Information Systems Management, 24:361–372, 2007
Copyright © Taylor & Francis Group, LLC
ISSN: 1058-0530 print/1934-8703 online
DOI: 10.1080/10580530701586136

Taylor & Francis
Taylor & Francis Group

An Information Security Governance Framework

A. Da Veiga
PhD Student,
University of Pretoria,
South Africa.

J. H. P. Eloff
Head of Department and
Professor of Computer Science,
Department of Computer
Science,
University of Pretoria,
South Africa.

ABSTRACT Information security culture develops in an organization due to certain actions taken by the organization. Management implements information security components, such as policies and technical security measures with which employees interact and that they include in their working procedures. Employees develop certain perceptions and exhibit behavior, such as the reporting of security incidents or sharing of passwords, which could either contribute or be a threat to the securing of information assets. To inculcate an acceptable level of information security culture, the organization must govern information security effectively by implementing all the required information security components. This article evaluates four approaches towards information security governance frameworks in order to arrive at a complete list of information security components. The information security components are used to compile a new comprehensive Information Security Governance framework. The proposed governance framework can be used by organizations to ensure they are governing information security from a holistic perspective, thereby minimising risk and cultivating an acceptable level of information security culture.

KEYWORDS information security governance framework, information security components, information security culture, information security behavior

INTRODUCTION

Information security encompasses technology, processes, and people. Technical measures such as passwords, biometrics, and firewalls alone are not sufficient in mitigating threats to information. A combination of measures is required to secure systems and protect information against harm. Processes such as user registration and de-registration and people aspects such as compliance, training and leading by example need to be considered when deploying information security. As the deployment of information security evolved, the focus has been shifting towards a people-orientated and governance-orientated approach.

The so-called first phase of information security was characterised by a very technical approach in securing the IT environment. As time went by, the "technical people" in organizations started to realize that management played a significant role in information security and that top management

Address correspondence to
A. Da Veiga,
PO Box 741, Glenvista,
Johannesburg, 20098, South Africa.
E-mail: adele.daveiga@kpmg.co.za

needed to become involved in it too (Von Solms, 2000). This led to a second phase, where information security was incorporated into organizational structures. These two phases, namely technical protection mechanisms and management involvement have since continued in parallel. Organizations came to realize that there were other elements of information security that had been disregarded in the past. They concluded that the human element, which poses the greatest information security threat to any organization, urgently needs to be addressed (Da Veiga, Martins, & Eloff, 2007; Von Solms, 2000, 1997) and more attention be given to the information security culture within organizations (Von Solms, 2000). This third phase of information security emphasizes that information security should be incorporated into the everyday practices performed as part of an employee's job to make it a way of life and so cultivate an effective information security culture throughout the organization. An information security culture is defined as the assumption about those perceptions and attitudes that are accepted and encouraged in order to incorporate information security characteristics as the way in which things are done in an organization (Martins & Eloff, 2002).

According to the Cobit Security Baseline (2004), executives are responsible for communicating the right information security culture and control framework and for exhibiting acceptable information security behavior. This relates to the fourth phase of information security, namely the development and role of information security governance (Von Solms, 2006). Information security governance can be described as the overall manner in which information security is deployed to mitigate risks.

One of the key drivers in the fourth phase is the prevention of risks such as fraud and social engineering. The Information Security Breaches Survey conducted by PriceWaterhouseCoopers (PWC, 2004) stated that the number of technology-related security incidents such as system failures or data corruptions organization experience is very high, but that "human error rather than flawed technology is the root cause of most security breaches" (PWC, 2004). According to PriceWaterhouseCoopers, the solution would be to create a security-aware culture. Management is starting to realize that human interaction with technical controls could lead to serious risk such as fraud or social engineering. Von Solms (2006), consequently emphasises that good information security governance is essential to address these risks.

The risks faced by the organization can only be addressed when a governance framework for information security is in place and equipped with specific controls that executives may use to direct employee behavior. Such a governance framework can enable organizations to make provisions for human behavior in their information security initiatives, in order to cultivate an acceptable level of information security culture. In other words, there is a need for an information security governance framework that considers the technical and procedural controls of the past, but that also takes human behavior into account. Such a framework can be utilized to cultivate the acceptable level of information security culture in order to minimize risks posed to information assets.

The purpose of this article is to evaluate four current approaches towards information security governance frameworks in order to construct a new comprehensive Information Security Governance framework. This new Information Security Governance framework considers technical, procedural and human behavioral components to provide an all-encompassing and single point of reference for governing information security. The four approaches that are evaluated in the following section are ISO 17799 (2005), PROTECT (Eloff & Eloff, 2005), the Capability Maturity Model (McCarthy & Campbell, 2001), and the Information Security Architecture (ISA) (Tudor, 2000). The third section provides a comprehensive list of information security components based on the components of the four mentioned approaches. The information security components are used to construct the Information Security Governance framework (see Figure 1). Finally, the Information Security Governance framework is proposed and discussed in the last section.

INFORMATION SECURITY GOVERNANCE FRAMEWORKS—EXISTING APPROACHES

Information security behavior could be explained by illustrating the security we implement in our

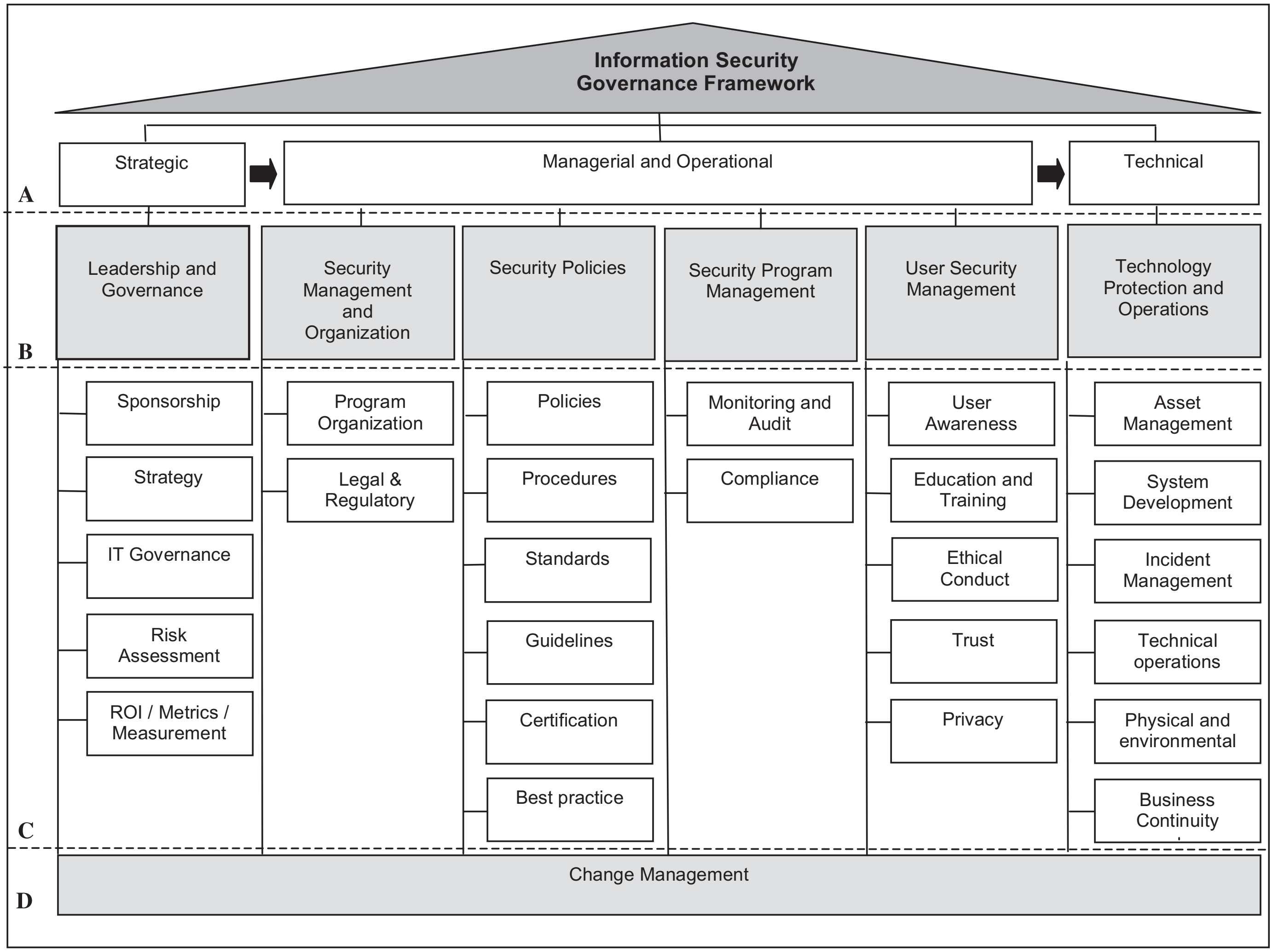

FIGURE 1 Information Security Governance framework.

houses. A homeowner could implement burglar proofing at each window, but upon leaving the house leave the front door unlocked. The security measures are therefore ineffective due to his behavior. In the same way, organizations implement security controls such as anti-virus programs, firewalls, and passwords. There is no sense in implementing these controls if users share passwords and connect through dialup to the Internet, bypassing the firewall.

The behavior of employees needs to be directed and monitored to ensure compliance with security requirements. As such, management needs to implement and communicate specific security controls—also referred to as components (Tudor, 2000; ISO 17799, 2005) —before they can expect employees to adhere to and exhibit an acceptable level of information security culture.

Various researchers and organizations have defined the components of information security and how an organization should go about implementing them (ISO 17799, 2005; Tudor, 2000; McCarthy & Campbell, 2001; Teufel, 2003). Information security components can be described as the principles that enable the implementation and maintenance of information security—such as an information security policy, risk assessments, technical controls, and information security awareness. These components can be encompassed in an information security governance framework where the relationship between the components is illustrated. The Information Security Governance framework provides organizations with an understanding of the requirements for a holistic plan for information security. It also combines technical, procedural, and people-orientated components for the purpose of cultivating an appropriate level of information security culture and minimising risks posed to information assets.

The subsequent sections provide a description of four current approaches to information security governance frameworks in order to define and construct a comprehensive new Information Security Governance framework (Figure 2).

ISO/IEC 177995 and ISO/IEC 27001

The Information Technology Security techniques—Code of Practice for Information Security Management (ISO/IEC 17799, 2005) of the Information Security Organization (ISO) take the form of guidance and recommendations and are intended to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used. ISO/IEC 17799 (2005) has gradually gained recognition as an essential standard for information security (ISO/IEC, 2005). It consists of the 11 control sections detailed in Table 1.

The certification standard ISO 27001 (2005) is regarded as part two of ISO/IEC 17799 (2005) and proposes an approach of continuous improvement through a process of establishing, implementing, operating, monitoring, reviewing, maintaining and improving the organization's information security management system (ISO, 2005; IEC, 2005). The previously mentioned international standards are considered as a single encompassing approach since ISO/IEC 17799 (2005) details the components of information security and ISO/IEC 27001 (2005) outlines the approach aimed at implementing and managing them.

TABLE 1 **Control Sections of ISO/IEC 17799 (Adapted from ISO/IEC 17799, 2005)**

1 **Security policy** that aims to provide management direction and support for information security, including laws and regulations.

2 **Organization of information security** that constitutes the process implemented to manage information security within the organization.

3 **Asset management** that focuses on asset inventories, information classification, and labeling.

4 **Human resources** security that considers permanent, contractor, and third-party user responsibilities to reduce the risk of theft, fraud, and misuse of facilities. This section also includes awareness, training, and education of employees.

5 **Physical and environmental** security controls that allow only authorized access to facilities and secure areas.

6 **Communications and operations management** that focus on the correct and secure operation of information-processing facilities, such as segregation of duties, change management, malicious code, and network security.

7 **Access controls** that manage user access to information and include clear desk principles, network access controls, operating system access controls, passwords, and teleworking.

8 Information **systems acquisition, development, and maintenance** that ensure the security of user-developed and off-the-shelf products.

9 Information security **incident management** that ensures that incidents are communicated in a timely manner and that corrective action is taken.

10 **Business continuity management** that focuses on business continuity plans and the testing thereof.

11 **Compliance** in terms of statutory, regulatory or contractual, laws, audit and organizational policy requirements, or obligations.

PROTECT

The research conducted by Eloff and Eloff (2005) introduced a comprehensive approach towards information security, namely PROTECT. This is an acronym for Policies, Risks, Objectives, Technology, Execute, Compliance, and Team. PROTECT is aimed at addressing all aspects of information security. It involves an approach that considers various and well-integrated controls in order to minimize risk and ensure effectiveness and efficiency in the organization. The seven control components of PROTECT are aimed at implementing and managing an effective information security program from a technology perspective as well as a people perspective and are summarised in Table 2.

Capability Maturity Model

The Capability Maturity Model (McCarthy & Campbell, 2001) approach provides a set of security controls used to protect information assets against unauthorised access, modification or destruction. The model is based on a holistic view of information security and encompasses seven main control levels as portrayed in Table 3.

TABLE 2 Control Components of PROTECT (Adapted from Eloff & Eloff, 2005)

1 The **policy** component includes information security policies, procedures, and standards, as well as guidelines for maintaining these.
2 **Risk** methodologies such as CRAMM and Octave, as well as automated tools to identify system vulnerabilities are covered in the risk component.
3 **Objective** refers to the main objective of PROTECT, namely to minimize risk exposure by maximizing security through the implementation and monitoring of a comprehensive set of controls.
4 **Technology** refers to hardware, software, and systems product components of the IT infrastructure and, where possible, the use of certified products.
5 Information security controls need to be established, maintained, and managed. **Execute,** therefore, refers to a proper information security management system environment.
6 The **compliance** component covers both internal compliance with the organization's policies and external compliance with information security expectations set by outside parties to the organization. Compliance also includes international codes of practice, legal requirements, and international standards.
7 **Team** refers to the human component, namely all the employees of the organization, where each has a responsibility towards securing information. The objective is to create a security-aware workforce that will contribute to an improved information security culture.

TABLE 3 Controls Levels of the Capability Maturity Model (Adapted from McCarthy & Campbell, 2001)

1 **Security leadership:** Security sponsorship/posture, security strategy, and return on investment/metrics.
2 **Security program**: Security program structure, security program resources, and skill sets.
3 **Security Policies**: Security policies, standards, and procedures.
4 **Security Management**: Security operations, security monitoring, and privacy.
5 **User Management**: User management and user awareness.
6 **Information Asset Security:** Application security, database/meta security, host security, internal and external network security, anti-virus, and system development.
7 **Technology Protection & Continuity**: Physical and environmental controls and continuity-planning controls.

The first level, security leadership, stresses the importance of an executive level security representative and an information security strategy. This should be the starting point for deploying both a long-term and short-term information security strategy within an organization. Next, a security program with defined roles and responsibilities for information security tasks should be developed and implemented. The roles of inter alia information security officer, network specialist, anti-virus specialist, database specialist, and Helpdesk personnel need to be defined. On the third level, security policies, standards, and guidelines need to be compiled to direct the implementation of information security. These policies, standards, and guidelines should cover the technical, procedural, and human aspects of information security. Security management will then form part of day-to-day operations, which include the monitoring of users and the technology deployed as directed by the previous layers. The organization subsequently needs to ensure that users are aware of policies and that user profiles are managed. Finally, the approach addresses information asset security that encompasses the technology aspects of information security, such as configuring a secure firewall, network and database. Technology protection comprises the last layer and focuses not only on the IT environment and its continuity, but also includes business continuity and disaster recovery.

The objective of the Capability Maturity Model approach is to start from the top on a strategic level and work down to the technology levels, guided by the direction provided by the strategic levels. In implementing information security, the model is used to assess the current information security capability and risks and to architect the appropriate solution to mitigate risks. The solution as well as monitoring capabilities are then implemented and integrated with current processes.

Information Security Architecture (ISA)

Tudor (2000) proposes a comprehensive and flexible Information Security Architecture (ISA) approach to protect an organization's assets against threats. This approach highlights five key principles, listed in Table 4, that are used to understand the risk environment in which organizations operate in order to evaluate and implement controls to mitigate such risks. There is also a focus on country regulations to ensure that each organization's confidential

TABLE 4 **Principles of the Information Security Architecture (Adapted from Tudor, 2000)**

1 **Security organization and infrastructure:** Roles and responsibilities are defined and executive sponsorship is established.
2 **Security policies, standards, and procedures**: Policies, standards and procedures are developed.
3 **Security program:** A security program is compiled taking risk management into account.
4 **Security culture awareness and training:** Users are trained and awareness is raised through various activities. Trust among users, management, and third parties are established.
5 **Monitoring compliance:** Internal and external monitoring of information security is conducted.

information is protected accordingly. The principles encompass aspects of process, as well as technology to address organizations' security needs.

The first principle relates to security organization and infrastructure with defined roles and responsibilities, as well as to executive sponsorship. The second principle requires that security policies, standards and procedures supported by management be developed and implemented. Security control requirements stated in the security policies cannot be deployed in isolation, but must be considered in terms of the risks the organization faces. Therefore, as a third principle, risk assessments must be performed across platforms, databases, applications, and networks, and a process should be instituted to provide an adequate budget for resources to address risks and implement controls. In order for the controls to operate effectively, users need to be made aware of their responsibility and encouraged to attend training programs. This fourth principle aims to establish an environment of trust among users, management and third parties to enable transactions and protect privacy. The fifth and last principle focuses on compliance testing and audits by internal and external auditors to monitor the effectiveness of the security program. The number of security incidents and Internet sites visited, as well as the levels of network and email usage constitutes aspects that must be monitored to allow a proactive approach towards addressing threats to information. In Tudor's latest research, aspects such as business continuity and disaster recovery are included as part of the approach aimed at preserving organizational information and assets (Holborn, 2005).

A COMPREHENSIVE LIST OF INFORMATION SECURITY COMPONENTS

A comprehensive list of components was compiled from the relevant sections of ISO 17799, components of PROTECT, levels of the Capability Maturity Model and principles of the ISA approach. These components were selected from each approach where a component was depicted as a key principle (e.g., "risk focus"), or as an information security control (e.g., "business continuity"). Where components overlapped between approaches such as "policies," a combined component category was defined.

A comprehensive list of components is presented in Table 5. The objective of Table 5 is to consolidate the components of the various approaches as discussed in the previous paragraph. It also shows the % representation of each approach's components. This comprehensive list of components forms the basis of the Information Security Governance framework, as discussed in the next section. Each component addressed by a specific approach is indicated on Table 5 by an inclusion tick ("•"). The sum of the ticks is divided by the total number of components to give the percentage of representation for each approach. This is depicted at the bottom of the table (ISO17799—68%, Eloff and Eloff—63%, McCarthy and Campbell—77%, and Tudor—59%).

Based on the assessment of the approaches, the components of ISO/IEC 17799 (2005) and the Capability Maturity Model of McCarthy and Campbell are the most comprehensive in addressing the breadth of information security components and therefore the percentage representation is higher compared to the approach of Eloff and Eloff and Tudor. Corporate governance, ethical conduct, and trust are not included in either of these two approaches, although all three components are considered by various researchers (Donaldson, 2005; Flowerday & Von Solms, 2006; Trompeter & Eloff, 2001) when governing information security in an organization.

The approach put forward by Eloff and Eloff (2005) suggests a holistic set of controls to consider and focuses mainly on providing a standardised approach for the management of an information security program. It is the only approach that mentions ethical values. Employees need to integrate

TABLE 5 **Information Security Governance Approach Components**

	Information security components	ISO 17799 (2005)	Eloff & Eloff	McCarthy & Campbell	Tudor
1	Corporate governance	X	X	X	X
2	Information security strategy	X	X	•	X
3	Leadership in terms of guidance and executive level representation	•	•	•	•
4	Security organization (internal organization such as management commitment, responsibilities, and coordination; external parties)	•	•	•	•
5	Security policies, standards, and guidelines	•	•	•	•
6	Measurement / Metric / Return on investment	X	•	•	X
7	Compliance and monitoring (legal, regulatory, and auditing)	•	•	•	•
8	User management (user, joiner, and leaver process)	•	X	•	X
9	User awareness, training, and education	•	•	•	•
10	Ethical values and conduct	X	•	X	X
11	Privacy	X	X	•	X
12	Trust	X	X	X	•
13	Certification against a standard	•	•	X	X
14	Best practice and baseline consideration	•	•	•	•
15	Asset management (responsibility and classification)	•	•	X	•
16	Physical and environmental controls (secure areas and equipment)	•	•	•	•
17	Technical operations (e.g., anti-virus, capacity, change management, and system development)	•	•	•	•
18	System acquisition, development, and maintenance	•	•	•	X
19	Incident management	•	X	•	X
20	Business continuity planning (BCP)	•	X	•	•
21	Disaster recovery planning (DRP)	X	X	•	•
22	Risk assessment process	•	•	•	•
Number of components derived from each approach		**15**	**14**	**17**	**13**
Percentage		**68%**	**63%**	**77%**	**59%**

ethical conduct or behavior relating to information security into their everyday life in the organization (Trompeter & Eloff, 2001). According to Baggett (2003), it is the responsibility of management and the board to develop and distribute corporate codes of conduct that should cover both commercial and social responsibilities. Ethical conduct, for example, not copying organizational software at home or using the Internet for private purposes during working hours, needs to be enforced as the accepted way of conduct in the work environment in order for the desired information security culture to emerge. Although the Eloff approach (Eloff & Eloff, 2005) is very comprehensive, it does not mention aspects such as business continuity or incident management. These could, however, be covered under the policy and procedures component.

Only Tudor (2000) mentions trust in his approach. According to Von Solms (2000), trust is arguably the most important issue in establishing information security in an IT environment. If management trusts its employees and the employees trust management, it is easier to implement new procedures and guide employees through changes of behaviour pertaining to information security. Corporate governance, ethical considerations and trust would all need to be incorporated into the approach adopted by an organization to provide a comprehensive set of information security components that can deal with its risks such as attempts at social engineering, fraud and staff misuse of information systems.

A NEW APPROACH TO AN INFORMATION SECURITY GOVERNANCE FRAMEWORK

In consolidating the four approaches towards information security governance discussed above, one assembles a comprehensive set of components to consider for information security governance. The proposed Information Security Governance framework (see Figure 2) can be used as a starting point by an organization to govern information security by developing guidelines and implementing controls to address risks identified by the organizations, such as misuse of web browsing, data corruption, or identify theft. This new framework can be utilized to govern employee behavior in all required facets of information security and cultivating an acceptable level of information security culture.

Ultimately, this governance framework provides management the means to implement an effective and comprehensive information security governance program that addresses technical, procedural, and human components. It integrates the components of the four discussed approaches, as well as components not considered, such as trust. Hence, the framework provides a single point of reference for the governance of information security to inculcate an acceptable level of information security culture. As each organization's environment is different and subject to different national and international legislation and regulations, additional components might be required, while others may not be relevant.

The information security governance framework, Figure 2, is partitioned into four levels, namely A, B, C, and D. Level A consists of strategic, managerial/implementation and technical protection components. The strategic components, shown on the left side of the figure, provide direction to the managerial and operational implementation components, depicted in the middle section of the figure. The technical protection components are shown on the right side of Figure 2.

Level B consists out of six main categories which are grouped according to the three Level A categories. The six main categories are:

- Strategic:
  - Leadership and governance.
- Managerial and Operational:
  - Security management and organization;
  - Security policies;
  - Security program management; and
  - User security management.
- Technical:
  - Technology protection and operations.

Level C consists of a comprehensive list of information security components categorised under each of the six main categories (level B). All six of the main categories are influenced by change depicted at the bottom of the figure (level D).

Implementing the information security components institutes change in the organization's processes and will influence the way people conduct their work. An important consideration is that organizations do not change, but people do, and therefore people change organizations (Verton, 2000). Information security changes in the organization need to be accepted and managed in such a way that employees are able to successfully incorporate such changes into their work. The component indicated as "Change" (Figure 2), needs to be considered when implementing any of the information security components. The six main categories (level B) of information security components and the composition thereof are discussed below.

Leadership and Governance

This category comprises executive level sponsorship for information security, as well as commitment from the board and management to protect information assets. This is due to the fact that information security governance is accepted as an integral part of good IT and Corporate Governance (Von Solms, 2005). Corporate governance refers to organization controls such as reporting structure, authority, ownership, oversight, and policy enforcement (Knapp, Marshall, Rainer, & Morrow, 2004). Corporate governance relates to the responsibility of the board to effectively direct and control an organization through sound leadership efforts (King Report, 2001; Donaldson, 2005). This is associated with IT governance, which is concerned about the policies and procedures that define how an organization will direct and control the use of its technology and protect its information (Posthumus & Von Solms, 2005).

Based on a study conducted by Gartner (Security, 2005), some of the top 10 business and technology priorities of Chief Information Officers (CIOs) in 2005 were to implement security enhancement tools, and to address security breaches and disruptions, as well as privacy issues. These actions would illustrate that management is realising that information security can add great value to the organization – which is the starting point for illustrating information security leadership.

The leadership and governance category also involves the compilation of an information security strategy that addresses information threats by conducting risk assessments aimed at identifying mitigation strategies and required controls. The information security strategy should be linked to the organizational and IT strategy to ensure that the organization's objectives are met both in the short and in the long term.

Finally, the category includes the concepts of metrics and measurement to measure how effective the organization is in addressing threats to information security. Many organizations are turning to metrics to evaluate the overall effectiveness of their information security programs (Witty & Hallawell, 2003) and whether it contributes in achieving the organization's strategy. The number of security incidents or even empirical results of awareness surveys can be used as metrics. Metrics will assist organizations in converting today's security threats into tomorrow's business opportunities (Ponemon, 2005).

Security Management and Organization

Program organization and legal and regulatory considerations are covered in this category. The objective of the category is to manage information security within the organization (ISO 17799, 2005). Program organization refers to the information security organizational design, composition and reporting structures (e.g., centralized or decentralized management of security). It also incorporates the roles and responsibilities, skills and experience, and resource levels committed to the enterprise security architecture (McCarthy & Campbell, 2001).

Different pieces of national and international legislation need to be considered for information security—for example, the Health Insurance Portability and Accountability Act (HIPAA) (Bresz, 2004); the Sarbanes-Oxley Act (Donaldson, 2005); the King Report II (2001); the Electronic Communications and Transactions Act (ECT) (2002); and the Promotion of Access to Information Act (PROATIA) (2000).

Security Policies

Security policies, procedures, standards, and guidelines are key to the implementation of information security in order to provide management with direction and support (ISO 17799, 2005) and they should clearly state what is expected of employees and guidelines for their behavior (Richards, 2002). ISO 17799 (2005) defines a policy as an "overall intention and direction as formally expressed by management." The security policies should consider the categories mentioned earlier (e.g., legal considerations) and must be implemented in the organization through effective processes and compliance monitoring. Examples of information security policies are an access control policy, e-mail, and Internet policy and a physical and environmental policy. A procedure such as a user registration and deregistration procedure explains or spells out statements of the security policy and is the steps that need to be taken to accomplish the policy (Von Solms & Von Solms, 2004). Procedures are underpinned by standards such as a password standard and guidelines for example how to configure a firewall to meet the requirements of the security policy.

Security Program Management

Monitoring and compliance as well as auditing are included in this category, which involves management of the security program. It is essential to measure and enforce compliance (Von Solms, 2005), and both technology and employee behavior (Vroom & Von Solms, 2004) should be monitored to ensure compliance with information security policies and to respond effectively and timely to incidents that are detected. Monitoring of employee behavior could include monitoring the installation of unauthorized software, the use of strong passwords or Internet sites visited. Technology monitoring could relate to capacity and network traffic monitoring. Information security auditing is necessary to ensure that the policies, processes, procedures and controls are in line with the objectives, goals and vision of the organization (Vroom & Von Solms, 2004).

User Security Management

This category addresses user awareness; education and training; ethical conduct; trust and privacy. ISO/IEC 17799 (2005) states that the organization must have plans and programs in place to implement, maintain, and effectively promote information security awareness and education throughout the organization.

According to the Guidelines for the Security of Information Systems and Networks of the Organization for Economic Cooperation and Development (OECD) (Baggett, 2003), one of the principles in creating a security culture is ethical conduct—where both management and the board develop and communicate corporate codes of conduct. Hellriegel, Slocum, and Woodman (1998) define ethics as the values and rules that distinguish right from wrong. It is management's responsibility to establish ethical standards of conduct that are in essence rules to be followed by employees and to be enforced by the organization (Cardinali, 1995). As part of the information security governance framework, ethical conduct must be addressed by the organization to minimize the risk of for instance invasion of privacy, selling of customer information and unauthorised altering of data. These rules should be communicated to employees as part of the security awareness programme.

N. Martins (2002) defines trust as "the process in which a trustor relies on a trustee (a person or group of people) to act according to specific expectations that are important to the trustor without taking advantage of the trustor's vulnerability." When implementing the Information Security Governance framework components, management must be able to trust employees to adhere to information security policies, while employees must be able to trust management to demonstrate commitment to information security (trust is seen as the primary attribute of leadership) (Robbins, Odendaal, & Roodt, 2001). A trusting relationship should also be established between trading partners and clients who could contribute to the organization's reputation. One possible way of establishing such a relationship could be for the organization to illustrate that information and assets are secured and that employees comply with requirements.

Privacy is an essential issue of trust when it comes to good relationships with customers, suppliers and other business partners (Tretic, 2001). If there is no privacy in business, there will be no trust (Ross, 2000). When implementing information security privacy, both employees and customers must be considered and controls must be implemented to protect their identity.

Technology Protection and Operations

The technology protection and operations category relates to the traditional focus of information security. It involves the technical and physical mechanisms implemented to secure an IT environment (Von Solms, 1997; Von Solms, 2000). When implementing the security governance framework, the technology controls applicable to the organization's environment and identified risks must be implemented. These include asset management, system development requirements, incident management, technical operations such as network security, and physical, environment, and business continuity controls. It is essential that the technology environment be monitored on a constant basis and that the risks of technology changes in the market be addressed—e.g., the use of personal digital assistants and teleworking technology.

CONCLUSION

The first step in developing an information security culture and empowering the workforce to be aware of their responsibilities towards protecting information assets would be to implement a comprehensive Information Security Governance framework—as is proposed in this article. It is evident that one approach alone is not sufficient in governing information security, but that an integrated approach should be adopted to ensure that all components pertaining to information security is considered. The new Information Security Governance framework can be deployed by organizations as a comprehensive and single point of reference towards governing information security. It considers a broad spectrum of components to assist in addressing risks to information assets on a technology, processes and people level. Management and executives can use the Information Security Governance framework as a reference for governing information security in all facets of the organization's information asset environment. The implementation of the applicable components of the Information Security Governance framework in an organization should have a positive impact on the behavior of employees and on how they protect the organization's assets, thereby minimising risks to information assets and cultivating an acceptable information security culture. The governance framework can be used in future research as a reference to develop an information security culture assessment tool to measure whether the level of information security culture is on an acceptable level, and to employ action plans for areas of development.

References

Baggett, W. O. (2003). Creating a culture of security. *The Internal Auditor*, *60* (3), 37–41.

Bresz, F.P. (2004). People—Often the weakest link in security, but one of the best places to start. *Journal of Health Care Compliance*, *6* (4), 57–60.

Cardinali, R. (1995). Reinforcing our moral vision: Examining the relationship between unethical behaviour and computer crime. *Work Study. 44* (8), 11–18.

COBIT security baseline—An information security survival kit. (2004). Rolling Meadows, USA: IT Governance Institute.

Da Veiga, A., Martins, N., & Eloff J. H. P. (2007). Information security culture—validation of an assessment instrument. *Southern African Business Review, 11* (1): 147–166.

Donaldson, W. H. (2005). U.S. capital markets in the post-Sarbanes-Oxley world: Why our markets should matter to foreign issuers. *U.S. Securities and Exchange Commission.* London School of Economics and Political Science.

Electronic Communications and Transactions Act. (2002). Retrieved 12 January 2006 from site: http://www.acts.co.za/ect_act/

Eloff, J. H. P. & Eloff, M. (2005). Integrated Information Security Architecture, *Computer Fraud and Security*, *2005* (11), 10–16.

Flowerday, S., & Von Solms, R. (2006). Trust an element of information security. In *Security and Privacy in Dynamic Environments*. IFIP/SEC2005; Boston: Kluwer Academic Publishers, 87–97.

Hellriegel, D., Slocum, J. W. (Jr), & Woodman, R. W. (1998). *Organizational Behavior.* (8th ed.). Cincinnati, OH: South-Western College Publishing. Holborn Books. Information Security architecture: An integrated approach to security in the organization (2005). Retrieved 18 April 2005 from: http://www.holbornbooks.co.uk/details.aspx?sn=1244811

ISO/IEC 17799 (BS 7799-1) (2005). Information technology. Security techniques. Code of practice for information security management, Britain.

ISO/IEC 27001 (BS 7799-2) (2005). Information technology. Security techniques. Information security management systems—requirements, Britain.

King Report. (2001). The King Report of corporate governance for South Africa. Retrieved 12 January 2006: http://www.iodsa.co.za/downloads/King%20II%20Report%20CDRom%20Brochure.pdf

Knapp, J. K., Marshall, T. E., Rainer, R. K., & Morrow, D. W. (2004). Top ranked information security issues: *The 2004 International Information Systems Security Certification Consortium (SIC) survey results*. Auburn, Alabama: College of Business Auburn University.

McCarthy, M. P. & Campbell, S. (2001). *Security Transformation*. McGraw-Hill: New York.

Martins, A. (2002). *Information Security Culture*. Master's dissertation, Rand Afrikaans University, Johannesburg, South Africa.

Martins, A. & Eloff, J. H. P. (2002). Information Security Culture. In *Security in the information society. IFIP/SEC2002*. (pp. 203–214). Boston: Kluwer Academic Publishers.

Martins, N. (2002). A model for managing trust. *International Journal of Manpower. 23* (8), 754–769.

The Concise Oxford Dictionary. (1983). Sykes, J.B. (Ed.) Oxford: Clarendon Press.

Posthumus, S. & Von Solms, R. (2005). IT Governance. *Computer Fraud and Security. 2005* (6), 11–17.

PriceWaterhouseCoopers. Information Security Breaches Survey. (2004). Retrieved 12 March 2005 from http://www.dti.gov.uk/industry_files/pdf/isbs_2004v3.pdf

Promotion of Access to Information Act. (2000). Retrieved 12 January 2006 from http://www.acts.co.za/prom_of_access_to_info/index.htm

Richards, N. (2002). The critical importance of information security to financial institutions. *Business Credit*, *104* (9), 35–36.

Robbins, S. (2001). *Organizational Behaviour*. (9th ed.). New Jersey: Prentice Hall.

Ross, B. (2000). New directives beef up trust in e-commerce. *Computer Weekly News*.

Security. 2005. Security, innovation head CIO's 2005 agenda. *Computer Fraud and Security*, *2005* (1), 1–2.

Teufel, S. (2003). Information Security Management—State of the art and future trends. In *Proceedings of the Annual International Information Security South Africa (ISSA) conference*. Johannesburg, SA, UNISA Press.

Tretic, B. (2001 January). Can you keep a secret? *Intelligent Enterprise*. *4* (1).

Trompeter, C. M. & Eloff, J. H. P. (2001). A framework for the implementation of Socio-ethical controls in Information Security. *Computers and Security*, *20* (5), 384–391.

Tudor, J. K. (2000). *Information Security Architecture—An integrated approach to security in an organization*. Boca Raton, FL: Auerbach.

Verton, D. (2000). Companies aim to build security awareness. *Computerworld*, *34* (48), 24.

Von Solms, R. (1997). Driving safely on the information superhighway. *Information Management & Computer Security*, *5* (1), 20–22.

Von Solms, B. (2000). Information security—The third wave? *Computers and Security*, 19(7). November, 615-620.

Von Solms, S. H. (2005). Information Security Governance—Compliance management vs. operational Management. *Computers and Security*, *24* (6), 443–447.

Von Solms, S. H. (2006). Information Security—The fourth wave. *Computers and Security. 25* (2006), 165–168.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers and Security*, *23* (33), 191–198.

Witty, R. J. & Hallawell, A. (2003). Client issues for security policies and architecture. *Gartner.* ID number: K-20-7780.

BIOGRAPHIES

Adele da Veiga is currently completing her PhD (IT) focusing on information security culture at the University of Pretoria, South Africa. She is a management consultant focusing on information security, risk management, and auditing.

JHP Eloff received a PhD (Computer Science) from the Rand Afrikaans University, South Africa. He gained practical experience by working as management consultant specializing in the field of information security. He is the Head of Department and full professor in Computer Science at the Department of Computer Science, University of Pretoria. He has published extensively in a wide spectrum of accredited international subject journals. He is evaluated as a B2 researcher from The National Research Foundation (NRF), South Africa. He is a member of the Council for Natural Scientists of South Africa.