THE ROLE OF THE COMPANY SECRETARY IN INFORMATION SECURITY MANAGEMENT

KARIUKI MUIGUA*

In this article the writer gives a brief overview of Information Security and Information Security Management within the context of an organization. Information Security is becoming a key concern in the management of organizations where the Company Secretary may be expected to play a key role in formulation of policy regarding Information Security Management and its implementation. It would therefore be useful to know a bit more about Information Security Management and Information Security Standardization through ISO 27001:2005.

The Company Secretary needs to be in an informed position so as to be able to advise the company of the need to address Information Security issues and set up an acceptable and effective Information Security Management system.

Information is an asset that has great value to an organization within which a Company Secretary works. An information Asset is a definable piece of information, stored in any manner which is recognized as 'valuable' to the organization. Information Security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. It has the goal of protecting the confidentiality, integrity and availability of information.

Information Security also aims at protecting data in various modes such as print, electronic and other forms of data. Companies and organizations

* CPS (K); MCIArb; LL.B (Hons), LL.M (Hons) Nrb; MKIM; Dip. In Law (KSL); Consultant: Lead expert EIA/EA NEMA; BSI ISO/IEC 27001:2005 ISMS Lead Auditor/ Implementer;

gather a lot of confidential information about their products, projects, customers, employees, research, and financial standing. Should such information fall into the wrong hands, it could lead to loss of business, loss of credibility and litigation.

Protecting confidential information is a business requirement and can also be viewed as an ethical and legal obligation placed on all the employees of a company, including the management and the Company Secretary. The Company Secretary should play a role in ensuring proper Information Security Management within the organization.

The Company Secretary is often involved in the planning, implementation, testing and improvement of Information Security systems. They should be developed so as to ensure confidentiality of information, availability of the same and integrity thereof.

Confidentiality means the information in question should not be disclosed to unauthorized persons. Integrity means that data cannot be modified without authorization. Availability means the information must be available when it is needed.

One school of thought advances an alternative model known as the six atomic elements of information: The elements are confidentiality, possession, integrity, authenticity, availability and utility[1].

Authenticity of information is necessary so as to ensure that the data communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.

The information should be such that it cannot be repudiated. Non repudiation implies one's intention to fulfill their obligations to a contract.

[1] Don Parker, 2002

It also implies that one party to a transaction cannot deny the authenticity of the transaction. Electronic commerce for instance uses technology such as digital signatures and encryption to establish authenticity and non repudiation.

Information Security and Risk Management aims at recognizing the value of information and defining appropriate procedures and protection requirements for the information.

Information is normally assigned a security classification. A classification policy defines the different classification labels and lists the required security controls for each classification.

BSI, ISO/IEC 27001: 2005 Information Security Management Systems – (ISMS) Standard

This is standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its full name is ISO/IEC 27001/2005 Information Technology Security Techniques- Information Security Management systems- Requirements but is commonly known as "ISO 27001"

ISO/IEC 27001 formally specifies a management system that is intended to bring Information Security under explicit management control. Being a formal specification means that it mandates specific requirements.

Organizations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified compliant with the standard.

This is a move away from the use of disjointed and disorganized adhoc controls which often address certain aspects of IT and data security leaving non IT information assets (such as paperwork and proprietary knowledge) less well protected on the whole.

ISO/IEC 27001 requires the management to firstly systematically examine the organizations Information Security risks, taking into account, the threats, vulnerabilities and impacts; secondly it also requires the design and implementation of a coherent and comprehensive set of Information Security controls and/or other forms of risk management (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable;[2] Thirdly the management is required to adopt a process that ensures that the Information Security controls continue to meet the organisation's Information Security needs on an ongoing basis. In other words there should be continuous improvement of Information Security Management for the sake of smooth business continuity.[3]

Annex A to ISO/IEC 27001 succinctly lists the Information Security controls from the code of practice (ISO/IEC 27002)

The code of practice provides additional information and implementation advice on the controls.

An ISO/IEC 27001 compliance certificate provides assurance that the management system for Information Security is in place. The organization is presumed to have adopted all necessary Information Security controls through an Information Security Management System (ISMS) which is in place.

The management determines the scope of the ISMS for certification purposes and may limit it to a single business unit or location.

An ISMS may be certified compliant with a ISO/IEC 27001 by a number of accredited Registrars. These are sometimes known as "Certification bodies" "Registration bodies" or "Registrars".

[2] ISO 27001:2005 clause 4
[3] Ibid clause 8

The Kenya Bureau of Standards for instance is a certification body among other roles that it plays.

The ISO/IEC 27001 like other ISO management certifications usually involves a three stage audit process. Stage one, is a preliminary informal review of the ISMS. The auditors check the existence and completeness of key documentation such as the organizations Information Security policy, Statement of Applicability (SOA) and Risk Treatment Plan (RTP).

Stage Two is a more detailed and formal compliance audit independently testing the ISMS against the requirements specified in ISO/IEC 27001. The auditors seek evidence to confirm that the management system had been properly designed and implemented and is in fact in operation.

Certification audits are usually carried out by ISO 27001 Lead Auditors. Passing this stage results in the ISMS being certified compliant with the ISO/IEC 27001.

Stage Three involves follow up reviews or audits to confirm that the organization remains in compliance with the standard. Certification maintenance requires periodic re-assessment audits to confirm that the ISMS continues to operate as specified and intended. These should happen at least annually but (by agreement with management) are often conducted more frequently particularly which the ISMS is still maturing.

The International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining an Information Security System (ISMS).[4]

The adoption of an ISMS should be a strategic decision for an organization. The design and implementation of an organization ISMS is influenced by

[4] ISO 27001:2005 clause 0.1, introduction

their needs and objectives, security requirements, the processes employed and the size and structure of an organization.[5]

These and their supporting systems are expected to change over time. It is expected that an ISMS implementation will be scaled in accordance with the needs of the organization e.g. a simple situation requires simple ISMS solutions.[6]

The International Standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing and improving an organization's ISMS.[7]

The application of a system of processes within an organization together with the identification and interaction of these processes, and their management can be referred to as the process approach.[8]

The process approach for Information Security Management presented in the International Standard encourages users to emphasize the importance of understanding an organization's Information Security requirements and the need to establish policy and objectives for each Information Security; implementing and operating controls to manage the organizations Information Security risks in the context of the organisation's overall business risks; monitoring and reviewing the performance and effectiveness of the ISMS and continual improvement and objective measurement.[9]

The International Standard adopts the "Plan-Do-Check-Act" (PDCA) model which is applied to structure all ISMS processes.[10]

The requirements set out in the International Standard are generic and are intended to be applicable to all organizations regardless of the type, size and

[5] Ibid
[6] Ibid
[7] Ibid clause 0.2
[8] Ibid
[9] Ibid clause 0.2(a) (b)(c) d introduction
[10] Ibid

nature. Excluding any of the requirements specified in clauses 4,5,6,7 & 8 is not acceptable when an organization claims conformity to the International Standard.[11]

If an organization already has an operative business process management system (e.g. in relation with ISO 9001 or ISO 14001) it is preferable in most cases to satisfy the requirements of ISO/IEC 2701:2005 within the existing Management System.[12]

The Information Security Management System (ISMS) is that part of the overall Management System, based on a business risk approach, to establish implement operate, monitor, review, maintain and improve Information Security.[13]

Clause 4.1 requires the organization to establish, implement, operate, monitor review, maintain and improve a documented ISMS within the context of the organisation's overall business activities and the risks it faces.

The organization is required to define the scope and boundaries of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology and including any justifications for exclusion from the scope. [14] An organization is also supposed to define an ISMS policy in terms of the characteristics of the business, the organization, its assets and technology[15].

The ISMS should take into account business legal and regulatory requirements and contractual security obligations.[16]

[11] ISO IEC 27001:2005 clause 1.2
[12] Ibid
[13] Ibid clause 3.7
[14] Ibid clause 4.2 .1 (a)
[15] Ibid clause 4.2.1(b)
[16] Ibid clause 4.2.1 (b) (3) ; Annex A 15

This is one area where the Company Secretary has a role to play. Information provided by the Company Secretary relating to legal and regulatory requirements and contractual obligations will to a large extent inform the contents of the ISMS.

Documentation requirements under clause 4.3 include records of management decisions so as to ensure that actions are traceable to management decisions and are reproducible. Keeping clear records by the Company Secretary is thus vital to the success of an ISMS.

The standard requires management commitment to its implementation.[17] It should among other things provide the resources with which to establish, operate monitor, review, maintain and improve the ISMS[18]. It should also provide training awareness and competence[19].

Internal audits at planned intervals are carried out to determine whether the controls objectives, controls processes and procedures of the ISMS conform to the requirements of the International Standard and relevant legislation or regulations[20], conform to the identified Security Information Security requirements[21] and are effectively implemented and maintained [22] and perform as expected[23]

Clause 7 provides for Management Review of the organization ISMS at planned intervals (at least once a year) to ensure its continuity sustainability adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for the change to the

[17] Clause 5.1 Annex A.6.1.1
[18] Ibid clause 5.1 e;5.2.1
[19] Ibid clause 5.2.2
[20] Ibid clause 6 (a)
[21] Ibid clause 6 (b)
[22] Ibid clause 6(c)
[23] Ibid clause 6 (d)

ISMS including the Information Security Policy and Information Security Objectives[24].

A Company Secretary would ordinarily be expected to attend such a review. It is thus vital that the said Company Secretary has a working knowledge of Information Security Management and the ISO 27001:2005 ISMS Standard.

Clause 8.1 require organizations to continually improve the effectiveness of ISMS through the use of the Information Security Policy, Information Security Objectives, audit results, analysis of monitored events, corrective and preventative actions and management review. Corrective action should be taken to eliminate the cause of non conformation with the ISMS requirements in order to prevent recurrence[25] .

Annex A deals with the control objectives and controls and covers internal organization of an organisation[26]; external parties [27] asset management[28], Human resource Security[29]; Physical and environmental security[30]; communications and operations management[31]; access control[32]; Information Systems acquisition development and maintenance[33]; Information Security incident management [34] business continuity management.[35]

[24] Ibid clause 7.1
[25] Ibid clause 8.2

[26] Annex A 6

[27] Ibid Annex A 6.2

[28] Ibid Annex A7

[29] Ibid Annex A8

[30] Ibid Annex A9

[31] Ibid Annex A10

[32] Ibid Annex A11

[33] Ibid Annex A12

[34] Ibid Annex A13

[35] Ibid Annex 14

Annex A 15 deals with compliance with legal requirements with the objective of avoiding breaches of any law, statutory, regulatory or contractual obligations or of any security requirements.[36]

The Company Secretary may have a role to play here; all relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented and kept up to date for each Information System and the organisation[37].

Intellectual property rights are to be respected: Appropriate procedures shall be implemented to ensure compliance with legislative regulatory and contractual requirements of the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products[38].

The Company Secretary should take note that there is correspondence between ISO 9001:2000, ISO 14001:2004 AND ISO 27001:2005. They are compatible and can exist within one Management System.

While the ISO 27001:2005 deals with the Information Security Management System the ISO 9001:2000 lays out a Quality Management System. The process approach is used both in ISO 27001:2005 and ISO 9001: 2000. The three systems provide the general requirements and require implementation monitoring and review of either th4e System or the process[39].

[36] Ibid 15.1

[37] Ibid Annex 15.1.1

[38] Ibid 15.1.2

[39] ISO 27001:2005 clause 4;clause 4.2.3(monitor and review the ISMS); ISO 9001:2000 clause 8.2.3, 8.2.4 (monitoring and measurement of processes and product)

The three standards require management responsibility and commitment to providing resources competence and awareness. They require continuous improvement, corrective and preventive actions.[40]

Information Security Management should exist within a framework that ensures that security strategies are aligned with organizational objectives and consistent with applicable laws and regulations. The Company Secretary is indeed a compliance officer in this regard.

It is imperative that the Company Secretary be conversant with matters concerning Information Security. The Company Secretary should be concerned to see that information that is valuable to the organization is handled is such a way that ensures its confidentiality (where appropriate), its integrity and availability.

Today a Company Secretary is invariably a senior person, concerned with policy formulation, and ensuring that the organization complies with relevant standards, laws and regulations. High Information Security standards are ideals that every organization should aspire for.

The Company Secretary can assist in the planning, setting up, testing and improvement of an effective Information Security System for the sake of business continuity and risk management.

Information is an asset that can make or break an organization. The management has a duty to safeguard it and manage it appropriately. The Company Secretary's role is crucial. It is a steering role that requires an understanding of the workings of Information Security Management.

Gone are the days when the Company Secretary was merely a minute taker. In modern organizations the Company Secretary takes part in the

[40] See clause 5,7,8 of ISO 27001:2005; clause 5,6,8 of ISO 9001:2000; clause 4.3, 4.4.2, 4.6 of ISO 14001: 2004

management and decision making of the organization. The setting up of an effective Information Security Management System will require the active participation of the Company Secretary at various stages beginning from policymaking, implementation monitoring, review and continuous improvement.