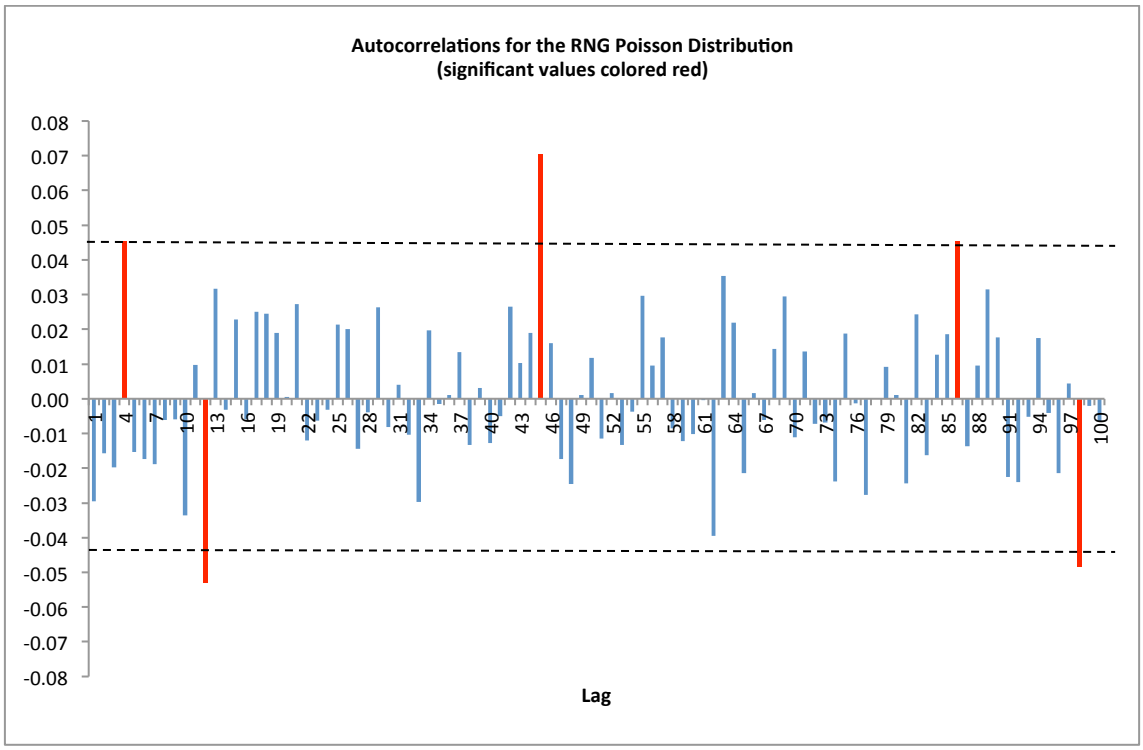


Figure 4-17: Autocorrelations of the RNG Poisson distribution

4.5 Summary

This chapter provided the design of the conceptual models for the baseline ISG and VSMISG. The activity diagram following UML notion was used to design the conceptual models. The simulation models for the baseline ISG and VSMISG were developed using. Simul8 software. These simulation models were developed in order to create the environment required to investigate the impact of direct reporting, as described in the next chapter.

The simulation models were validated by comparing them to real model data provided by the HP case study. The uniform and Poisson distributions of the Simul8's RNG were tested by using the Chi-square goodness of fit and autocorrelation tests to check the randomness properties of the RNG before use. The Simul8's RNG passed the Chi-square and Autocorrelation tests and it may now be used to generate the random numbers required in conducting simulations, as described in the next chapter.

Chapter 5. Effects of the VSMISG

In this chapter we show how we used the ISG baseline and VSMISG computer models, developed as described in the previous chapter, to conduct the research experiment. The main objective was to investigate the impact of the VSMISG on the time taken to identify security crises that affect organisational viability for different organisation sizes, level of threat intensity and time scales. We define the security incidents that affect organisation viability as Strategic Security Crises (SSC).

To investigate the impact of the VSMISG on these attributes we ran two models: the ISG baseline model and the VSMISG. For each we varied the attributes and used four-way ANOVA to analyse the data.

This investigation answered the following research questions:

RQ4 *Does the VSMISG have significant effects on the time taken to identify SSCs?*

RQ5 *Is this effect related to organisation size?*

RQ6 *Is this effect related to the intensity of security threats?*

RQ7 *Q4: Is this effect related to simulation time*?

This chapter describes how we relaxed the models developed in the previous chapter to make them suitable for experimentation at all organisation sizes and for different threat intensities. We then outline the experiment design and explain the methodology, followed by the results and analysis.

5.1 Need to Relax Simulation Parameters

In Chapter 4 the baseline and VSMISG models' design and development required for conducting the research experiment were described. The resources and parameters used for their development were based on a case study provided by HP, the requirements of which were for a large organisation.

We faced some challenges during experimentation in the settings for small and medium organisations. The number of people that we used to represent a small and medium organisation was, following the standards, in the ranges of 1–50 and 51–250 respectively. When we ran the small and medium organisations models, unrealistic SSC

times were reported. Since our experiment required the modelling of a small and medium organisation in addition to a large one, we needed to relax the models' parameters in such a way as to accommodate all organisation sizes to achieve realistic results. The parameters were relaxed to accommodate greatly reduced number of information security staff in order to achieve reasonable results. They were guided by the original parameters of HP case study. It has been broadly reduced by a factor between 2-4 to be more appropriate for the proportionality smaller organisation. The resulting relaxed parameters yielded tractable model which gave a plausible results in relation to small size of organisation being modelled. Tables 5-1 and 5-2 show the relaxed parameters of the models' inputs and activities.

Table 5-1: Relaxed simulation input parameters

Input	**Mean (inter-arrival time) (h)**		**Statistical distribution**
	Original	**Relaxed**	
False positives	1.2	12	Poisson
Incidents	0.27	3	
Crises processed by system #1	3	20	
Crises processed by system #3	20	120	
Crises processed by system #4	120	240	
Crises processed by system #5	240	360	

Table 5-2: Relaxed simulation activity parameters

Input	Upper and lower bounds (h)		Statistical distribution
	Original	Relaxed	
Reporting	0.25–1	0.1–0.2	Uniform
Info collection 1	8–80	0.5–1	
Assessment 1	1–16	0.5–1	
Info collection 2	8–24	0.5–1	
Assessment 2	4–16	0.5–1	
Immediate response	1–4	0.25–0.5	
Incident categorisation and classification	1–2	0.25–0.5	
Respond to security crises	1–2	0.5–1	
Report to System #3	16–24	1–2	
Report to System #4	16–40	1–2	
Report to System #5	16–40	1–2	
Direct Response #5	1–2	1–2	
Direct Response #4	1–2	1–2	
Direct Response #3	1–2	1–2	
Organisational response to crises	1–2	0.5–1	

5.2 Experiment Design

A factor is a variable that is investigated in an experiment. To investigate the impact of a factor on the response, two or more values of the factor are studied. These values are known as levels or settings. The combination of factor levels is known as treatment (Wu & Hamada 2000).

We defined four experimental factors for this research investigation, as follows:

1. Models
2. Organisation size
3. Threat intensity
4. Simulation time.

Figure 5-1 depicts the cause-and-effect diagram, known as a fishbone diagram, organising the factors and their levels that may impact the time taken to identify SSC.

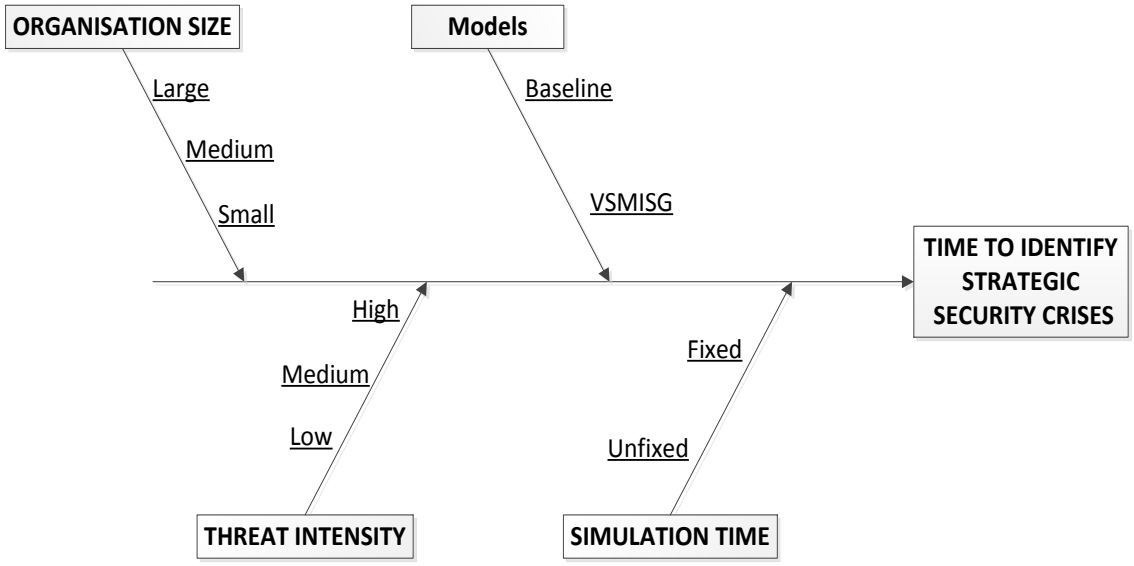


Figure 5-1: Cause-and-effect diagram for the VSMISG experiment

The factors are organised under the following headings: model; organisation size; threat intensity; and simulation time. More details on each of these factors are provided in the following sections.

5.2.1 Models

The models' factors have two levels: the baseline and the VSMISG. The baseline model used normal reporting, while the VSMISG used direct reporting of SSC from Information security operations system #1 to Information security policy system #5.

5.2.2 Threat Intensity

Threat intensity was considered at three levels: low; medium; and high. These were based on the number of different information security events occurring per year. We set

the medium threat level from data provided by the HP case study, which we later relaxed to make them suitable for experimentation for all organisation sizes with different threat intensities, and set the high threat level as double and the low threat intensity as the half this medium threat level. Table 5-3 shows the threat intensity levels by the event types handled by the security system.

Table 5-3: Threat intensity levels by security system and events type per year

Security system	Events type	Low threat	Medium threat	High threat
System #1	False positives	124	248	495
	Incidents	471	945	1937
	Crises	71	143	282
System #3	Crises	12	23	48
System #4	Crises	5	12	24
System #5	Crises	4	8	16
Total/year		**687**	**1379**	**2802**

5.2.3 Organisation Size

Organisation size can be measured in different ways, such as by the number of human resources, sales or the number of IT platforms installed (Chang & Ho 2006; Kotulic & Clark 2004). However, the number of human resources is the criterion most frequently used by governments and researchers (Raymond 1990).

Organisations were small, medium or large. We set the sizes by the number of 'people' in the Simul8 models representing these organisations. The numbers of human resources in the small, medium and large organisation were altered to be in line with the relaxed simulation parameters. The 2011 information security and data privacy staffing survey concerns with staffing levels and other properties of the information security function. The percentage of IS staff varied considerably by industry. The more the business operations depend on information, the higher the percentage of IS staff. Across all industries and regions, IS staff represent roughly 0.5% of all full-time employees (FTE) jumped 880% since the previous survey which was conducted in 1997. That is,

information security staff now constitutes one out of every 200 employees (Wood 2011).

In this research, the number of IS staff required for simulating small organisation was defined with consideration to the following criteria:

- To avoid inappropriate queues
- To avoid any blockage in the system which would lead to unreliable data
- To ensure only few incidents remain to be processed by the end of the simulation run
- Queues are largely emptied

It has been found that to meet these criteria, 7 information security staff were required for simulating small organisation. For medium organisation, double the number of IS staff in small organisation was used to define the number of IS staff required which was 14 and 28 for large organisation which is double the size of medium organisation. Based on the percentage of IS staff to the total workers defined by the 2011 survey, this means that the total number of the FTE in small, medium, and large organisations defined in this research are 1400, 2800, and 5600. These figures coincide with the classifications of organisation sizes defined by (Wood 1990).

Table 5-4 shows the number of people at each organisation size after relaxing the simulation parameters. The numbers were broken down into the security teams operating in each.

Table 5-4: Human resources in different organisation sizes after relaxing simulation parameters

Security system	Security team	Number of resources			
		HP model	Relaxed models		
			Small org.	Med. org.	Large org.
	PoC	144	1	2	4
System #1	ISIRT	122	2	4	8
	Crisis	6	1	2	4
System #3	Crises	1	1	2	4
System #4	Crises	1	1	2	4
System #5	Crises	1	1	2	4
Total		**275**	**7**	**14**	**28**

The number of people in the HP model was extremely large (over 250), because it represented an organisation providing outsourcing services for other client organisations. The relaxed models required far fewer human resources to yield reasonable results.

5.2.4 Simulation Time

When simulation times are fixed, different numbers of SSC can be reported due to the impact of variation in organisation size and threat intensity. The minimum reported number of SSC is 105, which is the required sample size computed for the experiment. Table 5-5 shows the different number of reported SSC, as organisation size and threat intensity vary with a fixed simulation time.

On the other hand, when the simulation time is unfixed, the same number of SSC can be reported, that is 105, regardless of variation in organisation size and level of threat intensity, as shown in Table 5-6.

To investigate whether the time taken in the simulation had any impact on the time taken to report SSC, we defined two levels. The first level was the fixed simulation time

taken to generate different numbers of SSC in different organisation sizes and levels of threat intensity. The second level was an unfixed simulation time taken to generate the same number of SSC.

Table 5-5: Number of reported SSC using the fixed simulation time taken

Organisation size	Threat intensity	Simulation time (h)	Reported SSC
Large	Low	75600	105
Medium	Low	75600	105
Small	Low	75600	105
Large	Medium	75600	210
Medium	Medium	75600	210
Small	Medium	75600	210
Large	High	75600	420
Medium	High	75600	420
Small	High	75600	420

Table 5-6: Reported SSC when using an unfixed simulation time taken

Organisation size	Threat intensity	Simulation time (h)	Reported SSC
Large	Low	75600	105
Medium	Low	75600	105
Small	Low	75600	105
Large	Medium	37800	105
Medium	Medium	37800	105
Small	Medium	37800	105
Large	High	18800	105
Medium	High	18800	105
Small	High	18800	105

5.3 Methodology

We ran the ISG baseline model and the VSMISG described in Chapter 4 and relaxed at the beginning of this chapter. We ran 36 simulations for the 3 X 3 X 2 X 2 factorial experiment to investigate effects of organisation size, threat intensity, model, and

simulation time. Using GPower software, the sample size was determined as N = 105, that is, 105 SSC were required. The effect size, error Type I probability and power were determined as 0.5, 0.05 and 0.95, respectively. The allocation ratio was set to one, because all sample sizes were equal. Figure 5-2 shows the parameters used to calculate sample size.

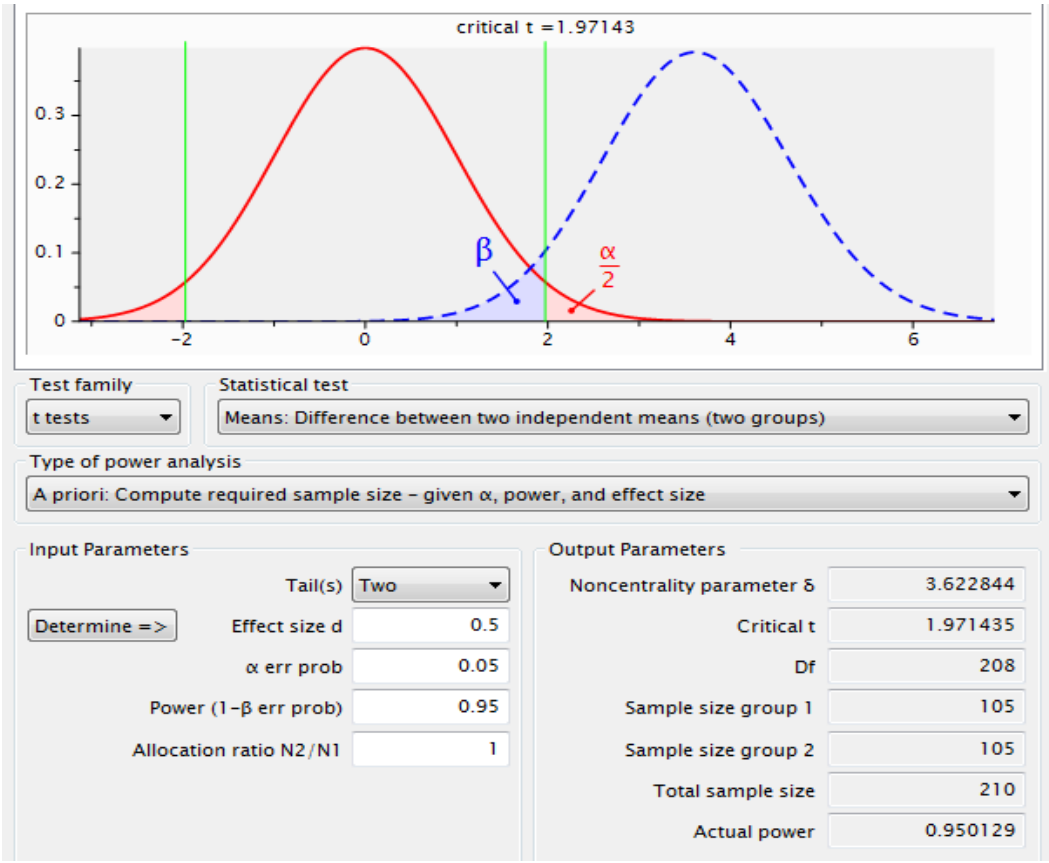


Figure 5-2: Sample size calculation

Table 5-7 illustrates the experiment to run 36 simulations. The number of SSC generated in each simulation is 105. There was no specific order followed in running these simulations. We ran 18 simulations for the baseline model, and in nine of these we fixed the simulation time and in the other nine we did not, to examine whether the time taken to report SSC is impacted by differences in the simulation time. Each of the simulations involved the same combination of organisation size and threat intensity variations, as shown in Table 5-7.

Table 5-7: Experiment design and the number of simulations conducted

Model		**Baseline**						**VSMISG**					
Simulation time		**Fixed**			**Unfixed**			**Fixed**			**Unfixed**		
Organisation size		Large	Medium	Small	Large	Medium	Small	Large	Medium	Small	Large	Medium	Small
Threat intensity	Low												
	Medium												
	High												

Another 18 simulations were conducted for the VSMISG. We followed the same design of simulation time, organisation size and level of threat intensity in the baseline model shown in Table 5-7. The only change was that we used the VSMISG instead of the baseline model, to investigate whether there was a difference in the time taken to identify SSC when we used the VSMISG.

We used the Analysis of Variance (ANOVA) statistical model to analyse the data. It is the most efficient parametric method available (Armstrong et al. 2002) and is used to understand the interactions between groups. We tested two assumptions of ANOVA: the homogeneity of variances and the normality of the distribution of SSC reporting times for each combination of the groups. The results showed that the normality assumption was violated for all the groups – Figure 5-3 shows normality test histograms for some of the experimental groups.

The assumption of the homogeneity of variance was also violated for all experimental groups. In this case, however, other techniques can be considered such as data transformation (Shapiro & Wilk 1972; Field 2002). We tried to transform the data using the log10 function and the results showed some improvement, but the normality and homogeneity of variance assumptions remained violated. Figure 5-4 shows some normality test histograms after transformation. Although these results were a discouragement to use ANOVA in the experiment, Field has identified that the technique is fairly robust when sample sizes are large and equal (Field 2002). Accordingly, we proceeded to use ANOVA on the original data as all the sample sizes are indeed equal and large.

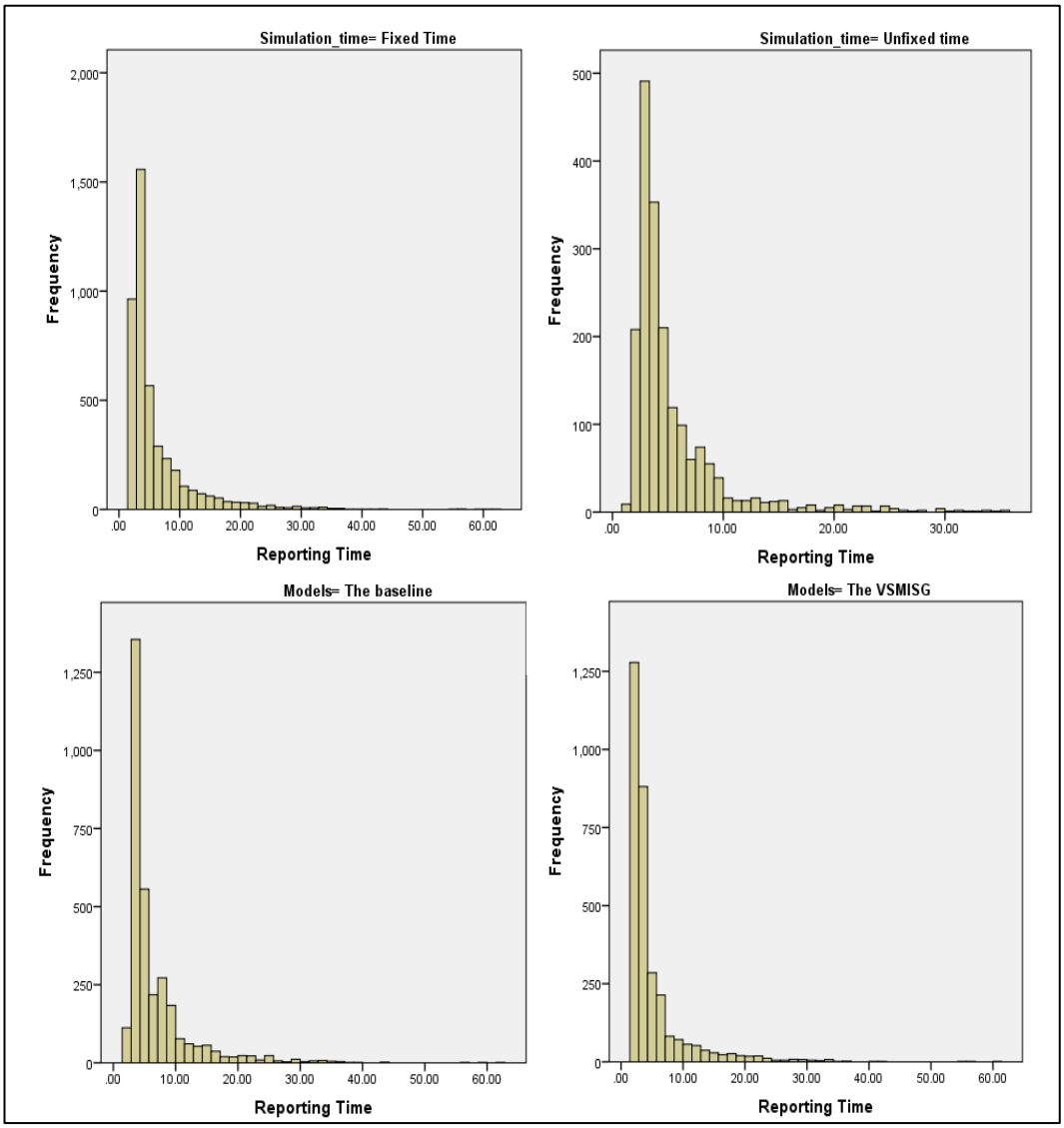


Figure 5-3: Normality test histograms of some experimental groups

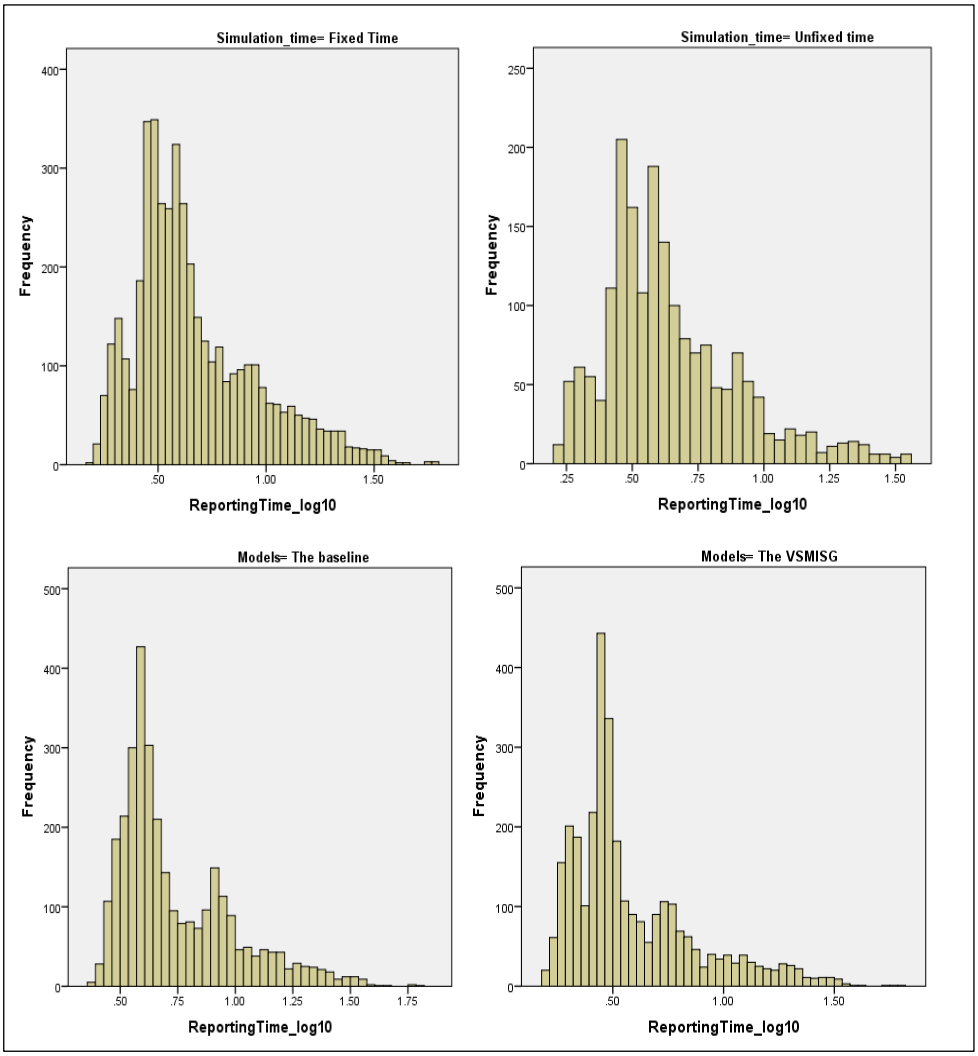


Figure 5-4: Normality test histograms after transformation

5.4 Results and Analysis

A factorial ANOVA was performed to identify the interaction and group differences in organisation size, level of threat intensity, model and simulation time. In the following sections we present the results of the interactions of four, three and two factors in the experiment.

5.4.1 Interaction between Organisation Size, Model, Simulation Time and Threat Intensity

Table 5-8 shows the results of the experiment. The results revealed a non-significant four-factor interaction effect between simulation time, threat intensity, organisation size

and model on the time taken to identify SSC, F (4, 36) = 0.156, p> .05. None of the three-factor interactions were significant, but two significant two-factor interaction effects were detected. The first was between organisation size and model, while the second was between organisation size and threat intensity. The main effect of simulation time taken may only be interpreted, as it was not involved in any statistically significant interaction; its effect was not significant, as can be seen in Figure 5-5. The statistical results of the effect of simulation time taken is shown in Table 5-9.

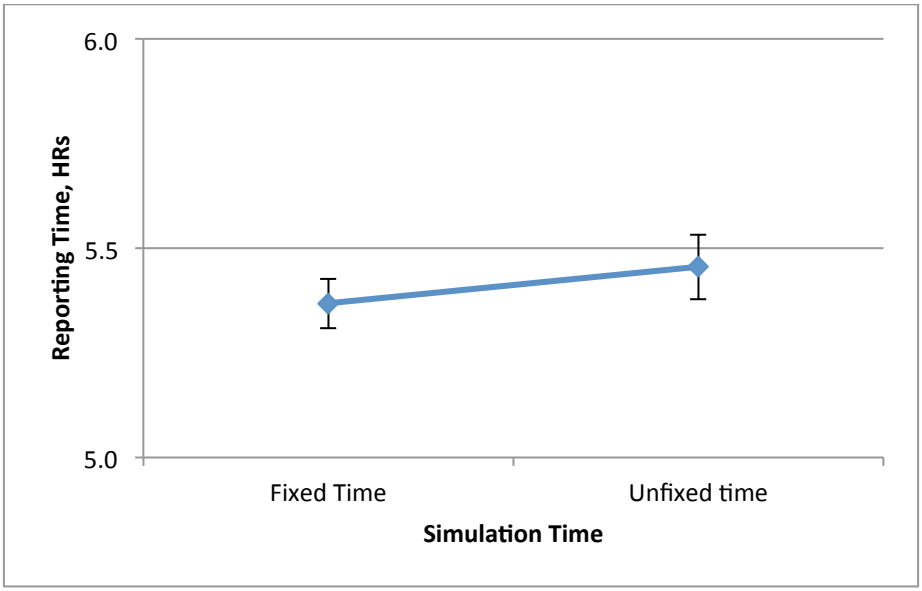


Figure 5-5: Comparison effect of simulation time taken

Table 5-8: Tests of between-subjects effects

Source	Type III Sum of Squares	df	Mean Square	F	P
Model	337882.626	36	9385.628	835.344	<.000
Simulation_time	9.127	1	9.127	.812	.367
Threats_intensity	10611.849	2	5305.924	472.241	<.000
Organisation_size	41482.255	2	20741.127	1846.012	<.000
Models	3228.840	1	3228.840	287.375	<.000
Simulation_time * Threats_intensity	32.998	2	16.499	1.468	.230
Simulation_time * Organisation_size	8.309	2	4.154	.370	.691
Simulation_time * Models	.145	1	.145	.013	.909
Threats_intensity * Organisation_size	17877.372	4	4469.343	397.783	<.000
Threats_intensity * Models	2.172	2	1.086	.097	.908
Organisation_size * Models	427.032	2	213.516	19.003	<.000
Simulation_time * Threats_intensity * Organisation_size	44.807	4	11.202	.997	.408
Simulation_time * Threats_intensity * Models	5.390	2	2.695	.240	.787
Simulation_time * Organisation_size * Models	.236	2	.118	.010	.990
Threats_intensity * Organisation_size * Models	4.827	4	1.207	.107	.980
Simulation_time * Threats_intensity * Organisation_size * Models	7.000	4	1.750	.156	.960
Error	70391.281	6265	11.236		
Total	**408273.907**	**6301**			

Table 5-9: Statistical result of simulation time effect

			95% Confidence Interval	
Simulation time	**Mean**	**Std. Error**	**Lower Bound**	**Upper Bound**
Fixed time	5.368	.059	5.252	5.483
Unfixed time	5.455	.077	5.304	5.606

5.4.2 Interaction between Organisation Size and Model

The results showed that there was a statistically significant interaction effect between organisation size and model, F (2, 36) = 19, $p < .05$. However, plotting the organisation size against the models showed a similar profile for both the baseline and VSMISG models for all sizes of organisation.

Figure 5-6 compares the mean reporting time at different organisation sizes for the baseline and VSMISG models. It shows that there was a difference between the small and medium organisations, between the small and large organisations, and between the medium and large organisations. These are statistically significant, as can be seen by the absence of overlap between the mean standard errors.

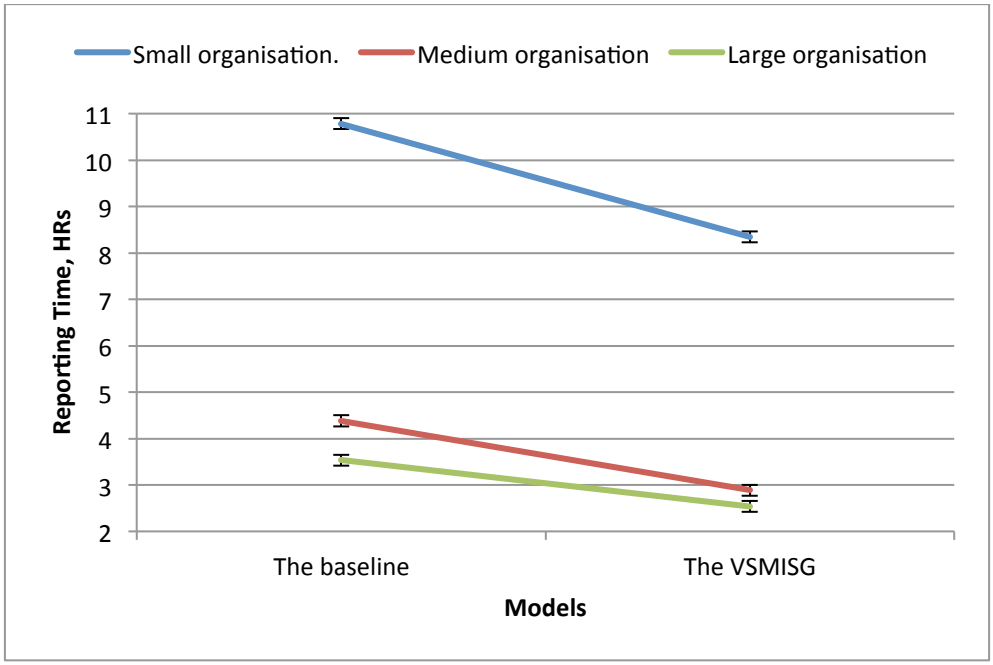


Figure 5-6: Comparison of mean reporting times for different organisation sizes and models

Another view of the same data shows the difference between the models for different organisation sizes. Figure 5-7 displays the mean reporting time taken in the baseline and VSMISG models for each organisation size, showing there was a difference between the mean reporting time in each model at each level of organisation size. This difference was statistically significant, as seen by the absence of overlap between the mean standard errors.

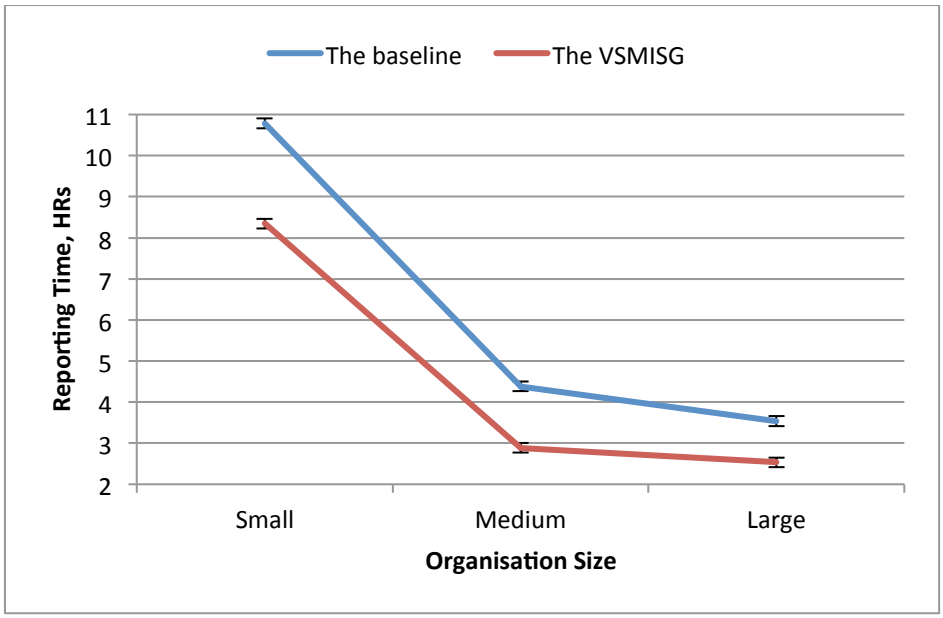


Figure 5-7: Comparison of mean reporting times in baseline model and VSMISG for different organisation sizes

Despite the overall similarity of the profiles, the statistically significant interaction between organisation size and model required further analysis. This was examined using pairwise comparison.

Figure 5-8 shows the trend of the difference in means for the baseline and VSMISG models at each size of organisation. It can be seen that the greatest difference was found in the small organisation, while the least difference was in the large organisation. There was no overlap between the means difference standard errors, indicating significant differences between the models at each size of organisation that is inherent in the interaction between size and model.

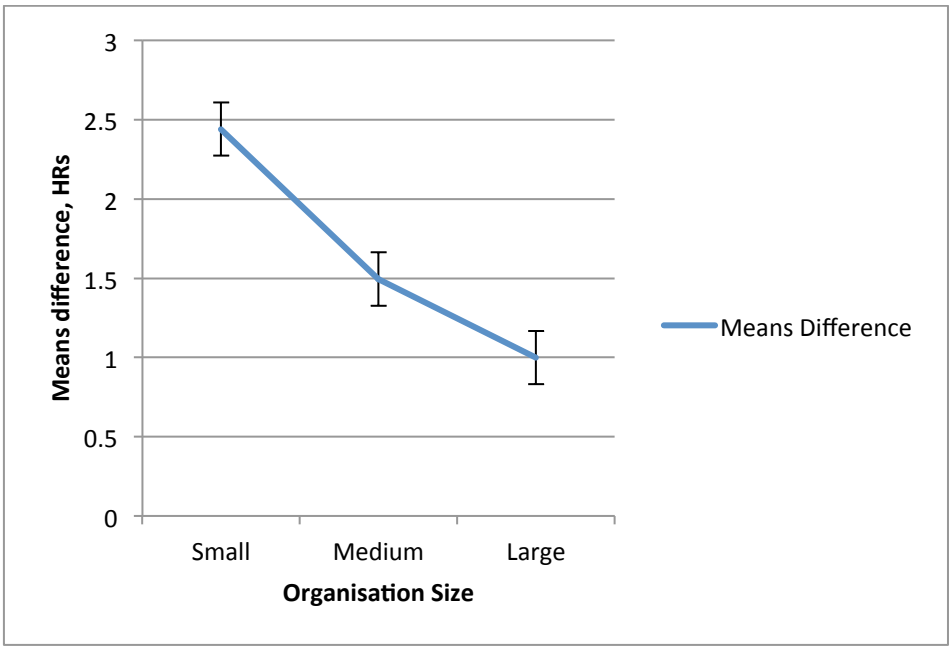


Figure 5-8: Comparison of mean differences of the baseline model and VSMISG for different organisation sizes

Table 5-10 shows the mean reporting time of the interaction effect between the levels of models and the levels of organisation size, while Table 5-11 shows a pairwise comparison of the two factors.

Table 5-10: Statistical results of organisation size and model interaction

Organisation size	Models	Mean	Std. Error	95% Confidence Interval	
				Lower Bound	Upper Bound
Small	Baseline	10.786	.119	10.553	11.019
	VSMISG	8.345	.119	8.112	8.578
Medium	Baseline	4.380	.119	4.148	4.613
	VSMISG	2.887	.119	2.654	3.120
Large	Baseline	3.535	.119	3.302	3.768
	VSMISG	2.536	.119	2.303	2.769

Table 5-11: Pairwise comparison between organisation size and models

Organisation size	(I) Models	(J) Models	Mean Difference (I-J)	Std. Error	P	95% Confidence Interval for Difference	
						Lower Bound	Upper Bound
Small	Baseline	VSMISG	2.441*	.168	<.000	2.111	2.770
	VSMISG	Baseline	-2.441*	.168	<.000	-2.770	-2.111
Medium	Baseline	VSMISG	1.494*	.168	<.000	1.164	1.823
	VSMISG	Baseline	-1.494*	.168	<.000	-1.823	-1.164
Large	Baseline	VSMISG	.999*	.168	<.000	.670	1.329
	VSMISG	Baseline	-.999*	.168	<.000	-1.329	-.670

5.4.3 Interaction between Organisation Size and Threat Intensity

The results shown in Table 5-8 indicate that there was a statistically significant interaction effect between organisation size and threat intensity F (4, 36) = 397.78, p < .05. Figure 5-9 displays the mean reporting time of the levels of organisation size at different intensities of threats. It shows that there was a significant difference between the small and medium organisation, and the small and large organisation, at each level of threat intensity.

A small difference between the medium and large organisation at high and medium levels of threat intensity can be seen, while no statistical significant difference at a low threat intensity was found, as indicated by the overlap of their means standard errors. It can be seen that the greatest significant difference was in the small organisation, at apparently high threat intensities.

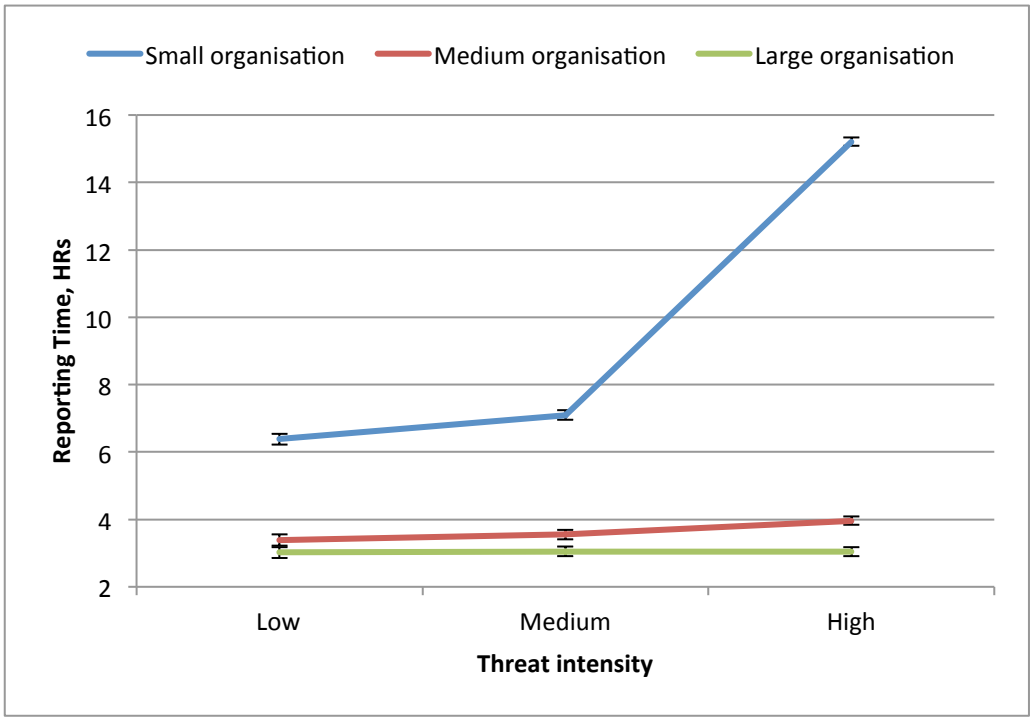


Figure 5-9: Comparison of mean reporting times at different levels of threat intensity and organisation size

Another view of the same data shows the difference between the levels of threat intensity at different organisation sizes. Figure 5-10 shows the trend of the mean

reporting time taken at varying levels of threat intensity in the small, medium and large organisation.

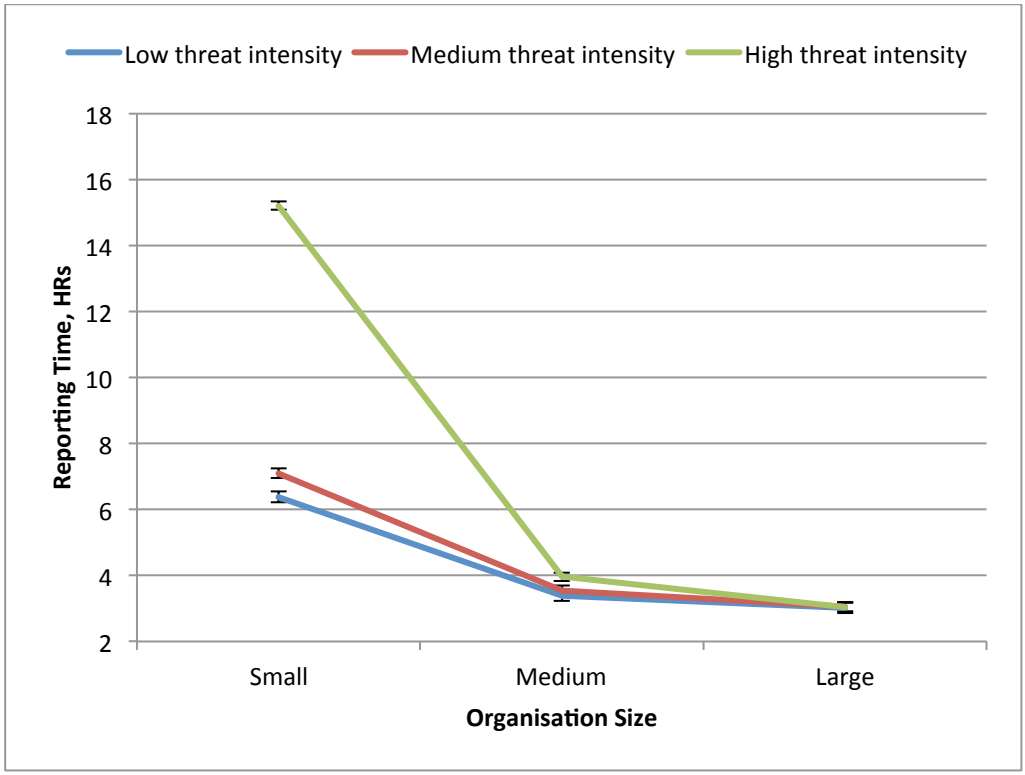


Figure 5-10: Comparison of mean reporting times at varying levels of threat intensity and organisation size

It shows that there was a statistically significant difference between high and medium, and high and low levels of threat intensity in a small organisation. While there was no statistically significant difference seen between levels of threat intensity in the large organisation, there was a small statistically significant difference between high and medium, and between high and low threat intensities in the medium-size organisation.

In the small organisations, there was a statistically significant difference between medium and low levels of threat intensity, but no significant difference was seen between these in the medium and large organisations.

In the large organisation, there was no difference found between the levels of threat intensity. The greatest statistically significant difference was seen was in the small organisation when threat intensity was high, while the smallest statistically significant difference was seen in the medium organisation between high and medium

levels of threat intensity. Table 5-12 shows the statistical results of the interaction between threat intensity and organisation size.

Table 5-12: Statistical results of interaction between organisation size and level of threat intensity

Threat intensity	Organisation size	Mean	Std. Error	95% Confidence Interval	
				Lower Bound	Upper Bound
Low	Small	6.385	.164	6.065	6.706
	Medium	3.386	.164	3.065	3.706
	Large	3.019	.164	2.698	3.340
Medium	Small	7.098	.142	6.821	7.376
	Medium	3.551	.142	3.273	3.829
	Large	3.048	.142	2.770	3.325
High	Small	15.213	.129	14.960	15.467
	Medium	3.964	.129	3.710	4.217
	Large	3.040	.129	2.786	3.293

5.5 Summary

In this chapter we investigated the impact of the VSMISG for the three organisation sizes at different levels of threat intensity and simulation duration. The experimental factors and the simulations design were described. We ran 18 simulations on the ISG baseline model with variations in the levels of organisation sizes, threat intensity, and simulation time, and another 18 with the same variations on the VSMISG.

The results showed that there were no four-factor or three-factor interactions among organisation size, model, threat intensity and simulation times, but that there were two two-factor interaction effects. The first was between model and organisation size, and the second was between organisation size and level of threat intensity. There was no significant main effect of simulation time.

Chapter 6. Cost–Benefit Analysis

We conducted Cost–Benefit Analysis (CBA) to investigate the economic aspects of implementing the VSMISG. This was to enable an informed decision to be made on the use of the VSMISG on economic grounds, as it allocates a monetary value to the benefits. It is useful in model evaluation as it compares models to see which achieves the greatest benefit (Cellini & Kee 2010). This chapter aims to answer the following research question:

RQ8 *Is using the VSMISG more beneficial than using the baseline ISG model?*

The costs associated with information security operations include expenses for software, hardware, office requirements, training and human resources; further costs are found in Harris (2008), Witty (2001) and Roper (1999). The benefits that may be achieved include organisation viability, better reputation and compliance with regulations; other benefits are identified in Kim and Lee (2005) and Scott (1998). Although information security managers recognise that precise metrics for measuring benefits are unobtainable, they are able to make estimates (Butler 2002).

The Net Present Value (NPV) is an important calculation for CBA and is considered the ideal economic method to budget for information security expenditure (Cellini & Kee 2010). It requires organisations to weigh expected benefits against future expected information security expenditure in monetary terms. Additional expenditure is acceptable if the monetary value of the expected benefits exceeds the expenditure. Implementing a model is acceptable if its NPV is greater than zero, but should be rejected if it is equal or less than zero (Gordon & Loeb 2006). To calculate the net present value of costs and benefits, CBA analysts use a percentage known as a discount rate.

To assess the value of a model based on whether a specific percentage rate of return is acceptable comparing to other opportunities, CBA analysts use what is known as the Internal Rate of Return (IRR). The IRR is the discount rate when the total present value of benefits equal to costs. The higher the IRR, the more desirable it is to implement the model. They also calculate what is known as a payback period, namely the period of time required to regain funds spent on an investment (Cheng et al. 1994).

Another financial method that can be used in assessing models is the profitability index, calculated as the ratio of estimated present value of positive Cash Flows (CF) to estimated present value of start-up costs. Implementing a model is considered profitable when the profitability index or ratio is greater than one. Conversely, if the profitability index below one, the action may be to reject the implementation of the model (Miller 1987).

The figures of the input for the cost benefit analysis came from three ways: results from simulation experiment of this research, assumptions, and from recruitment websites such as www.total jobs.com and www.indeed.com. These websites make announcement for current openings of job positions including IS jobs such as IS technician, engineer, manager, crisis manager, CISO, and CIO. These websites also show salary of these jobs. These salaries were used to define the input for the cost benefit analysis in this research.

In the following sections, we analyse the costs and benefits of implementing the VSMISG in a medium size organisation over three years. The number of SSCs per year was eight based on the results of simulation run, resulting in 24 SSCs over three years. We defined the items of the start-up costs, operating costs and benefits. The results of the CBA can be scaled for large and small organisations. The results of the NPV, IRR, profitability index, and payback period are given at the end of this chapter.

6.1 Operating Costs

Operating costs are the running expenses for organisational assets including hardware, software and human resources to ensure the continuity of the operations. We defined four operating cost items for the cost and benefits analysis: human resources; office requirements; computer provision and training.

The number of people in the baseline ISG and VSMISG models did not change. We considered their deployment at the models' design stage; that is, the same number was used in both. This means that the costs of human resources, their training and relevant office requirements were identical.

6.1.1 Human Resources

To calculate the costs of human resources we identified the number of people working in both models. There were six security teams, namely Point of Contact (PoC), Information Security Immediate Response Team (ISIRT), crisis team, System #3 team, System #4 team and System #5 team.

The number of human resources in each model was 14. We identified the hourly rate for all the defined teams based on figures published by online recruiting organisations. The number of working hours per year was 2880, based on an eight-hour working day as defined in the simulation design. The cost of a resource was given by multiplying 2880 by the hourly rate for that resource. Inflation was defined as 3 percent and calculated in the second and third years. Table 6-1 shows the costs of human resources over three years for each model.

Table 6-1: Costs of human resources for each model in three years

Security team	Hourly rate (£)	No. people	No. hours per year	Cost (£)		
				Y1	Y2	Y3
PoC	6	2	2880	34,560	35,597	36,665
ISIRT	12	4		138,240	142,387	146,659
Crises	15	2		86,400	88,992	91,662
System #3	18	2		103,680	106,790	109,994
System #4	30	2		172,800	177,984	183,324
System #5	34	2		195,840	201,715	207,767
Total		**14**		**731,520**	**753,465**	**776,071**

6.1.2 Office Requirements, Computer Provision and Training

The cost of office requirements was estimated at £12,000 per annum per person, to cover rent, gas, electricity and communication expenses. For everyone, the annual cost of office requirements under each model was calculated as £168,000.

The cost of computer provision including hardware, software and maintenance was estimated as £1000 per annum per person. For everyone, the annual cost of computer provision in each model was calculated as £14,000.

Training costs were estimated as £1000 per annum per person to cover training courses and materials. For everyone, the annual cost of training under each model was calculated as £14,000. Table 6-2 shows the operating cost of office requirements, computer provision and training for each model. The costs were different in each year because we calculated the inflation rate as 3 per cent over the three years.

Table 6-2: Costs of office requirements, computer provision, and training for each model for three years

Cost of item	Annual cost per person (£)	No. people	Cost (£)		
			Y1	Y2	Y3
Office requirements	12,000		168,000	173,040	178,231
Computer provision	1,000	14	14,000	14,420	14,853
Training	1,000		14,000	14,420	14,853

6.2 Start-up Costs

There are some costs that need to be paid in advance in order to implement the VSMISG. These costs are known as start-up costs or initial investment. To implement the VSMISG, the organisation needs to achieve the following:

1. Design, implement and test a direct reporting channel between information security operations and policy systems
2. Deactivate, check, and remove regular reporting channel between information security planning and policy systems
3. Train four crisis team members.

A good system programmer is required to implement Requirements Numbers 1 and 2 above. We assumed that the salary of a good system programmer is £80,000 per year. On top of that, we added another £80,000 for full economic costing, calculated as the salary per annual plus 100 per cent. The total cost of the system programmer per annum is £160,000.

We estimated that the system programmer needs four weeks to design, implement and test a direct reporting channel and two weeks to deactivate, remove and check the routine reporting channel. Table 6-3 shows the cost of the system programmer to achieve the requirements for implementing the VSMISG.

Table 6-3: Cost of the system programmer to achieve the requirements for implementing VSMISG

Programmer salary (£)	Requirements	Duration (week)	Cost (£)
160,000	Design, implement and test a direct reporting channel	4	13,333
	Deactivate, check, and remove regular reporting	2	6,667

For the training requirements, we estimated that the four members of the crisis team needed three days' training on how to deal with the new design to report SSC appropriately to the information security policy system. We set the cost per training day per person to be £500. Table 6-4 shows the total cost of training the crisis team.

Table 6-4: Cost of training the crisis team

Training duration (day)	No. trainees	Cost per day (£)	Total cost (£)
3	4	500	6000

6.3 Benefits

We defined three benefits items: organisational viability; reputation; and compliance with regulations, to calculate the benefits of the change from using the baseline ISG model to using the VSMISG. The benefits were calculated by determining the difference between the cost of the VSMISG and the baseline ISG model.

6.3.1 Organisational Viability

Viable organisations strive to avoid or at least limit damage that may hinder the continuity of critical services. Reporting strategic security crises directly to Information security policy system #5 enables faster response and limits non-inevitable damage. Organisation viability is one of the benefits of implementing the VSMISG. We valued this by determining the reporting time by which System #5 becomes aware of SSC and the cost of that time in the baseline ISG and VSMISG models.

The reporting time is that by which System #5 becomes aware of possible disruption to organisation-critical operations to be able to respond. The faster System #5 becomes aware of SSC, the faster it responds to preserve organisational viability.

From the simulation of medium-sized organisation, we determined the reporting times of the SSC over the three simulated years. The number of SSC in each simulated year was eight. Table 6-5 shows the SSC reporting time in the baseline ISG and VSMISG models over the three years.

To determine the cost of SSC per hour, we created a scenario of disruption to an organisation's operations. We assumed there were cybercriminals who committed financial fraud and caused disruption to business operations in a medium sized organisation. According to Gartner,[2] an advisory firm providing technology-related insights, annual revenues of medium sized organisations is £32,792,482–£655,786,759. We estimated the annual revenue of a medium sized organisation to be £344,289,621 (i.e. the middle value between the upper and lower limits, representing an 'average'). From this simulation of a medium-sized organisation, the number of simulated hours per year was 2880. As a result, business loss during disruption was £119,545 per hour.

Table 6-5: Reporting time in the baseline ISG model and VSMISG

Model	Year	Reporting time (h)							
		SSC1	SSC2	SSC3	SSC4	SSC5	SSC6	SSC7	SSC8
Baseline	1	2.48	1.85	2.23	2.06	1.95	2.71	2.5	1.94
	2	2.32	2.32	2.45	2.12	2.69	2.03	2.04	2.32
	3	2.05	2.13	2.18	2.39	2.32	2.17	2.13	1.86
VSMISG	1	0.69	0.65	0.95	0.75	0.5	0.75	0.9	0.83
	2	0.68	0.82	0.87	0.5	0.85	0.84	0.65	0.58
	3	0.56	0.79	0.96	0.71	0.82	0.81	0.8	0.63

[2] http://www.gartner.com/it-glossary/smbs-small-and-midsize-businesses

Having determined the SSC reporting times in the three simulated years and the cost of disruption per hour, we calculated the cost of reporting SSC, by multiplying the reporting time of that SSC to the cost of disruption per hour. Table 6-6 shows the cost of reporting time over three simulated years for the baseline ISG and VSMISG models. This table was used in calculating the costs of reputation and compliance with regulations in next sections.

Table 6-6: Total organisation viability cost in the baseline ISG model and VSMISG

Model	Year	Organisation viability cost per SSC (£)								Total viability cost
		SSC1	SSC2	SSC3	SSC4	SSC5	SSC6	SSC7	SSC8	
Baseline	1	296,472	221,158	266,585	246,263	233,113	323,967	298,863	231,917	**2,118,337**
	2	277,344	277,344	292,885	253,435	321,576	242,676	243,872	277,344	**2,186,478**
	3	245,067	254,631	260,608	285,713	277,344	259,413	254,631	222,354	**2,059,760**
VSMISG	1	82,486	77,704	113,568	89,659	59,773	89,659	107,591	99,222	**719,661**
	2	81,291	98,027	104,004	59,773	101,613	100,418	77,704	69,336	**692,166**
	3	66,945	94,441	114,763	84,877	98,027	96,831	95,636	75,313	**726,834**

6.3.2 Reputation

Reputation can be defined as the set of common opinions that forms a level of trust when these are combined (Preece et al. 2005). To calculate the benefit of reputation in the baseline and VSMISG models, we first identified the reputation decline percentages. The reputation value can decline as much as by 17 per cent to 31 per cent of annual gross revenue (Ponemon Institute 2011). We defined the average reputation decline as 25 per cent of the annual gross revenue, and as a result, the average reputation cost per annual was defined as £86,072,405. Then, the reputation cost per hour of disruption was calculated to be £29,886, by dividing the average reputation cost per annum by 2880, the number of simulated hours per year.

Having defined the average reputation cost per hour, we calculated the reputation costs incurred in three simulated years as a result of the SSC occurrences under both the baseline ISG and VSMISG models. The number of the SSCs per one simulated year was eight. We calculated the reputation cost by multiplying the reporting times of SSCs per hour as they appear in Table 6-5 to the defined reputation cost per hour, £29,886. Table 6-7 shows the total reputation costs of the baseline ISG and VSMISG models over three simulated years.

6.3.3 Compliance with Regulations

Organisations that do not comply with data protection laws and regulations face penalties that can be as high as 5 per cent of annual gross revenue (Hornung 2012; Trend Micro 2014). Information security governance must ensure data protection measures in order to ensure organisation viability. The VSMISG is composed of viable security systems and principles that work together to preserve organisation viability.

We defined the average compliance penalty percentage to be 2.5 per cent of the annual gross revenue. As a result, the average compliance penalty cost per annual was defined as £8,607,241. Then, the compliance penalty cost per hour of disruption was calculated as £2989, by dividing the average compliance penalty cost per annum by 2880, the number of simulated hours per year.

Table 6-7: Total reputation cost of using the baseline ISG model and VSMISG

Model	Year	Reputation cost per SSC (£)								Total reputation cost
		SSC1	SSC2	SSC3	SSC4	SSC5	SSC6	SSC7	SSC8	
Baseline	1	74,117	55,289	66,646	61,565	58,278	80,991	74,715	57,979	**529,580**
	2	69,336	69,336	73,221	63,358	80,393	60,669	60,967	69,336	**546,615**
	3	61,266	63,657	65,151	71,428	69,336	64,853	63,657	55,588	**514,936**
VSMISG	1	20,621	19,426	28,392	22,415	14,943	22,415	26,897	24,805	**179,914**
	2	20,322	24,507	26,001	14,943	25,403	25,104	19,426	17,334	**173,040**
	3	16,736	23,610	28,691	21,219	24,507	24,208	23,909	18,828	**181,707**

Having defined the average compliance penalty cost per hour, we calculated the compliance penalty costs incurred over three simulated years as a result of the SSC occurrences under both the baseline ISG model and VSMISG. The number of SSC per simulated year was eight. We calculated the compliance penalty cost by multiplying the reporting times of SSC per hour as they appear in Table 6-5 to the defined penalty cost per hour, £2989. Table 6-8 shows the total compliance penalty costs of the baseline ISG and VSMISG models over three simulated years.

Having calculated the items of the costs and benefits of the baseline ISG model and VSMISG, and the start-up cost, we calculated the cash flows (CF) of using the models.

Table 6-8: Total compliance penalty costs of the baseline ISG model and VSMISG over three years

Model	Year	Penalty cost per SSC (£)								Total penalty cost
		SSC1	SSC2	SSC3	SSC4	SSC5	SSC6	SSC7	SSC8	
Baseline	1	7,413	5,530	6,665	6,157	5,829	8,100	7,473	5,799	**52,965**
	2	6,934	6,934	7,323	6,337	8,040	6,068	6,098	6,934	**54,669**
	3	6,127	6,367	6,516	7,144	6,934	6,486	6,367	5,560	**51,500**
VSMISG	1	2,062	1,943	2,840	2,242	1,495	2,242	2,690	2,481	**17,994**
	2	2,033	2,451	2,600	1,495	2,541	2,511	1,943	1,734	**17,306**
	3	1,674	2,361	2,869	2,122	2,451	2,421	2,391	1,883	**18,173**

6.4 Costs of the Baseline ISG Model and VSMISG

In previous sections we calculated the cost items of the baseline ISG and VSMISG models. In this section, we calculate the total cost of using the baseline ISG and VSMISG models by adding up the cost items for each. Table 6-9 and 6-10 show the costs of the baseline ISG and VSMISG models respectively.

Table 6-9: Costs of baseline ISG model

Costs	Year		
	1	2	3
HR	-731,520	-753,465	-776,071
Office requirements	-168,000	-173,040	-178,231
Computer provision	-14,000	-14,420	-14,853
Training	-14,000	-14,420	-14,853
Organisation viability	-2,118,337	-2,186,478	-2,059,760
Reputation	-529,580	-546,615	-514,936
Regulatory penalty	-52,965	-54,669	-51,500
Total	**-3,628,402**	**-3,743,107**	**-3,610,204**

Table 6-10: Costs of VSMISG

Costs	Year		
	1	2	3
HR	-731,520	-753,465	-776,071
Office requirements	-168,000	-173,040	-178,231
Computer provision	-14,000	-14,420	-14,853
Training	-14,000	-14,420	-14,853
Organisation viability	-719,661	-692,166	-726,834
Reputation	-179,914	-173,040	-181,707
Regulatory penalty	-17,994	-17,306	-18,173
Total	**-1,845,089**	**-1,837,857**	**-1,910,722**

6.5 Start-up Costs to Implement VSMISG

In section 6.2, we defined the items of the start-up and their costs. Table 7-11 shows the total investment at start-up.

Table 6-11: Total investment at start-up

Requirements	Year 0
Design, implement and test a direct reporting channel	-13,333
Deactivate, remove, and check regular reporting channel	-6,667
Training crises team (4 resources)	-6,000
Total investment at start-up	**-26,000**

6.6 Cost–Benefit Analysis of Change from Baseline ISG Model to VSMISG

Having defined the costs of the baseline ISG and VSMISG models, and the start-up costs of implementing the VSMISG, we calculated the costs and benefits analysis of change from the baseline ISG model to the VSMISG. We calculated the differences between the costs of both models in order to calculate the cash flow of the change.

Table 6-12 shows the costs and benefits analysis of change from the baseline ISG model to the VSMISG. It reveals the start-up costs in Year 0, the result of the calculations shown in Table 6-11, the benefits from change in costs and the cash flow change.

Table 6-12: Cost–benefit analysis of change from baseline ISG model to VSMISG

	Year 0	Year 1	Year 2	Year 3
Investment cost				
	-26,000			
Benefits from change in costs				
		1,783,313	1,905,250	1,699,482
Cash flow change				
	-26,000	1,783,313	1,905,250	1,699,482

The values of the benefits change were the result of subtracting the total cost of the VSMISG shown in Table 6-10 from the total cost of the baseline ISG model, shown in Table 6-9, for each year.

We used the built-in NPV and IRR functions in Microsoft Excel to calculate the NPV and IRR, while the profitability index was calculated by dividing the NPV by the start-up cost. When calculating the NPV, it is recommended to use a discount rate of 2–3 per cent (Cellini & Kee 2010). The discount rate we used in calculating the NPV was 3 per cent.

For the payback calculation, we used Table 6-13 to calculate the two payback approaches: the simple and discounted payback. We divided the value of the start-up cost in Year 0 by the first positive value of the cash flow to determine the simple payback. We followed the same calculation with the discounted cash flow in order to determine the discounted payback.

Table 6-13: Payback calculation

	Year 0	Year 1	Year 2	Year 3
Cash flow change	-26,000	1,783,313	1,905,250	1,699,482
Discount cash flow change	-26,000	1,731,372	1,795,881	1,555,267

6.7 Results and Analysis

We calculated the NPV, IRR, payback and profitability index to investigate whether implementing the VSMISG is financially better than the baseline model. Table 6-14 shows the results of the financial methods we used in assessing the profitability of implementing the VSMISG.

Table 6-14: Financial methods results of implementing VSMISG

Financial method		Value
NPV		£5,056,519
IRR		6865%
Payback period	Simple	0.15 years
	Discounted	0.15 years
PI (profitability index)		£194

The NPV of implementing the VSMISG is far greater than zero. The value of the revenues is greater than the costs, indicating an increase in the wealth of organisations or investors adopting the VSMISG. The result of the IRR showed a high discount rate, greater than the current recommended discount rate.

The results showed that the start-up costs for implementing the VSMISG were recovered early time in Year 1. Examining the discounted cash flow, which was smaller, resulted in a discounted payback of the same time. The profitability index was found greater than one, indicating that implementing the VSMISG is profitable. The value of each £1 invested in implementing the VSMISG worth £194, indicating a sound investment.

6.8 Summary

In this chapter, we investigated the economic aspects of implementing the VSMISG by conducting cost–benefit analysis. The costs of the baseline ISG and VSMISG, and start-up cost for implementing the VSMISG were defined.

The start-up cost of implementing the VSMISG was calculated as £26,000. This included designing, implementing and checking a direct reporting channel between the information security operations and policy systems, and deactivating and removing the regular reporting channel between the planning and policy systems. The start-up cost covered the training expenses for four members of the crisis team.

The costs of organisation viability, reputation, and compliance with regulations of the VSMISG were less than the cost of the baseline ISG model, which made the VSMISG more beneficial than the baseline ISG model. Four financial methods were used to investigate the economics of the VSMISG and each indicated good profitability. Implementing the VSMISG is more profitable than implementing the baseline ISG model.

Chapter 7. Discussion

This chapter first discusses the results of the information security expert review of VSM and its appropriateness for information security governance (section 3.3). It then discusses the results of the inter-rater agreement analysis among the information security experts on the importance of the VSM systems and principles for ISG (sections 0, 3.3.4, and 3.3.5). This is followed by a discussion of the results of investigating the impact of the VSMISG at various sizes of organisation, security threat intensities and simulation times (section 5.4). The chapter concludes by discussing the findings of the costs–benefit analysis in switching from the baseline ISG model to the VSMISG (section 6.7).

7.1 Expert Review of Viable System Model for Information Security Governance (VSMISG)

The VSMISG was reviewed by eleven information security experts to assess the importance of its components; the viable systems and principles for information security governance. Two groups, one from academia and the other comprised of information security practitioners, agreed on the importance of VSM for information security governance. According to Gokhale and Banks (2002), VSM provides a promising route for exploration of the increasing number of security threats that need rapid response at governance level.

The expert review aimed to answer the following research question:

RQ2 What is the importance of the VSM's systems and principles to ISG?

The results showed that the VSM systems and principles were recognised as 'important' and 'very important' components in information security governance. The importance of the VSM's systems and principles to ISG is discussed in the following sections.

7.1.1 Expert Review of VSM Systems

Eleven information security experts rated the importance of the VSM systems to ISG:

Information security policy system #5 is the 'head' security system in organisations. It was defined in section 3.2.2.3 and its importance assessed in section 3.3.1. The average rating of the importance of the Policy system #5 was a 'very important' system for ISG. Policy system #5 plays a vital role for ISG by setting the general security policy, defining the security identity of organisation, establishing the ground for the development of security guidelines and making final decisions regarding long-term security directions.

Information security planning (also called intelligent) system #4 is part of the information security governance level. It was defined in section 3.2.2.3 and its importance rated in section 3.3.1. The average rating of the importance of the Planning system #4 was a 'very important' system for ISG. It plays a key role in ISG by formulating strategic security plans and assessing and managing strategic security environments such as partners, security trends, technologies, regulations, business opportunities and risks.

Information security control system #3 and the compliance monitoring function enhance the cohesion inside organisations through managing resources and performance (Hoverstadt & Bowling 2002). They were introduced in section 3.2.2.2 and their importance was rated in section 3.3.1. The average rating of the importance of the Control system #3 was 'important' for ISG. This means that Control system #3 plays an important role in ISG by formulating operation security policies and providing the necessary resources to Information security operations system #1 for it to accomplish their objectives. Likewise, The average rating of the importance of the Compliance monitoring function was 'important'. It plays an important role in ISG by ensuring that the activities of Information security operations system #1 comply with security policies in order to enhance stabilisation.

The information security coordination system #2 regulates the different parts of information security operations system #1 and resolves possible conflicts between them. It was introduced in section 3.2.2.1 and its importance assessed in section 3.3.1. The average rating of the importance of the Coordination system #2 was 'important' for ISG. This means that Coordination system #2 plays an important role in ISG by stabilising the information security operations system and harmonising its activities.

The information security operations system #1 is concerned with daily operations of monitoring and adapting to dynamic changes in information security environments. It

was introduced in section 3.2.2.1 and its importance rated in section 3.3.1. The average rating of the importance of the Operations system #1 was 'important' for ISG. This means that it plays an important role for ISG by dealing with dynamic changes in information security environments such as vulnerabilities, threats, best practices, procedures and guidelines.

Looking at Figure 3-6, we can see that the security policy and planning systems, which represent the information security governance level, received the highest rating by the experts. This attitude accords with the perspective of ITGI (2006), that is, to achieve effectiveness and sustainability in today's complex, interconnected world, security must be addressed at the highest levels of the organisation. Several sources such as the CGTF (2004), Entrust (2004), Business Software Alliance (2003), Posthumus and von Solms (2004) and von Solms (2006) have asserted that information security management should be directed and controlled by executive management and boards of directors.

7.1.2 Expert Review of VSM Principles

Autonomy is necessary when responding to changes in security environments in order to minimise vulnerability (Lewis 1997). It was introduced in section 3.2.3.1 and its importance rated in section 3.3.2. The average rating of the importance of autonomy was 'important' for ISG. This means that autonomy plays an important role in ISG by enabling information security systems to make independent decisions in order to adapt and respond in a timely fashion to dynamic security changes in their information security environments.

Emergency direct reporting to the governance level is useful to embed within the organisational information security structure (Gokhale & Banks 2002). It represents one of the viable principles of VSM for ISG and is the means by which, when necessary, Information security policy system #5 is made aware of the current security situation in Security operations system #1. In this research, it was the sole principle in building the VSMISG used for the experiment (Chapter 4). It was introduced in section 3.2.3.2 and its importance rated in section 3.3.2. The average rating of the importance of emergency direct reporting was 'very important' for ISG. This indicates that it plays a very important role in ISG by making Security policy system #5 aware of threats with a

potentially severe impact on organisational viability, in order to respond to them immediately.

The recursion principle enables organisations to cope with complexity within their diverse information security environment by creating as many levels of controlling systems as required. It was introduced in section 3.2.3.3 and its importance rated in section 3.3.2. The average rating of the importance of recursion was 'important' for ISG. This means that recursion has an important role in ISG by enabling the information security systems to control the complexity involved in the security environment.

For a system to become or remain viable, a system or organisation must have variety in its environment. It must preserve a capacity to adapt to different states and dynamic changes within its operating environment (Brocklesby & Cummings 1996). The requisite variety principle was introduced in section 3.2.3.4 and its importance rated in section 3.3.2. The average rating of the importance of requisite variety was 'important' for ISG. This means that requisite variety has an important role in ISG by enhancing organisational viability through maintaining the necessary capacity for controlling uncertainties and changing states in the operating environment. The capabilities of the controlling system must absorb the uncertainties of the controlled system to maintain the balance of the whole system (Skyttner 2005).

Viability is one of the key principles of the VSM for ISG. A viable system is capable of maintaining a separate existence by surviving on its own (Beer 1979). The viability principle was introduced in section 3.2.3.5 and its importance rated in section 3.3.2. The average rating of the importance of viability was 'important' for ISG, thus it plays an important role in ISG by maintaining organisational viability. It does so by arranging and managing its information security structure, based on clear definitions of the roles and responsibilities of its information security systems.

7.1.3 Consensus among Information Security Experts

In previous sections, we discussed the ratings of eleven information security experts on the importance of VSM principles and systems to ISG. This section discusses the inter-rater agreement analysis among the experts, answering the following research question:

RQ3 To what extent do the information security experts agree on the importance of the viability system model's principles, systems, and principles and systems (combined)?

The agreement among the information security experts was analysed under the following three categories:

1- VSMISG systems
2- VSMISG principles
3- VSMISG systems and principles combined.

The agreement among the information security experts on rating the importance of the VSM systems to ISG was analysed in section 0. The results showed that there was a little agreement in rating the importance of the VSM systems for ISG. Similarly, the results showed that there was a little agreement in rating the importance of the VSM principles for ISG (section 3.3.4). The agreement among the information security experts on rating the importance of the VSM systems and principles combined for ISG was analysed in section 3.3.5. Likewise, the results showed that there was a little agreement among the experts.

7.2 Effects of VSMISG

The previous section discussed the results of expert ratings of the importance of VSM systems and principles to ISG. One of the viable principles is emergency direct reporting (Beer 1981), since this demands special care, involving as it does interaction with Information security policy system #5 (the head governance system). In addition, organisation viability relies on how quickly Security policy system #5 becomes aware of current security threats, in order to respond to them promptly. Therefore, reporting SSC from Security operations system #1 to Security policy system #5 lends this principle a higher level of importance than others.

Accordingly, this study focuses on investigating the effects of the VSMISG by examining the effect of emergency direct reporting on various sizes of organisation, threat intensities and time scales. Section 5.2 and Table 5-7 present the experiment design for this investigation. The experiment aimed to answer the following research questions:

RQ4 *Does the VSMISG have significant effects on the time taken to identify SSC?*

RQ5 *Are the effects of the VSMISG related to organisation size?*

RQ6 *Are the effects of the VSMISG related to the intensity of security threats?*

RQ7 *Are the effects of the VSMISG related to simulation time?*

The following sections discuss the results of investigating the effects of the VSMISG on the time to identify SSC with various sizes of organisation, threat intensities and simulation times.

7.2.1 Interaction between Organisation Size, Model, Simulation Time and Threat Intensity

The results of the experiment (section 5.4.1) show that there was a non-significant four-factor interaction effect between organisation size, threat intensity, simulation time and models on the time to identify SSC. Similarly, none of the three-factor interactions were significant. This means that interactions between the four or three factors do not make a significant difference to the time taken to identify SSC.

7.2.2 Interaction between Organisation Size and Models

The results revealed that there was a significant interaction between organisation size and models (Table 5-8). Significant differences in the time taken to identify SCC between the small, medium and large organisation in the baseline ISG model and VSMISG were reported (Table 5-10) and illustrated (Figure 5-6).

In the baseline ISG model, the time to identify SSC in the small organisation was usually longer than that in the medium-sized or large organisation, and the time taken to identify SSC in the large organisation was less than in the medium organisation. This means that in the large organisation Information security policy system #5 identified SSC faster than in the medium and small organisation, while in the medium-sized organisation it identified SSC faster than it did in the small one. Introducing emergency direct reporting into a small organisation is of greater benefit than in a medium-sized organisation, and introducing it into a medium-sized organisation is of greater benefit

than doing so in a large organisation (Figure 5-7 and Figure 5-8). Ryan (2009) concludes that the level of crisis preparedness is directly related to the size of the organisation; larger organisations are expected to exert more diligence in protecting organisational assets (Baker & Wallace 2007).

Similarly, under VSMISG in the large organisation, Security policy system #5 identified SSC faster than it did in either the medium-sized or small organisation. Moreover, in the medium-sized organisation, it identified SSCs faster than it did in the small.

The small organisation took the longest to identify SSCs, while the large organisation was the quickest under both the baseline ISG and VSMISG. This is due to the fact that there were fewer information security staff in the small than in the medium-sized and large organisation: just seven, compared to 14 and 28.

Under VSMISG, the time taken to identify SSC is shorter than that in the baseline ISG model (Figure 5-7). This is applicable to all organisation sizes, indicating that organisations that implement VSMISG identify SSC faster than those that implement the baseline ISG model, regardless of size. This is because they use emergency direct reporting, not routine reporting. Emergency direct reporting leads to effective security governance (Ross & Weill 2004; Brown & Nasuti 2005), while routine (hierarchical) reporting introduces delay, as it spans several layers (Bender 2010; Howes 2004).

7.2.3 Interaction between Organisation Size and Threat Intensity

The results revealed that there was a significant relationship between organisation size and threat intensity (Table 5-8).

In the case of a low intensity threat (Figure 5-9), the results reveal that the time taken to identify SSC in the small organisation was much greater than in the medium-sized organisation. This means that, in the medium-sized organisation, Information security policy system #5 identified SSC faster than in the small organisation when threat was low.

In addition, the time taken to identify SSCs in the small organisation was found to be longer than the time to do so in the large one. This is because most of the time the processing of SSC becomes delayed as staff are busy (Savarimuthu et al. 2004). The Information security policy system #5 in the large organisation identified SSC faster

than Security policy system #5 in the small organisation. Small organisations are generally human resource poor, therefore larger organisations with greater human resources are generally more successful in terms of information security (Yang et al. 2005; Chang & Ho 2006).

Despite the time taken to identify SSC in the large organisation being less than in the medium-sized organisation, the results show that the difference was not significant. This means that Information security policy system #5 in the large and medium organisation identified SSC in a similar time. The reason is that the extra number of information security staff in a large organisation does not make much difference when the level of threat intensity is low, that is, there is not a great volume of security threats that demands further information security staff to process them. Small organisations, with their fewer information security staff, are the slowest to identify SSC.

In the case of medium threat intensity, the results show that the time taken to identify SSC in large organisation was less than that in either the medium-sized or small organisation. This means that Security policy system #5 in the large organisation identified SSC faster than in the smaller organisations. Furthermore, the results show that the time taken in the medium-sized organisation was less than in the small organisation. This means that Security policy system #5 in the medium-sized organisation identified SSC faster than in the small organisation. The longest time taken to identify SSC was in the small organisation experiencing medium threat intensity.

Similarly in the case of high threat intensity, the large organisation identified SSC faster than medium-sized organisations, and those faster than the small organisation. As expected, the small organisation was found slow to identify SSC. The reason is that such firms experience a high volume of security threats and the existing information security staff require longer to process these. The longest time taken to identify SSC was found in a small organisation experiencing high threat intensity.

The results also show the differences in time taken to identify SSC when facing high, medium and low threat intensity in different organisation sizes (Figure 5-10). In the small organisation, the time to identify SSC by Information security policy system #5 experiencing high threat intensity was longer than that when experiencing medium threat intensity. Similarly, the time to identify SSC by Information security policy system #5 when facing medium threat intensity is longer than that when experiencing

only low threat intensity. The longest time taken to identify SSC was found in the small organisation under high threat intensity.

In the medium-sized organisation, the time taken to identify SSC under Information security policy system #5 when experiencing high threat intensity was longer than when experiencing medium and low threat intensity. On the other hand, experiencing low or medium threat intensity had no significant effect on the time taken to identify SSC, and speed is not affected if the threat intensity changed from low to medium in the medium-sized organisation. Current levels of information security staff in medium-sized organisations are capable of processing and identifying SSC with medium threat intensity at a similar rate as under low threat intensity; the information security staff in medium organisations can observe the threats of medium intensity just as fast as low.

For the large organisation, the results revealed no difference in the time taken to identify SSC by Information security policy system #5 when experiencing low, medium and high threat intensities. This means that changes in threat intensity had no effect on time taken to identify SSC in the large organisations; viability was not affected by threat intensity. The information security staff available in large organisations are capable of processing and identifying SSC promptly, regardless of changes in threat intensity.

Kankanhalli et al. (2003) and Hoffer and Straub (1989) conclude that large organisations invest more in information security than small organisations in terms of available human resources. The implication is that small organisations should be aware of the importance of having human resources available to process and report SSC directly to Information security policy system #5. In addition, executives should be aware of differences in organisation size and threat intensity in order to maintain organisational viability. For example, top management should pay close attention to the weakest link, which might very well be located in small organisations experiencing high threat intensity, in their viable ISG model. In addition, small organisations should realise that they are not favourably sited for viable ISG practice, and should work harder, for instance by allocating more human resources. Increasing staffing levels is recommended as one of the organisational and institutional responses not only for enhancing organisations viability, but also for responding to accidents in other domain such as safety management systems (Johnson et al. 2009).

7.3 Costs and Benefits of Changing from Baseline ISG Model to VSMISG

This section discusses the results of answering the following research question:

RQ8 Is using VSMISG more beneficial than using the baseline ISG model?

The study results showed that implementing VSMISG is more beneficial than the baseline ISG model (Table 6-14). This result is consistent with the conclusions made by (IT Governance Institute 2005; Lewis & Millar 2009). The viable system model for information security governance leads to continuous growth and keep costs at a minimum, thus organisations that change from using the baseline ISG model to VSMISG receive more benefits. They have the ability to identify SSC that prevent them from achieving their objectives faster than if they were using the baseline ISG model. The baseline ISG model takes longer to identify SSC that delay response, which can be expensive. Therefore, it is to be expected that it is difficult for organisations using the baseline ISG model to deal with SSC in a cost effective manner.

Executives should be aware of the difference between the baseline ISG model and VSMISG in terms of costs and benefits. For example, to implement a cost-effective ISG model, management should pay attention to the financial implications of using the baseline ISG model instead of VSMISG. Furthermore, organisations that use the baseline ISG model should realise that they need to work harder, for instance, by directly reporting SSC to the information security policy System #5 for immediate response.

Using VSMISG provides a number of benefits such as:

- Awareness, as SSC are directly reported to security governance level by a direct communication channel, as concluded by Beer (1984) and Gokhale & Banks (2002)
- Responsiveness, as there is a faster reporting method to identify SSC leading to a faster response, as concluded by Espejo (2003), Hutchinson and Warren (2002), Gokhale and Banks (2002), Davies (2002) and Lewis and Millar (2009)
- Viability, because fast reporting leading to a swift response to SSC results in enhancing the continuity of organisation operations, as suggested by Gmür et al. (2010), Hoverstadt & Bowling (2002) and Gokhale and Banks (2002)
- Cost-effectiveness, as VSMISG enhances continuous growth, keeping costs down, as concluded by IT Governance Institute (2005), and Lewis and Millar (2009).

7.4 Limitations

The first limitation is in the preliminary study conducted to review the appropriateness of adopting the viable system model for information security governance. There were eleven information security experts involved in this study, which may not be considered a large number. While using small samples can provide results quickly, they do not normally produce reliable assessment. If the aim is to establish reliable assessment on a risk factor, the study should be sufficiently large (Hackshaw 2008). Although the participants were few, all are highly experienced in the field of study; in addition, the main goal of this study is to assess the appropriateness of a well-established theory, not to establish a new one, which would requires a large number of participants.

Another limitation of this research is the use of simulation. There is no guarantee that the results achieved will actually be optimal. Simulation results are imprecise, as they are estimates with confidence intervals (Buchholz et al. 2006). Therefore, recommendations for real situations that are based on valid evidence cannot be provided. It is extremely difficult to conduct information security experiments with real life organisations; they are not willing to reveal data about their information security practices (Chandran 2004).

A third limitation of this study is the use of data based on a single case study and assumptions. Issues relating to generalisability and potential biases are a result of using

a single case study (Cavaye 2008; Leonard-Barton 1990). Although doing so does not lend itself to reliability in extending theory (Bansal & Roth 2000), here it helped to build a model with sufficient accuracy. It is difficult in the time available for this research to locate further studies that make available for researchers the data relating to specific information security activities and resources. Although it initially uses data from a single case study and assumptions, the data were later relaxed to accommodate all organisation sizes to achieve realistic results (section 5.1).

7.5 Summary

This chapter has discussed the research findings, starting by reviewing the appropriateness of VSMISG. This was conducted by an assessment of the importance of the principles and systems of the model to information security governance by eleven information security experts. The results identified the importance of the systems and principles of the viable system model to information security governance.

Furthermore, the agreement among the experts on rating the importance of the VSMISG was analysed. The results revealed that there was a little agreement among them in determining the relative importance of the principles, systems, and principles and systems (combined).

In addition, this chapter has discussed the investigation into the effects of VSMISG in different-sized organisations, threat intensities and simulation time. This revealed a non-significant four-factor and three-factor interaction effect between simulation time, threat intensity, organisation size and model on the time to identify SSC. Between organisation size and model it showed a statistically significant interaction effect.

Variations in model resulted in a statistical significant difference in the time taken to identify SSC. Using the VSMISG resulted in SSC being identified faster than under the baseline ISG model. Similarly, variations in organisation size resulted in statistically significant differences on the time taken to identify SSC. In both the baseline ISG and VSMISG, the large organisation identified SSC faster than the medium-sized organisation, and the medium-sized organisation identified SSC faster than the small organisation. The results showed no interaction between model and threat intensity, meaning that the effects of the VSMISG are not related to change in threat intensity.

Interestingly, the results showed an unexpected finding of a statistically significant interaction effect between organisation size and threat intensity in terms of time to identify SSC. The time taken under high threat intensity was greater than that to identify SSC under medium threat intensity. Similarly, the time to identify SSC under medium threat intensity is longer than that to identify SSC under low threat intensity.

The simulation time's main effect may be interpreted, because it was not involved in any significant interaction. The results showed that its main effect was not statistically significant.

This chapter has discussed the results of the cost–benefit analysis of changing from the baseline ISG model to VSMISG. The results revealed that organisations adopting VSMISG may expect to receive more benefit and show that cost reduction and benefit gain may be enjoyed from early in the first year of using VSMISG.

Finally, this chapter discussed the research limitations. These include the small number of participants reviewing the appropriateness of VSMISG, the use of simulation to conduct the research experiment, the use of data from a single case study and assumptions.

Chapter 8. Conclusion and Future Work

This chapter provides a conclusion to the work conducted in this research. It summarises the work undertaken to propose the VSMISG, review its appropriateness, investigate its effects and analyse it financially. Section 8.1 summarises the main points of the research. Section 8.2 revisits the research questions and provides a summary of the core findings, and, lastly, section 8.3 provides suggestions for further studies to be conducted in future.

8.1 Research Summary

Organisations need to implement VSMISG to ensure their viability, which is vital and serves as a powerful system in highly competitive security environments. Much research into information security governance has focused on security management structures, strategies, standards, risk management, roles and responsibilities, principles, resources and performance reporting (Corporate Governance Task Force 2004; Posthumus & von Solms 2004; Da Veiga & Eloff 2007; ITGI 2006; von Solms & von Solms 2006; Ohki, Yonosuke Harada, et al. 2009). An organisation can be viable if it is constructed on five main management systems: operations; coordination; control; planning (intelligence); and policy, and five principles: autonomy; emergency direct reporting; recursion; requisite variety; and viability (Beer 1984).

In this research, the VSM was redefined in the context of ISG, an expert review was conducted to identify the appropriateness of the VSM for ISG, and the inter-rater agreement was analysed to determine the level of consensus among the experts on the importance of the VSM components for ISG. As shown in sections 3.3.1 and 3.3.2, the results of the expert review showed that the average ratings of the VSM principles and systems for ISG are ‘important’ and ‘very important’. Our analysis (sections 0, 3.3.4, and 3.3.5) also found that there was a little agreement among the experts on rating the importance of the VSM principles, systems, and principles and systems (combined) for ISG. These results can be used to identify key viability principles and systems for ISG, and to help organisations to enhance their viability.

In addition, the baseline ISG model and VSMISG, which is based on the emergency direct reporting, were designed to model both the current ISG practice and

the viable ISG, and a simulation study was conducted to investigate the effects of the VSMISG on the time taken to identify SSC in different organisation sizes, threat intensities and simulation time. As presented in section 5.4.2, the results of the simulation study showed that there was a statistically significant interaction effect between models and organisation size in terms of the time taken to identify SSC. These can be used to demonstrate the effects of the baseline ISG model and VSMISG on the viability of small, medium and large organisations, and the effects of organisation size on viability in the baseline ISG model and VSMISG. Introducing emergency direct reporting in small, medium and large organisations reduces the time required to identify SSC; it is of great benefit to all sizes of organisation. These results help small, medium and large organisations to recognise the enhancing influence of VSMISG on their viability.

Furthermore, the results of the simulation study presented in section 5.4.3 showed that there was a statistically significant interaction effect between organisation size and threat intensity on the time taken to identify SSC. These results can be used to demonstrate the effects of different threat intensities in small, medium and large organisations. The results can be used to demonstrate the effects of the organisation size on the time taken to identify SSC when experiencing low, medium, and high threat intensities. Small organisations take the longest to identify SSC, especially when threat intensity becomes high. These results help executives to recognise the effects of different threat intensities on their viability. Consequently, appropriate planning based on viability can take place.

The results of the cost–benefit analysis of changing from the baseline ISG model to VSMISG (section 6.7) showed that the revenue outweighs the cost. Using VSMISG brings greater benefit than the baseline ISG model. These results can be used to help organisations to recognise the financial benefits of changing from the baseline ISG model to VSMISG, enabling them to make informed decisions for implementing a cost-effective ISG model.

The expected benefits from the results of this research are to help directors and decision makers to make informed decisions to implement a viability-based and cost-effective ISG model to ensure their organisation’s viability.

8.2 Research Findings

In this section, the findings of the research are summarised, are presented according to the following research questions:

RQ1 What are the components of ISG that enhance organisations' viability?

The viability components of the VSM were identified and redefined for ISG. These components include five viable systems and five principles. The viable security systems are: information security operations, co-ordination, control and compliance monitoring function, planning, and policy systems. The principles are autonomy, requisite variety, viability, emergency direct reporting, and recursion.

RQ2 What is the importance of the principles and systems of the viable system model to information security governance?

The results identified the importance of the systems and principles of the viable system model to information security governance. The principles and systems are 'important' and 'very important' to information security governance.

RQ3 To what extent do information security experts agree on the importance of the viability system model's principles, systems, and principles and systems (combined)?

The results revealed a little agreement among the experts on determining the importance of the principles, systems, and principles and systems (combined).

RQ4 Does the VSMISG have significant effects on the time taken to identify SSC?

Using the VSMISG results in faster identification of the SSC than the baseline ISG model. The faster identification of SSC enables a faster response and enhances the viability of organisations.

RQ5 Are the effects of the VSMISG related to organisation size?

Changes in the size of organisation result in changes in the effects of VSMISG. The identification of SSC in large organisations is faster than in medium-sized

organisations, and the identification of SSC in medium-sized organisation is faster than in small organisation. Therefore, the effects of VSMISG are related to organisation size.

RQ6 Are the effects of VSMISG related to the intensity of security threat?

The results showed no interaction between model and security threat intensity. The effects of VSMISG are not related to changes in security threat intensity.

RQ7 Are the effects of VSMISG related to simulation time?

There is no main effect of simulation time on the time taken to identify SSC, therefore the effects of VSMISG is not related to changes in simulation time.

RQ8 Is using VSMISG more beneficial than using the baseline ISG model?

The results revealed that using VSMISG can lead to greater benefit to organisations through enhancing their viability and decreasing the cost of damage to their reputation and violations of regulations. The results also show that benefits are secured from early in the first year of using VSMISG.

8.3 Future Work

This study may lead to a number of other research ideas, including investigating the effects of VSMISG in other scenarios to study its effectiveness.

8.3.1 Emergency Direct Reporting between PoC and Crisis Teams

This research investigated the effects of the VSMISG by studying the effects of emergency direct reporting between Information security operations system #1 and Information security policy system #5. Future research might investigate the effects of emergency direct reporting again, this time between the Point of Contact (PoC) team and the response to crisis team within Information security operations system #1. This is to investigate the impact of the emergency direct reporting at an earlier stage within Information security operations system #1. Since Information security operations system #1 actually encapsulates five viable systems according to the recursion principle discussed in section 3.2.3.3, it is worth investigating the impact of the emergency direct reporting between System #1 and System #5 within Information security operations

system #1. This investigation may include studying the effects of different organisation sizes, threat intensities and cost–benefit analysis.

8.3.2 Emergency Direct Reporting between System #1 and System #5, and between PoC and Crisis Teams

We may extend our study in future by investigating the effects of emergency direct reporting both between the Point of Contact (PoC) team and the response to crisis team within Information security operations system #1, and between Information security operations system #1 and Information security policy system #5. This is to study at the same time the dual effects of both emergency direct reporting within the information security operations system, and between it and Information security policy system #5. This investigation may include the effects of different organisation sizes, threat intensities and cost–benefit analysis.

8.3.3 Comparing the Effects of VSMISG in Different Scenarios

Future research may compare the results of investigating the effects of the VSMISG from the different scenarios identified above. The results of the scenario defined in section 8.3.1 may be compared to the results of this research and to the results of the scenario defined in section 8.3.2. Another comparison may be made between the results of the scenario defined in section 8.3.2 and the results of this research. These comparison studies may identify a viable system model for information security governance that leads to more resilient organisations.

8.3.4 Effectiveness of the VSMISG

Future research may be extended by defining the requirements for an effective emergency direct reporting channel. It may investigate the effectiveness of the emergency direct reporting channel between Information security operations system #1 and Policy system #5, and between the PoC team and the response to crisis team. This is to ensure effective reliable communication by reducing noise in the communication channel, such as non-critical crisis reporting to Policy system #5. The effects of such factors and the number and types of filters used for reliable communication may be studied.

8.4 Conclusion

In this thesis, study has focused on defining a viable system model for information security governance, investigating its effects on different-sized organisations at various threat intensities and simulation times, and analysing its costs and benefits. Beer's viable system model was redefined for information security governance and its appropriateness for information security governance was rated by experts in the field.

We considered the viable system model to be important to information security governance to enhance an organisation's viability. This research investigated the effects of the VSMISG, including other factors such as organisation size, intensity of threat and simulation time. In this context, we could say that the VSMISG enhances the viability of small, medium and large organisations, and viability is enhanced more as the size of organisation increases; changes to the intensity of threat and to organisation size affect the viability of organisations, while viability is enhanced more as threat intensity diminishes and the organisation grows in size. We analysed the costs and benefits of changing from the baseline ISG model to VSMISG and, in this regard, we can say that implementing the latter leads to greater benefit to organisations, and that these benefits can be secured from early in its first year.

Directors and decision makers can use the results of this research to see the value of the VSMISG, helping them to make informed decisions that enhance viability. This research can also be used as a foundation for further study into increasing the effectiveness of the VSMISG, leading to more resilient organisations.

Appendix A Ethical Approval

Appendix B Questionnaire for the VSMISG Review

Importance of the Viable System Model for Information Security Governance

The objective of this questionnaire is to assess the importance of the viable system model's principles and systems to information security governance.

The Viable System Model for Information Security Governance (VSMISG) includes five viable security systems and five principles, listed below:

The principles:

1. Viability
2. Recursion
3. Requisite variety
4. Autonomy
5. Emergency direct reporting.

The systems:

1. Security policy system
2. Security planning system
3. Security control system (with compliance monitoring function)
4. Security coordination system
5. Security operations system.

A short description of each of these principles and systems is provided. Please rate their importance by ticking ✓ in the box that matches your opinion most closely.

The "**security policy system**" sets the general security policy and defines the security identity of the organisation, establishing the basis for the development of security guidelines, and making final decisions regarding long-term security directions.					
	Not relevant	**Not important**	**Neutral**	**Important**	**Very important**
How do you rate the importance of the "security policy system"?					
The "**security planning system**" strategically assesses and manages the organisation security environments (e.g., risks, regulations, competition, environmental factors, partners, and technology changes) by formulating suitable strategic centralised security objectives and plan, that the other functional decentralised security objectives and plan should be consistent with.					
	Not relevant	**Not important**	**Neutral**	**Important**	**Very important**
How do you rate the importance of the "security planning system"?					
The "**security operations system**" deals with various information security environments such as vulnerabilities, best practices, policies, and standards to cope with dynamic security changes in these environments in order to protect the operations of the organisation.					
	Not relevant	**Not important**	**Neutral**	**Important**	**Very important**
How do you rate the importance of the "security operations system"?					
The "**security control system**" formulates the operations security policies that are based on the security strategic plan and provides the necessary resources to the parts of the security operations system to enable them to achieve their objectives that match the defined operations security policies.					
	Not relevant	**Not important**	**Neutral**	**Important**	**Very important**
How do you rate the importance of the "security control system"?					
The "**security coordination system**" coordinates the parts of the security operations system and resolves their conflicting operations security policies to ensure stabilisation and harmonisation in the information security operations system. It comprises the necessary resources for making autonomous decisions.					
	Not relevant	**Not important**	**Neutral**	**Important**	**Very important**
How do you rate the importance of the "security coordination system"?					
The "**security compliance monitoring function**" ensures that the activities of the information security operations system comply with defined security policies, and that the activities of the security coordination system ensures proper coordination between the parts.					
	Not relevant	**Not important**	**Neutral**	**Important**	**Very important**
How do you rate the importance of the "security compliance monitoring" function?					

The "**viability**" principle enables an organisation to arrange and manage its information security structure based on clear definitions of the roles and responsibilities of its information security systems, to be able to deal and control the dynamic changes in its security environments toward organisation viability.					
	Not relevant	**Not important**	**Neutral**	**Important**	**Very important**
How do you rate the importance of the "viability" principle?					
The "**recursion**" principle enables a security system to encapsulate itself in another security system in order to deal and cope with the embedded complexity in relevant security environments. That is, solving the complexity of a security system leads to solving the complexity of the whole.					
	Not relevant	**Not important**	**Neutral**	**Important**	**Very important**
How do you rate the importance of the "recursion" principle?					
The "**autonomy**" principle enables the information security systems to make their own independent decisions in order to deal and control the dynamic changes in their information security environments.					
	Not relevant	**Not important**	**Neutral**	**Important**	**Very important**
How do you rate the importance of the "autonomy" principle?					
The "**requisite variety**" principle enables the information security systems to have the required capabilities for controlling the changes in their information security environments and the changes of other information security systems they need to control.					
	Not relevant	**Not important**	**Neutral**	**Important**	**Very important**
How do you rate the importance of the "requisite varieties" principle?					
The "**emergency direct reporting**" principle enables the information security systems to communicate, escalate, and translate security events into an understandable format for making necessary decisions or taking required action. Critical warning signals may be routed directly to the information security policy system to act immediately.					
	Not relevant	**Not important**	**Neutral**	**Important**	**Very important**
How do you rate the importance of "emergency direct reporting" principle?					

References

Baker, W.H.B.W.H. & Wallace, L.W.L., 2007. Is Information Security Under Control?: Investigating Quality in Information Security Management. *IEEE Security & Privacy Magazine*, 5(1).

Bansal, P. & Roth, K., 2000. Why companies go green: A model of ecological responsiveness. *Academy of Management Journal*, 43(4), pp.717–736.

Beer, S., 1981. *Brain of the Firm* 2nd ed., Wiley, Chichester.

Beer, S., 1979. *The Heart of Enterprise (Classic Beer Series)*, Wiley.

Beer, S., 1984. The viable system model: its provenance, development, methodology and pathology. *Journal of the Operational Research Society*, 35(1), pp.7–25.

Bender, M., 2010. *A Manager's Guide to Project Management: Learn how to Apply Best Practices*.

Brocklesby, J. & Cummings, S., 1996. Designing a viable organization structure. *Long Range Planning*, 29(1), pp.49–57.

Brown, W. & Nasuti, F., 2005. Sarbanes–Oxley and Enterprise Security: It Governance and What it Takes to Get the Job Done. *Edpacs*, 33(2), pp.1–20.

Buchholz, P. et al., 2006. OPEDo : A Tool Framework for Modeling and Optimization of Stochastic Models.

Business Software Alliance, 2003. *Information security governance: Toward a Framework for Action*,

Cavaye, A., 2008. Case study research: a multifaceted research approach for IS. *Information systems journal*, (1996), pp.227–242. Available at: http://onlinelibrary.wiley.com/doi/10.1111/j.1365-2575.1996.tb00015.x/abstract.

Chandran, D., 2004. Customers Confidence in E-Business: An Evaluation of Australian Practices- A Case Study. , pp.1030–1034.

Chang, S.E. & Ho, C.B., 2006. Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3), pp.345–361.

Corporate Governance Task Force, 2004. Information security governance: a call to action. *National Cyber Security Summit Task Force*, 1(3).

Davies, J., 2002. Models of governance: A viable systems perspective. *Australasian Journal of Information Systems*, 9(2), pp.57–66.

Engel, A., 2010. *Verification, Validation, and Testing of Engineered Systems*,

Entrust, 2004. Information Security Governance (ISG): An Essential Element of Corporate Governance. , (April).

Espejo, R., 2003. The Viable System Model- A Briefing about Organisational Strucure. *Systems Practice*, p.221.

Espejo, R., 2004. Tribute to Stafford Beer.

Federal Financial Institutions Examination Council., 2004. FFIEC IT Examination HandBook InfoBase.

Gmür, B., Bartelt, A. & Kissling, R., 2010. Organization from a systemic perspective:

Application of the viable system model to the Swiss Youth Hostel Association. *Kybernetes*, 39(9/10), pp.1627–1644.

Gokhale, G.B. & Banks, D.A., 2002. Organisational Information Security : A Viable System Perspective, Information Security & Threats.

Gray, D, 2009. *Doing Research in the Real World*,

Hackshaw, A., 2008. Small studies: Strengths and limitations. *European Respiratory Journal*, 32(5), pp.1141–1143.

Henderson, H., 2003. *Encyclopedia of Computer Science and Technology*.

Hoffer, J.A. & Straub., D.W., 1989. The 9 To 5 Underground: Are You Policing Computer Crimes? *Sloan Management Review*, 30(4), p.35.

Hoverstadt, P. & Bowling, D., 2002. Royal Academy of Engineering Systems Engineering Workshop- Modelling Organisations using The Viable System Model. *System*.

Howes, N.R., 2004. *On Cyber Warfare Command and Control Systems*.

Hutchinson, B. & Warren, M., 2002. Information Warfare : Using the Viable System Model as a Framework to Attack Organisations. *Proceedings of the 17th International Conference of the System Dynamics Society and 5th Australian & New Zealand Systems Conference*, (May 2002), p.10.

IT Governance Institute, 2005. *Governance of the Extended Enterprise: Bridging Business and IT Strategies*.

ITGI, 2006. *Information security governance: guidance for boards of directors and executive management*, Isaca.

Johnson, C.W. et al., 2009. Recognition primed decision making and the organisational response to accidents: Überlingen and the challenges of safety improvement in European air traffic management. *Safety Science*, 47(6), pp.853–872.

Kankanhalli, A. et al., 2003. An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2), pp.139–154.

Kendall, M., 1948. Rank correlation methods.

Khan, M.E., 2012. A Comparative Study of White Box , Black Box and Grey Box Testing Techniques. *International Journal of Advanced Computer Science and Applications*, 3(6), pp.12–15.

Kotulic, A.G. & Clark, J.G., 2004. Why there aren't more information security research studies. *Information & Management*, 41(5), pp.597–607.

Leonard-Barton, D., 1990. A Dual Methodology for Case Studies: Synergistic Use of a Longitudinal Single Site with Replicated Multiple Sites. *Organization Science*, 1(3), pp.248–266.

Lewis, E. & Millar, G., 2009. The Viable Governance Model-A Theoretical Model for the Governance of IT. , pp.1–10.

Lewis, G., 1997. A cybernetic view of environmental management: The implications for business organizations. *Business Strategy and the Environment*, 6, pp.264–275.

Matell, M.S. & Jacoby, J., 1971. Is there an optimal number of alternatives for likert scale items?, *Educational and Psychological Measurement*, 31(3), pp.657–674.

Mears, L. & von Solms, R., 2004. *Corporate Information Security Governance: a Holistic Approach*.

Ohki, E., Harada, Y., et al., 2009. Information security governance framework. *Proceedings of the first ACM workshop on Information security governance - WISG '09*, p.1.

Ohki, E., Harada, Y. & Kawaguchi, S., 2009. Information security governance framework. *security governance*, pp.1–5.

Posthumus, S. & von Solms, R., 2004. A framework for the governance of information security. *Computers & Security*, 23(8), pp.638–646.

Raymond, L., 1990. Organizational Context and Information Systems Success: A Contingency Approach. *Journal of Management Information Systems*, 6(4), pp.5–20.

Richelson, J.T., 1995. The U.S. Intelligence Community. *Westview Press*, (third edition).

Ross, J.W. & Weill, P., 2004. How Top Performers Manage IT Decisions Rights for Superior Results. *IT Governance*, (Harvard Business School Press Boston, Massachusetts), pp.1–10.

Ryan, B., 2009. Crisis preparedness in government departments in Australia.

Saunders, M., Lewis, P. & Thornhill, A., 2009. *Research Methods for Business Students* Pearsoned Education, ed., Pearson Education.

Savarimuthu, B.T.R., Purvis, M. & Fleurke, M., 2004. Monitoring and Controlling of a Multi-agent Based Workflow System. , 32, pp.127–132.

Schwaninger, M., 2006. Theories of viability: a comparison. *Systems research and behavioral science*, 347, pp.337–347.

Siegel, S. & Castellan Jr, N.J., 1988. *Non parametric statistics for the behavioural sciences*,

Skyttner, L., 2005. General Systems Theory: problems, perspectives, practice.

von Solms, B., 2001. Corporate governance and information security. *Computers & Security*, 20(3), pp.215–218.

von Solms, B. & von Solms, R., 2005. From information security to…business security? *Computers & Security*, 24(4), pp.271–273.

von Solms, R. & von Solms, S.., 2006. Information security governance: A model based on the direct-control cycle. *Computers & Security*, 25(6), pp.408–412.

von Solms, 2006. Information Security – The Fourth Wave. *Computers & security*, 25(3), pp.165–168.

Ultsch, A. et al., 2005. Pareto Density Estimation: A Density Estimation for Knowledge Discovery. In *Innovations in Classification, Data Science, and Information Systems. Proceedings of the 27th Annual Conference of the Gesellschaft für Klassifikation e.V., Brandenburg University of Technology, Cottbus, March 12-14, 2003*. pp. 91–100.

Umpleby, S.A., 2006. The Viable System Model.

Da Veiga, A. & Eloff, J., 2007. An information security governance framework. *Information Systems Management*, 24(4), pp.361–372.

Vinnakota, T., 2011. Systems approach to Information Security Governance: An imperative need for sustainability of enterprises. *2011 Annual IEEE India Conference*, pp.1–8.

Weissberg, R. & Buker, S., 1990. Writing up research. *New Jersey: Pretice-Hall*.

Wood, C.C., 1990. How many information security staff people should you have? *Computers & Security*, 9(5), pp.395–402.

Wood, C.C., 2011. *Information Security and Data Privacy Staffing Survey 2011*,

Yang, S.-M., Yang, M.-H. & Wu, J.-T. Ben, 2005. The impacts of establishing enterprise information portals on e-business performance. *Industrial Management & Data Systems*, 105(3), pp.349–368.