Information Security Management – A New Paradigm

JAN ELOFF
Pretoria University
and
MARIKI ELOFF
University of South Africa

Information security management needs a paradigm shift in order to successfully protect information assets. Organisations must change to the holistic management of information security, requiring a well-established Information Security Management System (ISMS). An ISMS addresses all aspects in an organisation that deals with creating and maintaining a secure information environment. Organisational management and their staff to manage information security cost-effectively can use the ISMS. It can also help with the assessment of the trustworthiness of an organisation's information security arrangements by other organisations. An intelligent mix of aspects such as policies, standards, guidelines, codes-of-practice, technology, human issues, legal and ethical issues constitute an ISMS. Ideally organisations should opt for a combination of these different aspects in establishing an ISMS. The initial combination of all the aspects might by a bridge too far when embarking on the establishment of an ISMS, forcing organisations to take a 'phased' approach. One approach can be to implement the controls as contained in a standard such as ISO17799. In this case information security is driven from a management process point of view and referred to as 'process security'. Another approach that also complement or add to process security, is to use certified products in the IT infrastructure environment when possible. The approach here focuses on technical issues and is referred to as 'product security'.

Categories and Subject Descriptors: Km [**Computing Milieu**]: Miscellaneous – *Information Security Management*;
General Terms:
Additional Key Words and Phrases: certification, certified products, code of practice, controls, evaluation criteria, guideline, Information Security Management System, process evaluation, product evaluation, protection classes, self-assessment, standards

1. INTRODUCTION

Management who want to address any information security-related issues as part of Information Security Management in their organisation, need to implement some form of an Information Security Management System (ISMS). An Information Security Management System can be defined as a management system used for establishing and maintaining a secure information environment. This ISMS must address the implementation and maintenance of processes and procedures to manage Information Technology security. These actions include identification of information security needs, implementation of strategies to meet these needs, the measurement of results, and improving both the protection strategies and the ISMS over time. Information Technology (IT) security includes all aspects related to defining, achieving and maintaining the five security services of identification & authentication, authorisation, confidentiality, integrity and non-repudiation as specified by the ISO 7498-2 standard. (ISO 2002)

The domain of Information Security Management is no longer exclusively of a managerial nature, technical aspects also need to be considered on management level. Information Security Management can be approached from various perspectives. One way of establishing an ISMS is from a strategic perspective, addressing amongst others corporate governance, policies and pure management issues. Another approach can be from a 'human' side, addressing issues such as security culture, awareness, training, ethics and other human related issues. The technology ISMS may focus on software and hardware products. The process ISMS promotes the implementation of the controls as contained in a standard or code-of-practice, such as ISO17799 and compliance to these controls. It is important to note that Information Security Management need to take a holistic approach, requiring a combination and integration of all the abovementioned ISMSs. This holistic approach is illustrated in figure 1. Standards might include technical specifications which refer to aspects such as IT network security, digital signatures, access control, non-repudiation, key management and hash functions. Procedures refer to operational, management and technical procedures, e.g. procedures for classification of information or for obtaining a user-id. Management system audits, certification & accreditation is the audit and certification of information management systems. The South African National Accreditation System (SANAS) is the official accreditation body in South Africa that gives formal recognition that Certification Bodies, like STANSA (Standards South Africa) are competent to carry out audit and certification. Codes-

Author Addresses:
JHP Eloff, Department of Computer Science, University of Pretoria, Lynnwood Road, PRETORIA, 0002, South Africa; eloff@cs.up.ac.za.
MM Eloff, Department of Computer Science and Information Systems, University of South Africa, P O Box 392, UNISA, 0003, South Africa; eloffmm@unisa.ac.za

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial advantage, that the copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than SAICSIT or the ACM must be honoured. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists, requires prior specific permission and/or a fee.
© 2003 SAICSIT

of-Practice include ISO17799. Assurance and product and system testing and evaluation are addressed through protection profiles, frameworks for IT security assurance, the Common Criteria and system evaluation. (ISO 2003) Culture, Ethical and Social Issues address the human aspects in Information security management.

There are various different existing standards, guidelines and specifications that can be implemented in support of an ISMS (ISO 2003), such as ISO9001, ISO 17799, BS 16000, ISO Guide 62, TR13335, Common Criteria and many more (ISO 2003).

In this paper the authors will combine two of these aspects, namely the process ISMS, using ISO 17799 as basis, and the product ISMS, using the Common Criteria and other product evaluation standards as basis.

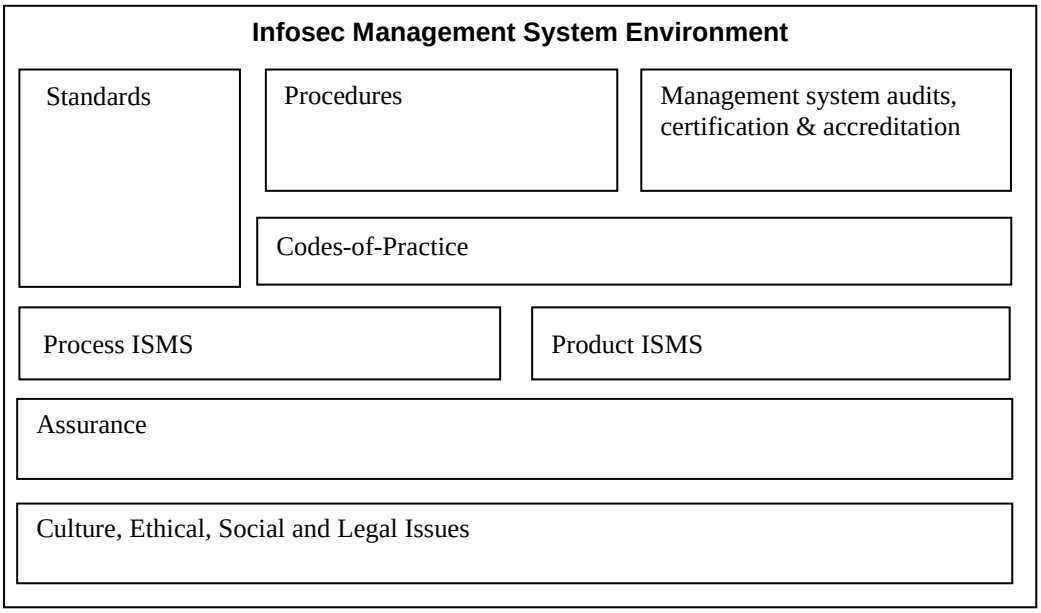

Figure 1. **Components of ISMS**

The remainder of this paper is structured as follows:

- Section 2 contains definitions of the process ISMS and the product ISMS.
- Section 3 contains a high-level overview of the concept of 'protection classes'
- Section 4 defines and explains the requirements for the different protection classes

2. PROCESS AND PRODUCT ISMS

2.1 Process ISMS

Process ISMS is defined as a two-phase information security management system focussing on planning and implementing management practices, procedures and processes to establish and maintain information security. The Information Security Policy will form the basis of the process ISMS (Hone, 2002). An organisation firstly needs to implement the controls or guidelines as contained in a standard code-of-practice such as ISO17799 (ISO17799). Secondly, these implemented controls need to be assessed to determine whether they comply with the specific standard. External certification is the formal process whereby an independent third party, who may be an individual or an organisation, that has the approval of a national or an international body, performs this assessment process. Internal certification is done within the organisation and no official formal recognition is attached.

Information security managers using this approach will first identify and select the processes to be implemented, such as the screening of new employees, then implement the processes to enable screening. The next step is to check if all new employees are indeed screened. Depending on the outcome, the action to take can be adjustments or additional processes. The process ISMS is an iterative system with feedback and continuous improvements. The concept of 'Plan-Do-Check-Act' is important when implementing an ISMS (ISO 2003). Each process may not necessarily be implemented correctly with the initial implementation, even with thorough planning. Some 'fine tuning' may be required after checking so as to assure that the process is enhanced if necessary to be implemented optimally.

This paper focuses on the process certification ISMS, by checking the processes implemented. This requires that the organisation has planned and implemented management processes and procedures such as the controls contained in ISO17799 standard (ISO17799) or something similar.

2.2 Product ISMS

Product ISMS is the management system where the organisation opts to use evaluated software products as far as possible in their IT infrastructure in order to establish and maintain information security. These evaluated software products and systems forms the basis of the product ISMS. Product evaluation is the process whereby a specific product or system is subjected to a detailed series of tests to determine whether it satisfies a predefined set of requirements.

Normally an independent third party expert technically reviews the design and implementation of a software product or system. If it satisfies the requirements, it will be classified at a specific level, for example the B2 level under TCSEC (NGI 1995). For example, Class B2: 'Structured Protection' increases the assurance by adding requirements to the design of the system and requires covert channel analysis and audit of events that can potentially create covert channels. The design and implementation of the Trusted Computing Base for B2 also require more thorough testing and a more complete review (Pfleeger 2003). These software products are also termed certified products. Trusted Oracle8i was evaluated EAL4 under the Common Criteria (CC 2002). It should be noted that the scope of product ISMS is limited to products or systems, and does not currently have any references to an organisation's information security management processes (Eloff 2000). However, evaluated software products should also form part of the process certification ISMS, but then the focus will not necessarily be on the product ISMS.

Evaluated or certified products can be categorised in a number of different generic product categories, such as Databases, Networks and Operating systems. Each of these different categories can be potentially linked and mapped onto the sections of a code-of-practice, such as the ISO17799 standard. If, for example, a product were certified as a secure database product, one could safely assume that such a product is aimed at enhancing for one the procedures and processes for secure application development. A secure database can also enhance for example procedures and processes in the personnel security section. The remainder of this paper is based on the ISO17799 standard. The reader should notice that any other code-of-practice could also be used as part of the illustration that follows.

A suggestion on how the relationship between the product categories and the ten sections of ISO17799 can be modelled, are summarised in table 1. Note that this table is not necessarily complete, but adequate to illustrate the concept of protection classes which is discussed the next section of this paper. Some lower level detail for 8. Communications and operations management is also illustrated. The proper relationship modelling between controls of a code-of-practice and the product categories is a comprehensive task and requires functional as well as technical expertise. The entries in the table show the strengthening of a control area in case certified products are used in implementing and managing the processes of that specific control area. Asset classification and control will gain from using a certified DBMS as the repository of information.

Table 1: Mapping some of the product categories on ISO 17799

ISO17799 Sections	Databases	Networks	Operating systems
3. Security policy			
4. Security organization		Y	
5. Asset classification and control	Y		
6. Personnel security	Y		
7. Physical and environmental security		Y	
8. Communications and operations management	Y	Y	Y
:			
8.4 Housekeeping			
8.4.1 Information back-up	Y		Y
8.4.2 Operator logs			Y
8.4.3 Fault-logging	Y	Y	Y
8.5 Network management			
8.5.1 Network controls		Y	
8.7 Exchanges of information and software			
8.7.1 Information and software exchange agreements	Y	Y	Y
8.7.2 Security of media in transit		Y	
8.7.3 Electronic commerce security		Y	
8.7.4 Security of electronic mail		Y	
8.7.5 Security of electronic office systems		Y	

:			
9. Access control	Y	Y	Y
10. Systems development and maintenance	Y	Y	Y
11. Business continuity management	Y	Y	Y

3. OVERVIEW OF PROTECTION CLASSES FOR COMBINING PRODUCTS ISMS WITH PROCESSES ISMS

The primary focus in process ISMS is on management processes and procedures, therefore compliance to each one of the ten sections of ISO17799 will be classified into one of four classes. This classification will be done on Section level for ISO17799, firstly to take cognisance of the fact that not all the sections may be of equal importance to organisations and secondly, certified products will not impact equally on all the sections of ISO17799. The focus on the sections of ISO17799 allows an organisation to initially concentrate on specific sections and expand to address subsequent sections at a later stage. Full compliance with ISO17799 may be 'a bridge too far' for many companies, and may, in fact, also be inappropriate.

The authors have decided to define four distinct protection classes, with increasing levels of protection (Eloff 2003). The implementation of the controls in each one of the ten sections of ISO17799 will be categorised into one of these four classes, firstly depending on the level of compliance to the controls of ISO17799, the process ISMS and secondly, influenced by the use of certified products associated with each section, the product ISMS (Eloff 2000[1]), (Eloff 2000[2]).

The four protection classes, in ascending order, are:

— Class 1: Inadequate protection

Sections of a code-of-practice will be classified in this class if no effort was made by the organisation to implement any of the recommended controls for their specific requirements. This is the lowest class. Certified products do not have any influence on the classification of sections on this level.

— Class 2: Minimal protection

If minimal effort was put into implementing some of the recommended controls, it will be possible to classify some sections in this class. The same requirement as for Class 1 is applicable for the code-of-practice controls in some of the sections. Certified products do not have any influence on the classification of sections on this level either.

— Class 3: Reasonable protection

The same requirement as for Class 2 is applicable for the code-of-practice controls in some of the sections. The majority of the sections must satisfy additional requirements based on implemented processes and procedures to prove that the recommended controls from the code-of-practice are implemented on a reasonable level. Some sections have an additional requirement for certified products to be used.

— Class 4: Adequate protection

For a section to be classified as adequately protected, it must be verifiable that considerable effort was made to implement the complete set of recommended controls for the section. This implies full compliance to a code-of-practice for that specific section. Furthermore, the majority of sections have an additional requirement that certified products, in all the product categories, must be implemented to illustrate adequate protection. If there are no related product categories for an ISO17799 section, it is possible for that section to advance to this class in the absence of certified products.

Figure 2 is an example of the graphical representation of the protection classes associated with each of the ten sections of ISO17799 (ISO17799).

ISO17799 Section name	Protection Class			
	Class 1: Inadequate protection	Class 2: Mini-mal protection	Class 3: Reasonable protection	Class 4: Adequate protection
Section 3: Security policy				
Section 4: Security organisation				
Section 5: Assets classification and control				
Section 6: Personnel security				
Section 7: Physical and environmental security				
Section 8: Communications and operation management				
Section 9: Access control				
Section 10: Systems development and maintenance				
Section 11: Business continuity planning				
Section 12: Compliance				

Figure 2. **The Graphic illustration of Protection classes**

From a graphic summary like this an organisation can determine the weak areas that needs improvement, for example the security policy, business continuity planning and compliance.

4. REQUIREMENTS FOR THE DIFFERENT PROTECTION CLASSES

4.1 Requirements for Class 1: Inadequate protection

If no effort was made by the organisation to implement any of the recommended controls for their specific requirements, the appropriate Sections of ISO17799 will be classified in this class. This is the lowest class.

The use of certified products on their own do not have any influence on the classification of ISO17799 sections; it can only enhance the implemented processes and procedures.

The following example illustrates this: An organisation are using only certified products associated with for example Section 9: Access Control, but have not implemented any of the procedural controls contained in this section of a code-of-practice. Section 9 can only be classified into the class of Inadequate protection.

All sections of ISO17799 can be classified in Class 1 if no effort was made to implement any of the controls.

4.2 Requirements for Class 2: Minimal protection

If minimal effort was put into implementing some of the recommended controls, it will be possible to classify some sections in this class. The same requirement as for Class 1 is applicable for the ISO17799 controls in some of the sections. The actual compliance of the implemented processes and procedures for the applicable sections should be at least 75% of the recommended controls before a specific section can be allocated in Class 2.

Certified products do not have any influence on the classification of sections on this level either. Take the same illustration as for Class 1, except that the implemented processes and procedures comply 80% with the controls contained in Section 9. Section 9 can therefore now be classified as minimally protected because of the implemented procedural controls.

It is clear that for Sections 6 to 9 to be classified as Minimally protected, an organisation need to prove that the implemented processes and procedures should comply with at least 75% of the controls as prescribed in ISO17799. The other sections can be classified as Minimally protected without proving any compliance.

4.3 Requirements for Class 3: Reasonable protection

The same requirement as for Class 2 is applicable for the ISO17799 controls in some of the sections. The majority of the sections must satisfy additional requirements based on implemented processes and procedures.

Some sections can advance to this class if actual compliance of the implemented processes and procedures comply with at least 75% of the recommended controls.

Some sections have an additional requirement for certified products to be used. Certified products for at least half of the appropriate product categories per section in ISO17799 should be implemented. A minimum of 75% of the implemented products within a specific product category, i.e. IT products already installed, must be certified products before it can influence the classification of a specific section.

These requirements will allow Section 9: Access Control, as used in the example for Class 2 to now be classified in the Reasonably protected class. Implemented processes and procedures comply 80% with the recommended, and all products used in both product categories applicable to this section, are certified products, satisfying the minimum 75% requirement for implemented products.

All sections have additional requirements to be classified as Reasonably protected.

4.4 Requirements for Class 4: Adequate protection

For a section to be classified as adequately protected, it must be verifiable that considerable effort was made to implement the complete set of recommended controls for the section. This implies full compliance to ISO17799 for that specific section.

Furthermore, the majority of sections have an additional requirement that certified products, in all the product categories, must be implemented to illustrate adequate protection.

If there are no related product categories for an ISO17799 section, it is possible for that section to advance to this class in the absence of certified products.

If we take the example of Section 9: Access Control as used in this explanation, this section can now be classified as adequately protected, as all products used are certified products, satisfying the requirement of certified products, in all the product categories, to be implemented.

The following table, table 2, summarises all the protection requirements for the ten sections of ISO17799.

Table 2: Protection requirements for ISO17799 sections

ISO17799	**Protection class**			
	Class 1: Inadequate protection	Class 2: Minimal protection	Class 3: Reasonable protection	Class 4: Adequate protection
3. Security policy			☒	☒
4. Security organisation			☒	☒☒
5. Asset classification and control			☒	☒
6. Personnel security		☒	☒☒	☒☒☒
7. Physical and environmental security		☒	☒☒	☒☒☒
8. Communications and operations management		☒	☒☒	☒☒☒
9. Access control		☒	☒☒	☒☒☒
10. Systems development and maintenance			☒	☒☒☒
11. Business continuity management			☒	☒☒☒
12. Compliance			☒	☒

Legend:

	no requirement
☒	additional requirement based on implemented processes and procedures
☒☒	additional requirement based on implementation of certified products in at least half of the applicable product categories
☒☒☒	additional requirement based on implementation of certified products in all of the applicable product categories

5. CONCLUSION

In order to successfully secure the information and technology related assets of an organization, management should aim towards establishing an ISMS. A well-defined ISMS includes a wide spectrum of issues to be addressed during the planning, management ad monitoring of information security within an organisation. Apart from the people issues, which are critical to any successful information security program, a relationship between processes as identified in a code-of-practice and certified IT products should be sought after. This paper proposes a framework to facilitate a relationship between processes and products. Successful implementation of the proposed framework will contribute to a holistic approach to Information Security Management.

6. REFERENCES

(CC 2002) Common Criteria http://niap.nist.gov/cc-scheme/iccc/TrackC/Smith/sld004.htm, October 2002

(Eloff 2000) ELOFF MM, VON SOLMS SH, 2000, Information Security management: a hierarchical framework for various approaches, Computers & Security, Volume 19 Number 3, pp 243-256

(Eloff 2000[1]) ELOFF MM, VON SOLMS SH, 2000, Information Security management: an approach to combine process certification and product evaluation, Computers & Security, Volume 19 Number 8, pp 698-709

(Eloff 2000[2]) ELOFF MM, 2000, A Multi-dimensional Model for Information Security Management, PhD thesis, RAU

(Eloff 2003) ELOFF, MM., ELOFF, JHP., 2003, Information Security Management System: processes and products Proceedings of IFIP SEC 2003, May 2003, Athens, Greece,

(Hone 2002) HÖNE, K, ELOFF, JHP (2002), What makes an Effective Information Security Policy? Network Security, Vol. 2002 (6), pp. 14-16

(ISO 2002) ISO 7498-2, International Standards Organisation, Nov 1999 http://www.iso.ch, October 2002

(ISO 2003) ISO/IEC JTC 1/SC 27 N 3518, Apr 2003, Summary of National Body contributions to SC 27/WG 1 study period on Information security management systems (ISMS) (ref. document SC 27 N 3331rev2),

(ISO17799) ISO/IEC 17799 Code of practice for Information Security Management, International Organization for Standardization/ International Electrotechnical Commission, 01-Mar-2000, http://www.iso.ch/iso/en/ISOOnline.openerpage

(NGI 1995) Evaluatie Kriteria voor IT-beveiliging, 1995, Nederlands Genootschap voor Informatica Afdeling Beveiliging, Edited by Dr Ir PL Overbeek, Kluwer BedryfsInformatie

(Pfleeger 2003) PFLEEGER, CP AND PFLEEGER, SL (2003). Security in Computing. Prentice Hall: Upper Saddle River, NJ