INFORMATION SECURITY MANAGEMENT SYSTEM: PROCESSES AND PRODUCTS

M.M. ELOFF[1], J.H.P. ELOFF[2]

[1]*eloffmm@unisa.ac.za*
Department Computer Science & Information Systems,
University of South Africa,
PO Box 392, Unisa, 0003
South Africa
Telephone: + 27 (0) 12 429 6336
Facsimile: + 27 (0) 12 429 6655
[2]*eloff@cs.up.ac.za*
Department of Computer Science,
University of Pretoria,
Pretoria, South Africa
Telephone: +27 (0) 12 420-3120
October 2002

Key words: certification, certified products, code of practice, controls, evaluation criteria, guideline, Information Security Management System, process evaluation, product evaluation, protection classes, self-assessment, standards,

Abstract: The executive and operational management of organisations today realise that the successful protection of information assets depend on a holistic approach towards the implementation of safeguards. A holistic approach requires that the focus of management should rather be on minimising overall risk exposure as opposed to "tick-off" security safeguards on a checklist. The holistic management of information security requires 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. Aspects such as policies, standards, guidelines, codes-of-practice, technology, human, legal and ethics issues all from part of an ISMS. Organisations can opt for different approaches to establishing an ISMS. One way is to implement the controls as contained in a standard or code-of-practice, 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

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35691-4_52

D. Gritzalis et al. (eds.), *Security and Privacy in the Age of Uncertainty*

approach here focuses on technical issues and is referred to as "product security". The 'process' ISMS and the 'product' ISMS approaches are only two ways to address information security, each from a different perspective. The question that arises is whether the 'process' ISMS and the 'product' ISMS can be combined into a more holistic ISMS and what the impact of the one will be on the other. The aim of this paper is to propose an ISMS that combines "process security" and "product security".

1. INTRODUCTION

Management who want to address any information security-related issues in their organisation, need to follow some form of an Information Security Management System. An Information Security Management System (ISMS) 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. 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. [ISO02]

An ISMS can be approached from various perspectives. One way of establishing an ISMS is from a strategic perspective, addressing amongst others corporate governance, policies and 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 products. Another ISMS, the technical ISMS may focus on physical issues such as hardware. The processes 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 an ISMS need to take a holistic approach, requiring a combination and integration of all the abovementioned ISMSs.

In this paper the authors will combine two of these approaches, namely the process ISMS and the product ISMS and determine the influence of the one on the other.

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. [HONE02]An organisation firstly needs to implement the controls or guidelines as contained in a standard such as ISO17799. [ISO17799] Secondly, these implemented controls need to be assessed to determine whether they comply with the specific standard. 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.

Information security managers using this approach by will first plan the processes to be implemented, such as the screening of new employees; then implement the processes to ensure screening. The next step is to check if all new employees are indeed screened. Depending on the outcome, action can be adjustments or additional processes. The process ISMS is an iterative system with feedback and continuous improvements.

This paper focuses on the second tier of the process ISMS by checking the processes implemented and 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 C2 level

under TCSEC. [NGI 95] These software products are also termed certified products. Trusted Oracle8i was evaluated EAL4 under the Common Criteria. [CC02] 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. [ELOF00] However, evaluated software products can also form part of the process ISMS, but then the focus will not necessarily be on the product ISMS.

In a previous article by the authors, [ELOF00[1]], the influence of evaluated products on the implemented controls from a code-of-practice were illustrated. Evaluated or certified products can be categorised in a number of different generic product categories, such as Communication systems, 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 ISO17799 standard. The remainder of this paper is based on the ISO17799 standard. The reader should notice that any other code-of-practice can 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 the next table. 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. 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.

ISO17799 Sections	Commu-nication systems	Data-bases	Net-works	Operating systems
3. Security policy				
4. Security organisation	Y		Y	
5. Asset classification and control		Y		
6. Personnel security	Y	Y		
7. Physical and environmental security			Y	
8. Communications and operations management	Y	Y	Y	Y
9. Access control	Y	Y	Y	Y
10. Systems development and maintenance	Y	Y	Y	
11. Business continuity management		Y	Y	Y
12. Compliance				

3. OVERVIEW OF PROTECTION CLASSES FOR COMBINING CERTIFIED PRODUCTS WITH EVALUATED PROCESSES

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 categorised 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. Classifying the sections of ISO17799 allows an organisation to initially focus 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. 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. [ELOF00[1]], [ELOF00[2]]

The four protection classes, in ascending order, are:

- Inadequate protection
- Minimal protection
- Reasonable protection
- Adequate protection

The following protection classes may, for example, be associated with each of the ten sections of ISO17799 [ISO17799]: This can be given in a graphic format, as illustrated in Figure 1.

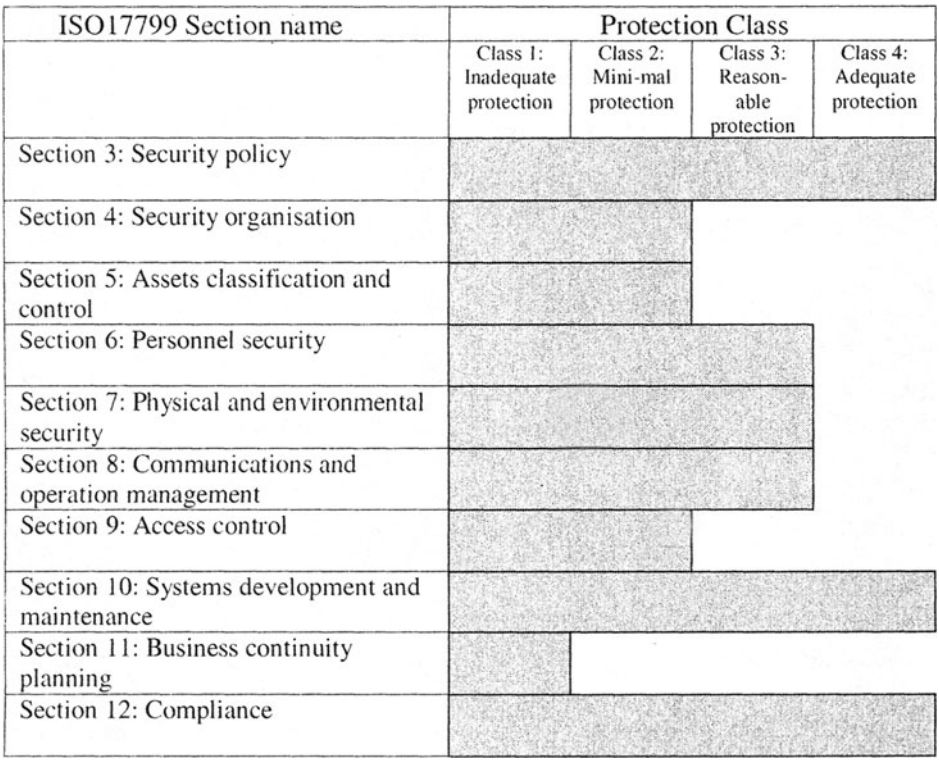

Figure 1. The Graphic illustration of Protection classes

From a graphic summary like this it will be easy for an organisation to determine weak areas that needs improvement.

A brief explanation of each protection class follows:

3.1 Class 1: Inadequate protection

Sections of ISO17799 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.

3.2 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.

Certified products do not have any influence on the classification of sections on this level either.

3.3 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 to prove that the recommended controls from ISO17799 are implemented on a reasonable level.

Some sections have an additional requirement for certified products to be used.

3.4 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 a ISO17799 section, it is possible for that section to advance to this class in the absence of certified products.

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 controls contained in this section. Section 9 can only be classified into the class of Inadequate protection.

Table 2 summarises the requirements for Class 1 for all the sections of ISO17799.

Table 2: Security Requirements for Class 1

ISO17799	Class 1: Inadequate 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

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.

Table 3 summarises the requirements for Class 2 for all the sections of ISO17799.

Table 3: Security Requirements for Class 2

ISO17799	Class 2: Minimal 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

From this table 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.

Table 4 summarises the requirements for all the sections of ISO17799 for Class 3.

Table 4: Security Requirements for Class 3

ISO17799	Class 3: Reasonable 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

From this table it is clear that 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 5, summarises all the protection requirements for the ten sections of ISO17799.

Table 5: 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

It has become manifest from this paper that management will, in future, have to follow a holistic approach when establishing an Information Security Management System, so that such issues could be addressed not only in the electronic domain but also in the procedural and process domains. In

addition, it has become abundantly clear that the mere use of products certified under, say, the Common Criteria, or any other formal product-evaluation scheme, will by no means guarantee the Information Security status of an organisation. Following guidelines such as those contained in ISO17799 will, however, not ensure adequate Information Security status in an organisation either.

The combination of a process ISMS and a product ISMS into this one classification model allows management to implement a standard such as ISO17799 as well as certified products such as Oracle 8i to the best benefit of the information security status of the organisation.

This article illustrates how the process ISMS and the product ISMS can be combined and further visualised by the proposed protection classes.

If two identical organisations were to implement the exact same ISO17799 controls to the same exacting standards, but one company elected to use only certified products in so doing, whilst the other elected not to, the Information Security status of the former would be bound to outrank that of the latter!

6. LIST OF SOURCES CONSULTED

[CC02] Common Criteria http://niap.nist.gov/cc-scheme/iccc/TrackC/Smith/sld004.htm, October 2002

[ELOF00] Eloff MM, Von Solms SH, 2000, Information Security management: a hierarchical framework for various approaches, Computers & Security, Volume 19 Number 3, pp 243-256

[ELOF00[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

[ELOF00[2]] Eloff MM, 2000, A Multi-dimensional Model for Information Security Management, PhD thesis, RAU

[HONE02] Höne, K, Eloff, JHP (2002), What makes an Effective Information Security Policy? Network Security, Vol. 2002 (6), pp. 14-16

[ISO02] ISO 7498-2, International Standards Organisation, Nov 1999 http://www.iso.ch, October 2002

[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

[NGI95] Evaluatie Kriteria voor IT-beveiliging, 1995, Nederlands Genootschap voor Informatica Afdeling Beveiliging, Edited by Dr Ir PL Overbeek, Kluwer BedrytsInformatie