Information Security: Process Evaluation and Product Evaluation

M.M. ELOFF[1], S.H. VON SOLMS[2]

[1]meloff@twrinet.twr.ac.za
School of Information Technology, Technikon Witwatersrand, Johannesburg, South Africa
[2]basie@rkw.rau.ac.za
Department of Computer Science
Rand Afrikaans University
PO Box 524
AUCKLAND PARK
2006
South Africa
March 1999
Tel: +27 11 489-2847 Fax: +27 11 489-2138

Key words: Certification, Controls, Standards, Guideline, Code of practice, Process evaluation, Evaluation criteria, Product evaluation.

Abstract: Effective management in any organisation requires a holistic approach in focusing on information security. Senior managers have to know how well their organisations are performing as measured against internationally accepted best practices. Part of the information security management problem is that it is viewed either from a technological perspective focussing on product evaluation only, or from a procedural and management perspective focussing on evaluation of the management processes. This paper aims to provide a consolidated perspective that takes both these aspects into consideration when measuring and evaluating the information security level of an organisation.

1. INTRODUCTION

Today, successful management of IT resources in any organisation necessitates taking a holistic approach to information security by addressing

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: 10.1007/978-0-387-35515-3_53

S. Qing et al. (eds.), *Information Security for Global Information Infrastructures*

all the security needs in a structured manner. Structured, in this context, refers not only to cost efficiency of operating budgets, but also to securing all the IT resources and assets of an organisation adequately. Two internationally accepted approaches in securing IT resources are:

ξ Information security process evaluation

ξ Information security product evaluation

These two approaches are depicted in the following diagram.

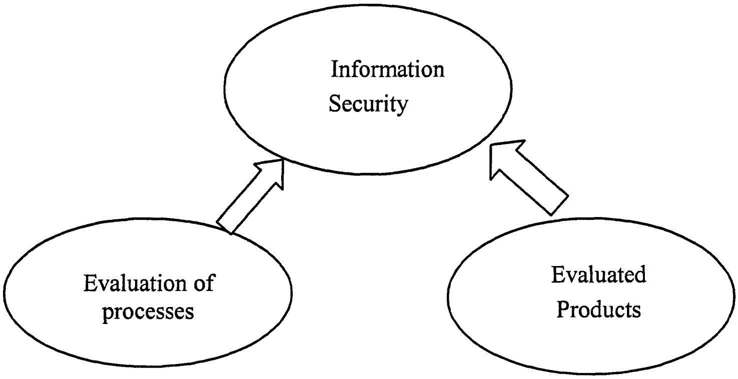

Figure 1. Scope of Information Security

Process evaluation is defined as the process whereby an organisation, procedure or process is tested and evaluated to determine whether it complies with a 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 the evaluation process. This third party has the authority to issue a formal statement on the compliance or non-compliance of the tested organisation, procedure or process's with the required standard.

The BS7799 Code of Practice for Information Security Management is already internationally well known and accepted as an approach to Information Security process evaluation and/or certification. [BS77 99]

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 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] It should be noted that the scope of product evaluation is limited to products or systems, and does not currently have any references to an organisation's information security management processes.

The main objective of this paper is to assess the impact of product evaluation on the evaluation of the processes and procedures that determine the overall information security level of the organisation.

The remainder of this paper is structured as follows:

ξ An illustration of what is meant with the overall information security level of an organisation.

ξ A discussion of concepts which might play a role in determining the overall information security level, including both process evaluation and product evaluation

2. THE OVERALL LEVEL OF INFORMATION SECURITY

The information used during the evaluation of information security procedures and processes can be quantified in order to indicate a percentage compliance with the particular standard, for example BS7799. 'Process evaluation'- can be presented graphically to indicate the level of information security, as depicted by the 70% for BS7799 in Figure 2. Figure 2 also gives an indication that product evaluation and process evaluation must be combined in determining the overall level of an organisation's information security level. In Figure 2, the compliance of Company_X with BS7799 is indicated on the right, i.e. process evaluation, as 70%. The evaluated products are depicted on the left.

It is important to note that compliance with an international information security management standard such as BS7799 is the primary aim. The secondary aim is to consider evaluated products in determining the overall level of information security. Use of evaluated products can only improve BS7799 compliance. The absence of evaluated products should not decrease this level.

The shaded area indicating the enhancement of process evaluation only represents a positive influence on the information security level and has no numerical value associated with it. Further research is required to develop such a quantification mechanism.

The objective of merging process evaluation and product evaluation demands consolidating common as well as distinctive issues from both product evaluation and process evaluation. Below some aspects will be outlined for combining process evaluation and product evaluation.

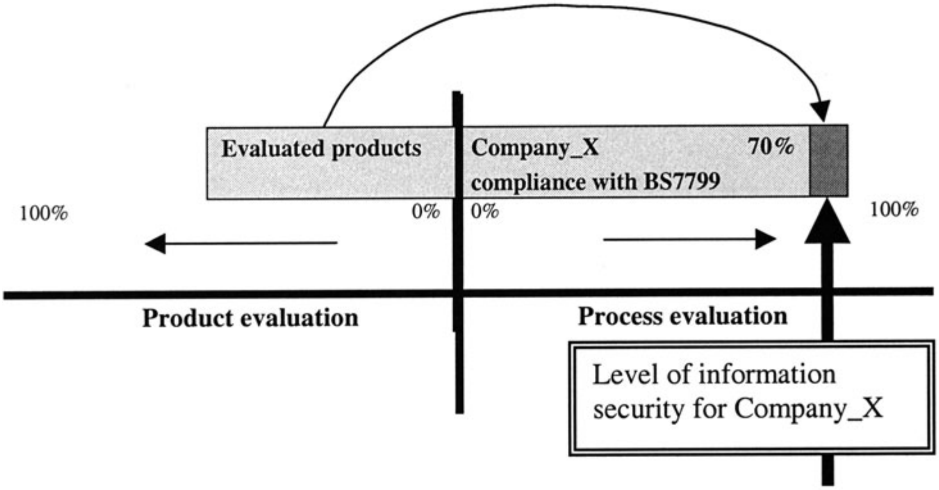
Evaluated products
Company_X compliance with BS7799
70%
100%
0%
0%
100%
Product evaluation
Process evaluation
Level of information security for Company_X

Figure 2. Indicating the potential influence of evaluated products on the information security level of Company_X

3. COMBINING PRODUCT EVALUATION AND PROCESS EVALUATION

Even though there is no direct link between for example BS7799 and ITSEC or CC, BS7799 states that a company should consider the use of independently evaluated products. On the other hand, BS7799 is not prescriptive about the use of evaluated software. [BS77 99] However, in the opinion of the authors of this paper, there are definite advantages to combining product evaluation and process evaluation in the process of determining an organisation's overall information security level.

With no direct link existing between BS7799 and product evaluation schemes, it was decided to build a link between product categories (Figure 3) and BS7799. Since the categories of evaluated products for the various product evaluation schemes appear to have a great deal in common, the authors of this paper have decided to use the following product categories in their analysis: [CCIN 99], [CCPP 00], [CSE 99]

Categories of evaluated products					
Database	**Communications**	**Miscellaneous**	**Networks**	**Operating System**	**PC Access**

Figure 3. Categories of evaluated products

It is important to notice that the categories depicted in Figure 3 are chosen specifically to assist in the matching of controls (processes and procedures), being part of a process evaluation scheme, with evaluated products. The reader should notice that these categories are only suggestions and can be adapted to include other product categories.

The categories mentioned in Figure 3 facilitate the merging of product evaluation and process evaluation. For example, if a product is evaluated as a secure database product, one can assume that it strengthens the procedures and processes in the secure application development section, of a process evaluation scheme. Furthermore, a secure database product will also have a positive effect on other procedures and processes being part of a process evaluation scheme such as BS7799 or COBIT.

Not all the controls in BS7799 can be related to specific products, and therefore only some of the sections can be influenced partially by evaluated products. As an example, consider the product evaluation categories mapped onto Section 6 of BS7799, which yield the following table. Only a sub set of the relevant sub controls of BS7799 – Section 6 is listed. [BS77 99]

Table 1. Mapping of product evaluation categories onto Section 6 of BS7799

	Database	Communications	Miscellaneous	Networks	Operating System	PC access
6.3 Protection from malicious software						
6.3.1 Virus controls		Y		Y	Y	Y
6.4 Housekeeping						
6.4.1 Data back-up	Y	Y			Y	
6.4.2 Operator logs					Y	Y
6.4.3 Fault logging	Y	Y		Y	Y	Y
6.4.4 Environmental monitoring						
6.5 Network management						
6.5.1 Network security controls		Y		Y		
6.7 Data and software exchange						
6.7.1 Data and software exchange agreements	Y	Y		Y	Y	Y
6.7.2 Security of media in transit		Y		Y		

The proper mapping of BS7799 controls and evaluated products is a difficult task and requires functional, as well as technical expertise. The concept of mapping evaluated products onto controls (BS7799) is believed to be one of the most interesting contributions that this research effort can make in the future. The purpose of the above table is primarily to indicate a linkage between evaluated network products and Section 6 of BS7799. It is reasoned that if evaluated network products form part of a company's product base, the relevant processes of Section 6 are strengthened.

The relationship between all the BS7799 controls and the product categories can be indicated in the same manner. The next paragraph gives suggestions on how to assess the status of implemented network products.

3.1 Assessing the impact of evaluated products

Studying the organisation's product profile can assist in assessing the impact of evaluated products. The inventory of information technology (IT) products can be used to determine which products are certified as evaluated products.

The results shown in the graphs below is based on the principle of expressing the number of evaluated products in a category, as a percentage of all products for that specific product category, used in the organisation. The reader should note that this simplistic way of assessing the impact of evaluated products could lead to misrepresentation. Another factor, which plays an important role in this calculation, is the importance of a specific IT product for the organisations processes and IT architecture. Furthermore, evaluated products must be used on at least an acceptable number of platforms within the organisation. Table 2 shows an example product profile extracted from the product inventory for Company_X. [CSE 99], [ITSE 99], [HIST 99], [SIN 99]

Table 2. Example product profile for Company_X

Product Category	Product	Level	Date	Evaluated by
Databases	Oracle7	C2/E3	1994/98	TCSEC/ITSEC
	INFORMIX-OnLine Dynamic Server v.7.23	E2	1998	ITSEC
	Paradox			Not evaluated
	Sybase, Inc.	C2	1997	TCSEC
Operating systems	MS Windows NT Workstation and Server	C2/E3	1999/99	TCSEC/ITSEC
	Sun Solaris 2.5.1SE	E2	1998	ITSEC
	UNIX			Not evaluated
Communications	The MLS LAN Secure Network Server System	A1	1991	TCSEC
	Microsoft Outlook Express 5			Not evaluated
	Netscape Navigator			Not evaluated
Networks	Banyan VINES Version 7.0	E2	1997	ITSEC
	VCS Firewall Version 3.0	EAL1	1999	CC
	Novell NetWare 4.11	C2	1997	TCSEC
	Hewlett Packard Openview			Not evaluated
PC-access	Disknet NT Version 1.70	E2	1999	ITSEC
	Watchdog PC Data Security version 7.0.2	D	1994	TCSEC
	Walther Cardtype Version E004/006	E2	1995	ITSEC
	WordPerfect			Not evaluated

The results, showing the percentage of evaluated network products in relation to the total number of network products, are depicted in the diagram that will follow.

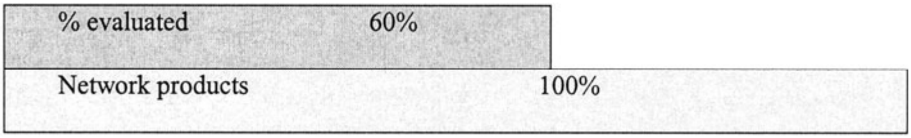

Figure 4. Profile of evaluated network products for Company_X

The objective as stated at the beginning of this paper is to determine the impact of Company X's evaluated products, in this case evaluated network products, at the level of BS7799 Section 6 compliance. At this stage of the research it will suffice to say that as the majority of network products for Company_X are evaluated, the implementation of the controls in Section 6 of BS7799 can be enhanced. The following diagram illustrates:

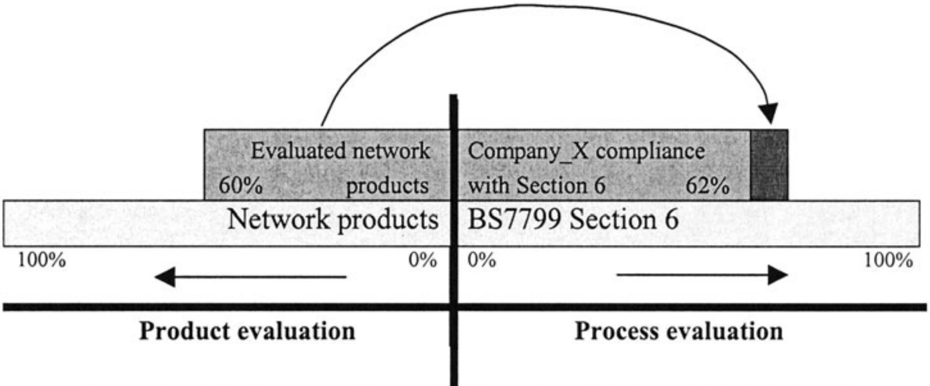

Figure 5. Influence of evaluated network products on Section 6 for Company X

Figure 5 indicates that Company_X's compliance with Section 6 was determined to be 62%. The level of the evaluated network products, which is 60%, (Figure 4) improves the overall level of Section 6 (Computer and Network Management). Note that the shaded area indicating the enhancement, only represents a positive influence, and that no numerical value should be associated with it. Further research needs to be done on this quantification aspect.

Similarly, all the other applicable evaluated product categories are mapped onto Section 6, enhancing the implementation of Section 6 controls in a similar fashion. As product categories differ in respect of their mapping onto detailed BS7799 controls, it stands to reason that each of the product categories may have a differing influence on process evaluation/certification.

4. CONCLUSION

Management must take a holistic approach to information security, thereby addressing issues in the electronic domain as well as the procedural and process domain. Using products evaluated under TCSEC, ITSEC or any other formal evaluation scheme is not sufficient to ensure the overall information security well being of an organisation. On the other hand, implementing guidelines like BS7799 is not sufficient to ensure an adequate information security level for an organisation.

This paper proposes a new approach for combining product evaluation and process evaluation. The argumentation used in this paper is that evaluated products must have a positive impact on information security processes and procedures because evaluated products are shipped with additional impartial information. If two organisations have implemented the BS7799 guidelines in an identical manner, but one uses evaluated products while the other does not, the information security level of the former cannot be the same as that of the latter - it has to be better!!

5. LIST OF SOURCES CONSULTED

[BS77 99] BS7799 Code of practice for Information Security Management, BSI **1999**

[CCIN 99] Common Criteria: An Introduction, **1999, Syntegra, CESG (UK), NIST (USA)**

[CCPP 00] Common Criteria: Protection Profile Listing by Type http://www.cesg.gov.uk/cchtml/ippr/list_by_type.html Jan 2000

[CSE 99] Computer Security Evaluation FAQ, Version 2.1 http://www.faqs.org/faqs/computer-security/evaluations/___6 Jan 2000

[ITSE 99] ITSEC Frequently Asked http://www.itsec.gov.uk **January 2000**

[HIST 99] Historical Evaluated Product List http://www.radium.ncsc.mil/tpep/epl/historical.html___ **January 2000**

[NGI 95] Evaluatie Kriteria voor IT-beveiliging, Nederlands Genootschap voor Informatica Afdeling Beveiliging, Edited by Dr Ir PL Overbeek, Kluwer BedryfsInformatie, 1995

[SINH 99] ORACLE Composite Evaluations: A Perspective, **15th Annual Computer Security Applications Conference, December 1999**