# ROLE OF CERTIFICATION IN MEETING ORGANISATION SECURITY REQUIREMENTS

William List CA FBCS
*Wm. List & Co., W.list@ntlworld.com*

Abstract: Security in systems is now a top priority. Management in organisations wish to be assured that their systems are reliable and that the information provided to stakeholders is secure and correct. This paper explores briefly the two main ISO standards for security - the Common Criteria and the 7799 family. It identifies current limitations in the standards and suggests area where the standards could be developed to assist everyone in meeting the future security needs

Key words: Common Criteria, ISO 17799, Information Security, Improvements, Internal Control, evaluation, certification

## 1. INTRODUCTION

Management wishes to have confidence that the systems they have put in place are functioning as expected and are able to continue to operate in adverse conditions. This is essentially the requirement for an Internal Control system mandated in the OECD guidance on Corporate Governance.

Part of these procedures are automated and there are two main ISO standards Common Criteria (ISO/IEC 15084) and ISO/IEC17799 (BS7799 part 2:2002) which are the basis of evaluation or certification. In addition, and not discussed here, are standards from ISACA (CobiT), IIA, and various other organisations.

The objective of this paper is to raise some issues about certification and evaluation for consideration by those involved as developers, certifiers or evaluators and the people who seek to rely on the certificates issued.

## 2. BACK GROUND

The paper briefly addresses the Common Criteria and 7799 family. The paper also considers the impact of risk analysis and the problems of misunderstandings.

### 2.1 The Common Criteria (CC)

This standard comprises:

- A set of components of security functionality.
- A set of rules for the creation of 'Targets of Evaluation (TOE) and Security Targets (ST)
- A methodology for evaluation of the ST or TOE

A TOis the specification of security functionality as prepared by the organisation submitting a product for evaluation. A ST is the specification of the requirements for a specific implementation.

In addition there are documents called Protection Profiles (PP) which set out generically the totality of the security requirements.

The common criteria is good for evaluation of hardware and/or software products (or groups of products). It does not cover the people element of security except in so far as the people procedures are asserted in the TOE or ST.

The limitations of the Common Criteria are:

- Functionality for batch processing (and essential element in many business processes) is missing.
- Requirement to build in mechanisms to report the contents of files (e.g. access tables) is not specified.
- Product manufacturers select those security functions for evaluation. There may be other security functions in the product, which are not evaluated.
- The evaluation methodology is based on the assumption that the development documentation available for evaluation is not for evolutionary product.

- It is suitable for a system only if the system is a collection of products excluding the people – its effectiveness decreases the more people intervention is required for the system to function.
- It covers security functionality only. If the rest of the product is poor or malfunctions this may cause the results of processing to be wrong (but securely wrong!).

## 2.2 The 7799 family

The 7799 family comprises two standards:

- ISO/IEC 17799 – at present the 2000 version – which is a list of some 125 controls. Organisations select appropriate controls from the list to meet their identified information security needs.
- BS7799 Part 2 – at present the 2002 version – which is the specification for an information security management system (ISMS). Organisations follow the standard to create a system for the ongoing management of information security based on risk analysis.

The 7799 family cover all aspects of Information security; hardware, software and people. Fundamental to the use of the Family is the decision on the scope of the security implementation. The scope could be the entire organisation or some part of it.

Limitations of the 7799 family

- The list of controls in 17799 is biased to the security of the IT infrastructure in that the controls identified for business processes are more concerned with development principles than detailed controls extant in line user departments or specific processes.
- The framework for an ISMS as set out in BS7799 Part 2 is applicable to all situations but if applied within an IT scope may not fully address the business process requirements. This is often true if the people involved have limited experience of the business processes.

## 2.3 Role of Risk analysis

Risk analysis is fundamental to any decisions on the extent to which security measure are required in a product or system. On the basis of the identified threats and vulnerabilities appropriate controls are implemented to cover the risks within the scope of the analysis.

There are always residual risks that are deemed acceptable and there are risks omitted from the analysis and no process is 100%. The result is that

certain impacts will occur and there requires to be processes to find the impacts and take appropriate action.

Where the scope of a certification or evaluation is anything less than the whole organisation the risk analysis will be limited and may therefore place undue weight on certain risks within scope when looked at from the viewpoint of the organisation as a whole.

The question is 'to what extent is the quality of the risk analysis a subject for certification or evaluation?'

In the 7799 schemes provided the risk analysis is accepted by the appropriate official it is unlikely that the auditors will challenge it.

In Common Criteria evaluations the analysis may be challenged but only in an abstract context of a product not the live environment of which the evaluators have no knowledge.

## 2.4 A material problem of misunderstanding?

There are a number of terms in the standards and common usage, which do not necessarily have a consistent meaning. Within individual security (or other) communities the terms are broadly agreed; but outside those communities other definitions exist. The possibility of misunderstanding between individuals and organisations implementing 'information security' and/or certifying or evaluating systems or products are quite substantial. This potential misunderstanding may materially limit the value or comprehension of a certificate or evaluation report to organisations wishing to rely on them.

To enumerate three particular areas as examples of the possible misunderstandings I cite systems, users and audit:

### 2.4.1 Systems

A system is what the writer (speaker) believes it to be at the time. It could be any or all of the following:

- The hardware
- The operating system - or other infrastructure software e.g. a DBMS
- The business process applications
- Including the IT people
- Including the line user people up to the Board level

The problem is whether the reader (or listener) understands the same system as the writer. This is a complication when people are discussing system certification or evaluation - what do they mean?

### 2.4.2 Users

In any particular situation it is reasonably clear who the users are. In general however there are at least three possible interpretations:

- Persons who are in the organisation where IT functionality is used in delivering the business objectives;
- Persons who are in the IT department;
- Customers if you are a vendor of hardware or software.

### 2.4.3 Audit

Audit in many security standards is considered as writing a log (after determining what content should be written to the log).

Audit is considered as the process of creating a certificate or evaluation (sometimes also called evaluation).

Audit may be an internal process whereby independent people check on the work done by other people or automated processes.

Audit is also the term for the performance of financial and other external examinations under a variety of company legislation.

## 3. ARE EVALUATIONS AND CERTIFICATIONS OF ANY VALUE?

The current evaluation of products and certification of security in systems are valuable. They provide a degree of assurance that specified objectives have been achieved. They are not perfect and therefore absolute trust in the results is unwise.

## 3.1 CC Evaluations

The evaluations performed under the CC are appropriate for hardware and software in any combination. They are best when the product requires no external activity to perform correctly and their value diminishes as the

amount of external activity increases. This is because the CC does not address people issues but only the functionality of hardware or software.

They suffer from the limitations set out in 2.1 above

## 3.2 7799 certifications

The usefulness of the certification depends on the scope of the ISMS. The wider the ISMS the more useful the certification is. A 7799 certificate indicates that the organisation has addressed information security in a systematic manner. It does not indicate if specific procedures are in place (which third parties may require) nor necessarily does it indicate effective security is in place.

## 3.3 Non security functionality

CC Evaluations and 7799 Certification are limited to security functionality. They do not intend to address other functions that the systems or products perform. Clearly if the non security functionality in a system fails to perform as expected then the result will be some form of error in the information in the system or reported from the system. Therefore the integrity, in the widest sense, of the information is compromised.

It is possible to set the scope of a 7799 certification to include the necessary controls to address malfunctioning of the non security functionality but it is not possible for CC evaluations.

# 4. WHAT DOES THE BOARD WANT?

The board expects:

- Good information to work on;
- That the system(s) are available when required;
- No loss of confidentiality for organisation's secrets;
- Reasonable confidentiality for legal reasons;
- Reasonable compliance with laws;
- No hindrance to meting business objectives.

These taken together will meet the requirement for the Board to effectively manage the organisation as set out in the OECD Corporate Governance guidelines.

At present the certification and evaluation processes are meeting parts of these objectives but not all of them.

## 5. WHAT COULD BE DONE TO IMPROVE THE SITUATION?

I would like to suggest that the development work at a standards level in regard to the CC and 7799 address the following issues to expand the current standards so as to more closely address the Board's requirements.

### 5.1 Within the CC

To develop the processes for the development components of the evaluation process to:

- Accommodate the development process for commercial (particularly business process) products;
- Permit a 7799 certification of the development process to be considered particularly for smaller developers.

To enhance the commercial value of the products evaluated by including components, which address commercial security requirements over and above those presently included. Consider evaluation of products being used in the automation of the business process. Possibly also to consider developing mechanisms whereby processes embedded in business process applications could be confirmed as being compliant with applicable laws and regulations.

### 5.2 Within the 7799 family

Ensure that the linkage between Information Security and the other parts of the Internal Control system is made explicit in the guidance provided. In general this could be achieved by developing guidance:

- To explain how IT risk fits in with the overall business risk;
- How business process security can be effected particularly in the area of the 'correctness' of the results presented to management and stakeholders.

To explore possible metrics which would enable people to evaluate better the quality of the ISMS.

## 6. CONCLUSION

In the future more and more of the business and home process will be automated. It is vital that these processes are secure and deliver correct information to the users of the systems.

Our present set of standards grew out of the needs of the large mainframe systems and need to be changed to reflect the reality of the systems of the future. In the security world we need a debate about what changes are required so that those charged with delivering security in the future have the tools they really need to do a first class job.

This paper has set out briefly the current major ISO standards and has made some suggestions as how they might be changed for the future.