A Viable System Model for Information Security Governance: Establishing a Baseline of the Current Information Security Operations System

Ezzat Alqurashi, Gary Wills, Lester Gilbert

A Viable System Model for Information Security Governance: Establishing a Baseline of the Current Information Security Operations System

Ezzat Alqurashi*, Gary Wills, Lester Gilbert

Electronics and Computer Science, University of Southampton, United Kingdom
{eha1r10, gbw, L.H.Gilbert}@soton.ac.uk

Abstract. The academic literature offers many different frameworks and models of Information Security Governance (ISG). Considerable advancements have been made in identifying the components and principles of ISG. However, the current research has not identified the viability principles and components of ISG that ensure business continuity. This paper proposes a systemic model of ISG using the principles and systems of cybernetics as embodied in Stafford Beer's Viable System Model (VSM). It also establishes a baseline of the current information security operations system by adopting and simulating the BS ISO/IEC 27035 and shows the results of the simulation. Adopting the proposed viable system model of information security governance helps organizations not only in ensuring the effectiveness of internal controls but also in ensuring business continuity.

Keywords: information security governance, viable system model, business continuity, BS ISO/IEC 27035.

1 Introduction

Information security has evolved in step with the increasing complexity of its diverse environments. During the last 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 organizations 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 organizations have proposed various ISG frameworks and models. The Corporate Governance Task Force (2004) has provided guidance in the development and implementation of an organizational ISG structure including recommendations for the responsibilities of members of or-

ganizations. 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 programs. 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 through a holistic perspective. Recently, Ohki et al. (2009) have identified functions and interfaces of ISG between stakeholders, auditors, executives, and managers.

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 organizations' complexity. The Viable System Model (VSM) provides a promising route for exploration to counter the increasing level of threats and to meet the need for rapid response at the organizational level (Gokhale, 2002). Although much work has been done to date, more studies need to be conducted to define the viability components of the ISG.

The purpose of this paper is to present a VSM of ISG (VSMISG) to address the current shortcomings. In more detail, in this paper we extend the state of the art in the following ways. 1) We provide viability principles to ISG: autonomy, feedback, recursion, requisite variety, and viability. 2) We suggest systems to ISG: information security operations, coordination, control and compliance monitoring, planning, and policy. 3) We introduce an ISG model based on the redefined principles and suggested systems. 4) We establish a baseline of the current information security operations system.

The rest of this paper is organized as follows. In section 2 we present a background on ISG frameworks and models. In section 3 we describe the VSM. Section 4 contains a description of our model, while in section 5 we describe the modeling and simulation process. In section 6 we define the research method, in section 7 we show the simulation results, and then we conclude in section 8.

2 Information Security Governance: Frameworks and Models

Before we proceed to proposing our VSMISG, we give a brief description of the current ISG frameworks and models.

2.1 ISG Framework by the CGTF

The Corporate Governance Task Force (CGTF) was formed in 2003 to develop a governance framework to drive implementation of effective information security programs. It defined a framework which covers the following areas:

- The roles and responsibilities of the board of directors/trustees

- The roles and responsibilities of the senior executives
- The roles and responsibilities of the executive team members
- The roles and responsibilities of senior managers
- Responsibilities of all employees and users
- Organizational unit security program
- Organizational unit reporting
- Information security program evaluation.

The framework provides recommendations on members' roles and responsibilities in all organizational levels. It specifies that every organizational unit should develop and evaluate its own security program and report its effectiveness to top management (Corporate Governance Task Force, 2004).

2.2 Governance and Management Strategy for Dealing with Business Information Risks

This framework is composed of two levels: ISG and Information Security Management (ISM). The ISG side, including the board of directors and executive management, directs the organization by formulating the strategy, mission, vision, and policy of information security. It controls the 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 impacts on information security such as business issues, IT infrastructure, standards, best practices and legal and regulatory matters (Posthumus & Von Solms, 2004).

2.3 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 program. It identified eight components for achieving effective ISG:

1. Organizational 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.

2.4 ISG Framework Based on Direct-Control Cycle

This is a model based on two principles required for governing information security. The first principle identifies three actions—direct, execute, and control—while the second principle identifies three management levels: strategic, tactical, and operational. The strategic level starts the direct process by defining the importance of protecting information assets in its vision. The tactical level should align to the strategic vision of information security by formulating appropriate information security policies, organization standards, and procedures that meet that vision. The operational level defines administrative guidelines and procedures.

The control process depends on the characteristic of "measurability": that is, any statement of information security policies or strategic directives should not be formulated unless it is measurable. The operational level collects measurement data electronically from log files of various resources, and 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 the compliance reports to relevant directives that need to reflect relevant risk situations (Von Solms & Von Solms, 2006).

2.5 ISG Framework Based on a Holistic Perspective

This framework is based on evaluation of four approaches in order to define a holistic perspective toward ISG. The framework is composed of the common components identified from these approaches. The identified components are arranged into six categorizations. The framework consists of three levels of management: strategic, managerial and operational, and technical. Every level consists of one or more of the six categorizations. It includes change management as it influences all the identified components in the framework that it needs to consider when implementing any of these components (da Veiga & Eloff, 2007).

2.6 ISG Framework based on Functions and Interfaces

This framework identifies five ISG functions: direct, monitor, evaluate, report, and oversee. It also identifies four interfaces between stakeholders, auditors, executives, and managers. Executives perform the first four functions and the auditors perform the overseeing. Executives direct the management of information security, monitor the information security management practice and security incidents, evaluate results against defined goals, and report security issues and activities to stakeholders. Auditors oversee executives' information security related activities (Ohki, Harada, Kawaguchi, Shiozaki, & Kagaya, 2009).

3 The Viable System Model (VSM)

Stafford Beer introduced the VSM as a blueprint for designing the communication and control aspects of viable systems. Beer described the VSM in his book *Brain of the Firm* (1972), and then developed it in the books *The Heart of Enterprise* (1979) and *Diagnosing the System for Organizations* (1985). The VSM is a model for organizational structure that is based on the structure of the human nervous system (Beer, 1981).

Beer claimed that an organization can be viable if it is constructed around five main management systems: operations, coordination, control, planning (intelligence), and policy. He labeled these systems from 1 to 5 respectively. Beer defined a function of the control system to monitor the performance of the operations system known as compliance monitoring. The systems are interconnected together by communication channels or information flows. In addition, Beer argued that an organization can be viable if it is based on 5 principles: autonomy, direct feedback, recursion, requisite variety, and viability. These are described in the next section.

4 The Viable System Model of Information Security Governance (VSMISG)

In this section we propose a Viable System Model for ISG (VSMISG) based on the Viable System Model. First, we present the principles followed by the systems of the VSMISG.

4.1 The Principles

The VSMISG is based on five principles: autonomy, feedback, recursion, requisite variety, and viability of the VSM. We define these principles in the following sections (Beer, 1981; Lewis, 1997; Schwaninger, 2006).

Autonomy

The adaptation to dynamic changes in diverse information security environments necessitates that organizations must be autonomous. This means that individuals need to possess the authority and the knowledge to be able to make necessary immediate actions. Autonomy does not mean separation but the freedom to act within a clear accountability. Autonomous information security operations deploy resources with minimal reference to senior managers, enabling the quick adaptation to dynamic changes in related environments. The large ellipse to the left in Fig. 1 represents the environment in which the organization is embedded. The operations system has its own environment within the organizational environment. In fact, every unit in the operations system has its own environment that it needs to deal with in the operations environment.

Direct Feedback

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 connect corporations or organizations with their diverse information security environments. For instance, when the information security operations system (S1) can not cope with the changes in its related environments, it will seek the intervention of the information security control system (S3) through the communication channels between them. If no proper response is received within a defined timeframe, then S1 will directly escalate the situation (direct feedback) to the information security policy system (S5) to immediately intervene through exceptionally designed communication channels known as algedonic channels which are indicated by red lines in Fig. 1. The system (S5) must eventually receive the urgent information and "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 essential elements behind the feedback principle.

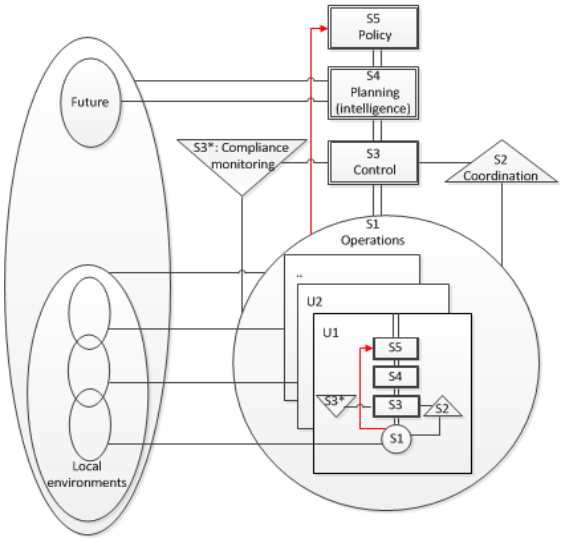

Fig. 1. The Viable System Model for Information Security Governance (VSMISG).

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 organization which is also a viable system. Furthermore, the organization is embedded within an industry which is also a viable system. The recursion principle is depicted in Fig. 1 by the viable systems inside the units (U1, U2, etc.) which are contained in the viable operations system. The recursion principle enables

organizations to cope with complexity within their diverse information security environments by creating as many levels of controlling systems as required.

Requisite Variety

In order for system S1 to cope with the dynamic changes in its environments, it must possess the necessary capabilities to control the changes in these environments. And in order for S3 to absorb the changes of S1, it must be able to contain its changes. Also, system S4 must possess the necessary capabilities to absorb the strategic changes in its environment depicted by the large ellipse in Fig. 1. The capabilities of the controlling system must absorb the uncertainties of the controlled system (Skyttner, 2005) to maintain the balance of the whole system.

Viability

A viable system is defined as one that is able to maintain a separate existence by surviving on its own (Beer, 1979). However, "survival" should not be understood as being able to merely 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 for arranging and managing the structure of organizational systems in a way that they merge with defined systems and interrelationships. The clear definitions of the systems, their internal sub-systems, and their intra- and interrelationships are essential to the continuity of business systems.

4.2 The Systems

The VSMISG consists of five systems and one function which are grouped into three groups as follows:

Information Security: Operations System (S1) and Coordination System (S2)

The information security operations system (S1) is where the organization's works to protect its information. The system continuously 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. The operations system (S1) must depend on other systems to keep decisions to a minimum. It must be autonomous to effectively respond and control its relevant environments. Being autonomous does not mean complete separation from the organizational system; rather, it is within an accountability framework. The information security coordination system (S2) coordinates the Units (U1, U2, etc.) of S1 to resolve possible conflicts and ensure stability and harmony. It dampens uncontrolled oscillations between the units of S1. The coordination system (S2) consists of the information security systems necessary for decentralized decision making (Skyttner, 2005) that the autonomy of S1 is based on.

Information Security: Control System (S3) and Compliance Monitoring Function (S3*)

The information security operations system (S1) includes one or more specialized units (Fig. 1) that deal with and control the dynamic changes in its information security environments. To do that, the specialized units require various resources. Sometimes these requirements conflict. The information security control system (S3) provides the required resources in a way that enables the units of S1 to accomplish their objectives. S3 is concerned with the "inside and now" world of corporations and organizations. It regulates the current information security activities and requirements of S1 for consistence with defined future requirements. S3 ensures through the compliance monitoring (S3*) function that current information security activities of S1 comply with defined information security policies and that current activities of S2 ensure a proper coordination between the units of S1.

Information Security: Planning (Intelligence) System (S4) and Policy System (S5)

The information security planning (intelligence) system (S4), which represents the ISG part in organizations, is responsible for the research and development of a strategic information security plan. Various information security environments such as risks, competition, clients, regulations, standards, and partners exist around the boundary of the organization system. S4 needs to interact with and adapt to the changes in these environments. It needs to direct the system toward achieving the goals of information security and to securely position the corporate system. S4 collects the necessary information about relevant strategic environments and analyzes them to formulate a suitable information security plan with defined requirements. The control system (S3) must implement this plan and maintain cohesion inside the corporate or organizational system. S4 is concerned with the "outside and future" world of the corporate system. It models and monitors the system and relevant strategic environments and makes predictions on future trends of information security environments.

The information security policy system (S5) sets the information security policy and defines the information security identity of the corporate or organizational system which is based on defined purposes. S5 establishes the basis for the development of information security guidelines, and makes final decisions regarding long-term information security directions.

5 Modeling and Simulation

This section introduces the information security operations system model that is adopted in this research for establishing the baseline. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) published an information security incident management model embodied in BS ISO/IEC 27035 (2011). The standard is intended to simulate information security incident management for large and medium-sized organizations. It provides guidance on managing information security incidents and vulnerabilities. The operational side

of the model, which is the focus of our study, is composed of three phases: detection and reporting, assessment and decision, and response. The activities of the model are grouped under these phases, described, and simulated below.

Detection and Reporting

1. Detection: events are detected by detection systems or by users.
2. Reporting: events are reported by reporting systems or by users.

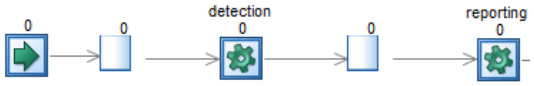

Fig. 2. Detection and reporting phase simulation.

In Fig. 2, Fig**. 3**, and Fig**. 4**, the squares with green arrows represent input entry points, the gray arrows represent routing, the white squares represent queues (storage), the squares with pinions represent activities, and the squares with check signs represent the end of work.

Assessment and Decision

1. Information collection by a Point of Contact (PoC): the (PoC) collects the required information related to a reported information security event.
2. PoC assessment: the PoC assesses the event to decide whether it is a false positive or a possible incident.
3. Information collection by Information Security Incident Response Team (ISIRT): the ISIRT collects the required information related to a possible incident received from the PoC. It also collects reports of information security incidents and alarms of abnormality or anomaly.
4. ISIRT assessment: the ISIRT assesses possible incidents, reports of incidents, and alarms to decide if they are false positives or confirmed incidents.

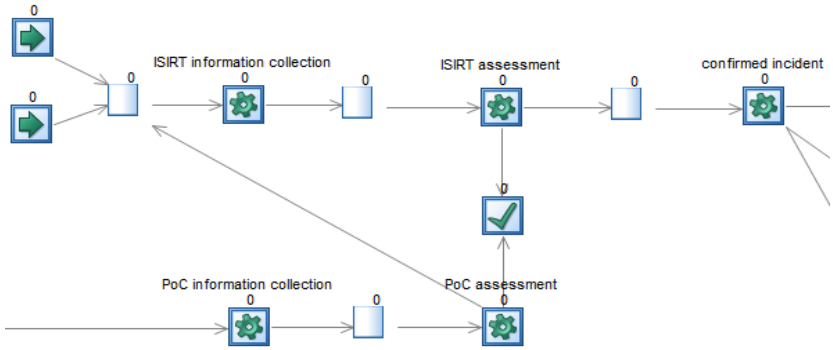

Fig. 3. Assessment and decision phase simulation.

Response

1. Immediate response: the ISIRT provides an immediate response to a confirmed incident which could include the activation of recovery procedures.
2. Incident categorization and severity classification: mapping an information security incident into relevant categorizations and determining the severity of the incident to the business.
3. Later response: other related effects to operations systems may need further responses to restore normal operations.
4. Digital evidence collection: The ISIRT collects digital evidence for information security forensic analysis to manage information security incident and for legal challenges.
5. Communication: the ISIRT communicates with stakeholders and the press to inform them about a confirmed incident.
6. Responses to crisis situation: activated when the ISIRT determines an information security incident is not under control and requires escalation to crisis situation.

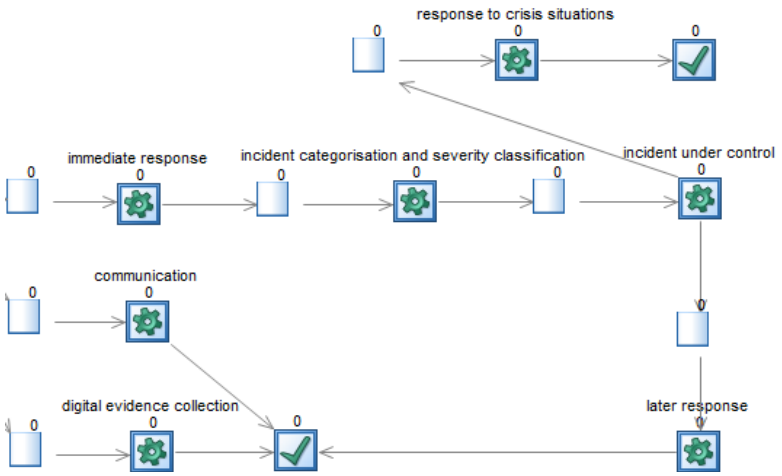

Fig. 4. Response phase simulation.

6 Research Method

A literature review was conducted to determine the information security components that ensure the viability of organizations. This has led to identifying the VSM which was adopted to be the theoretical background of the proposed model.

A baseline of the current information security operations system was established by adopting and simulating the current state of the operational side of the information security incident management model embodied in BS ISO/IEC 27035 (2011). The data used in the simulation came from two sources. The first source was from a case study undertaken by HP Laboratories (2012) and from an information security expert using a questionnaire. The simulation software package employed in this study is the

discrete event simulator SIMUL8, which allows the creation of a visual model of the system under study by directly drawing animated objects on the display.

All the entry inputs, queues, routing arrows, activities, and outputs of the model were visualized by using the objects of the SIMUL8. The number of exponential distributed inputs that were entered into the simulation (detected) is 1000 cases, including information security events, alarms, and reports at intervals of 19.2 (m), 68.55 (m), and 60 (m) respectively. The Poisson distribution was used for the queuing time of the model's activities. It is assumed that the Poisson distribution is the proper distribution used to describe random arrival rates over a period of time for models based on queuing theory (Black, 2009).

7 Results

The purpose of this section is to report the simulation parameters which constitute the baseline of the current information security operations system. The simulation parameters are shown in Table 1.

Table 1. The simulation parameters.

No.	Activity	Distribution type	Expected average queuing time (m)	Actual average queuing time (m)	Std. Dev.
1.	Reporting	Poisson	11	8	13
2.	PoC information collection		506	505	226
3.	PoC assessment		566	568	228
4.	ISIRT information collection		1282	1277	609
5.	ISIRT assessment		578	578	226
6.	Immediate response		1111	1120	476
7.	Communication		280	286	133
8.	Digital evidence collection		278	284	128
9.	Incident categorization and severity classification		294	300	120
10.	Later response		1502	1501	480
11.	Response to crisis situation		6643	6666	3717

Table 1 shows the activities of the simulation model, the statistical distribution of queuing time, the expected and actual average queuing time, and the standard deviation. The detection activity was not listed in the table since it defines the rate of inputs entered into the simulation; hence one of the input's entry points was used for this purpose. The response to crisis situation activity shows the longest queuing time. This is because it includes the time of reporting and remediating a crisis situation as defined by HP Laboratories (2012).

8 Conclusion

The adoption of the VSM from the cybernetics literature provides the principles and systems of viability to ISG. We conducted a simulation to establish a baseline of the current information security operations system as defined in BS ISO/IEC 27035 (2011). The results reported are comparable to those defined in the HP case study.

The current operations system is the only VSMISG component that the established baseline represents. Our future work will focus on demonstrating the importance of the direct feedback principle by simulating the information security policy system and connecting it to the current operations system through the direct feedback channels.

References

1. Beer, S. (1981). *Brain of the Firm* (2nd ed.). Wiley, Chichester.
2. Beer, S. (1984). The viable system model: its provenance, development, methodology and pathology. *Journal of the Operational Research Society*, *35*(1), 7–25. Retrieved from http://www.jstor.org/stable/2581927
3. Beer, Stafford. (1979). *The Heart of Enterprise (Classic Beer Series)* (p. 596). Wiley.
4. Black, K. (2009). *Business Statistics: Contemporary Decision Making* (p. 836). John Wiley & Sons. Retrieved from http://books.google.com/books?id=KQ25WExx5usC&pgis=1
5. BS ISO/IEC 27035. (2011). BSI Standards Publication Information technology — Security techniques — Information security incident management.
6. Corporate Governance Task Force. (2004). Information security governance: a call to action. *National Cyber Security Summit Task Force*, *1*(3).
7. da Veiga, A., & Eloff, J. (2007). An information security governance framework. *Information Systems Management*, *24*(4), 361–372.
8. Entrust. (2004). Information Security Governance (ISG): An Essential Element of Corporate Governance, (April).
9. Gokhale, G. B. (2002). Organisational Information Security: A Viable System Perspective. Information Security & Threats. *System*, *17799*.
10. HP Laboratories. (2012). *Security Analytics: Risk Analysis for an Organisation's Incident Management Process*. Retrieved from http://www.hpl.hp.com/techreports/2012/HPL-2012-206.html
11. ITGI. (2006). *Information security governance: guidance for boards of directors and executive management*. *Corporate Governance*. Isaca.
12. Lewis, G. (1997). A cybernetic view of environmental management: The implications for business organizations. *Business Strategy and the Environment*, *6*, 264–275.
13. Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T., & Kagaya, T. (2009). Information security governance framework. *Proceedings of the First ACM Workshop on Information Security Governance - WISG '09*, 1.

14. Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638–646.
15. Schwaninger, M. (2006). Theories of viability: a comparison. *Systems Research and Behavioral Science*, *347*, 337–347.
16. Skyttner, L. (2005). *General systems theory: problems, perspectives, practice.*
17. Vinnakota, T. (2011). Systems approach to Information Security Governance: An imperative need for sustainability of enterprises. *2011 Annual IEEE India Conference*, 1–8. doi:10.1109/INDCON.2011.6139620
18. Von Solms. (2006). Information Security – The Fourth Wave. *Computers & security*, *25*(3), 165–168.
19. Von Solms, R., & Von Solms, S. . (2006). Information security governance: A model based on the direct-control cycle. *Computers & Security*, *25*(6), 408–412.