Information Security Governance using ISO 17799 and COBIT

Elmari Pretorius

KPMG, Rand Afrikaans University – Johannesburg, South Africa

Prof. Basie von Solms

Rand Afrikaans University – Johannesburg, South Africa

Abstract: This paper discusses a project in which a mapping between ISO 17799 and COBIT's section DS 5 is being created. The purpose of this mapping is to synchronize these two documents to a certain extent, to make it easier to use both in an integrated way for information security governance and management.

Key words: ISO 17799, COBIT, Information Security Management, Information Security Governance

1. INTRODUCTION

In the last few years, Information Security had been moving very strongly towards the use of documents and guidelines based on so called Best Practices, Open Standards and Codes of Practice for governing and managing information security.

This can be seen as a very positive move, as it shows that a certain amount of maturity is being established in these areas.

Two documents that are playing an increasing role in this aspect are the ISO/IEC 17799 Code of Practice for Information Security Management, and Control Objectives for Information and related Technology, better known as COBIT. Section DS 5 of COBIT relates specifically to information security.

In many cases ISO 17799 is being used within IT departments as a guide for information security management, while COBIT DS 5 is used more by auditors for information security auditing. Furthermore, COBIT is raising its profile as an IT governance tool, and not only as an auditing tool.

In its role as an IT governance tool, COBIT can therefore be seen as being used on a strategic level, indicating the 'what' as far as governance is concerned. On the other hand, ISO 17799 can be seen more as being used on a lower level, specifying the 'how' as far as information security management is concerned.

Because of the wider use of these 2 documents (ISO 17799 and COBIT DS5), in many cases a need for synchronization between these two documents arise, in the sense that a mapping between the detailed control objectives of DS5 and the counter measures introduced by 17799, are beneficial.

This makes it easier in using COBIT DS5 for Information Security Governance and auditing, and implementing lower level counter measures based on ISO 17799.

Such a mapping will indicate which DS 5 detailed control objectives are mapped to which ISO 17799 controls, and vice versa.

Another angle that can prove to be beneficial for Information Security management and governance is a mapping of a company's Information Security policy to either ISO 17799 or COBIT DS5, or both. Such a mapping will indicate "compliance" areas within the policy document, and also highlight the "non-compliance" areas, and assist with the alignment of a company's IS policy to the ISO and COBIT frameworks.

This project will result in a database containing the mapping of ISO 17799 to COBIT, COBIT to ISO 17799, and a test case of a company Information Security mapping to the ISO and COBIT documents. A user interface will allow access from either the ISO 17799 side, or from the COBIT DS 5 side.

The purpose of this paper is to discuss these mappings, and to give an example of some of the results.

2. WHAT IS ISO 17799

ISO 17799 can be regarded as a comprehensive catalogue of "the best things to do in Information Security". Because it is a code, it is made up of best practice recommendations, which can be applied to fit each organisation's specific requirements.

Since ISO 17799 sets out the requirements for an Information Security Management System (ISMS), it helps to identify, reduce and manage the wide spectrum of threats to which information is commonly subjected.

ISO 17799 is organised into ten major domains, each covering a different topic or area. These domains are:

- Security policy;
- Organising information security;
- Asset classification;
- Personnel security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Systems development and maintenance;
- Business Continuity Management; and
- Compliance.

Each of these domains is divided into security control areas that can be applied to improve an organisation's information security. Each control area then has its own objective, and one or more controls to assist in achieving this objective.

ISO 17799's biggest exposure is to the IS manager. IT departments often use it as a foundation to build its Information security environment on.

3. WHAT IS COBIT?

The keystone of the COBIT framework is that control in IT is approached by looking at information as being the result of the combined application of IT related resources that need to be managed by IT processes, and by looking at information that is needed to support the business objectives or requirements.

COBIT presents IT activities in a manageable and logical structure and documents good practice across this structure. COBIT's good practices will help optimise information investments and provide a benchmark to be measured against when things go wrong.

COBIT's structure groups IT process into four broad groups:

1 Planning and organisation;

2 Acquisition and Implementation;

3 Delivery and Support; and

4 Monitoring.

It then defines high-level Business control objectives for these processes, and supports these with Detailed control objectives.

COBIT's biggest exposure is to the IS auditor (IA). Management and IA's often use it as a foundation to build IT audits on.

4. INFORMATION SECURITY POLICIES

The information security policy document is considered to be a control that is common best practice in any information security environment. This policy as a control, applies to most organisations and in most environments, and can provide a good starting point for implementing effective and efficient information security management.

An information security policy provides management with direction and support for information security management in accordance with the organisation's business objectives and requirements, and the relevant regulatory and legislative information.

To be effective an information security policy should be effectively communicated to all relevant personnel, and guidance on compliance to the policy should be provided.

It is crucial for an organisation to adopt a structured framework for policy definition, using a process that enables policies to be derived from the organisation's business requirements.

Failure to develop a meaningful information security policy, or developing a policy that does not cover all risks posed to the organisation in the information security environment, could expose the organisation to potentially catastrophic breaches. From this it is important to ensure that all risk areas within the information security environment, applicable to the specific organisation, is mitigated by an effective and comprehensive information security policy.

5. USING THE MAPPING

It is envisaged that the resultant database (mapping) can be used for different purposes.

5.1 Suppose the IT Department of Company X has based their information security policy and counter measures on ISO 17799. The Information Security Manager now wants to see which DS 5 detailed control objectives are covered by the ISO 17799 counter measures he/she had installed or implemented. The mapping will immediately provide an answer.

5.2 An internal auditor of Company X wants to audit the company's IT Department's information security using DS 5. The auditor can now, using the mapping, see which of the detailed control objectives specified in DS 5 are implemented through ISO 17799, used by the Department.

Both these uses basically allow IT people, using ISO 17799, and auditors, using DS 5, to 'speak the same language' and compare apples with apples.

Maybe it will even allow IT people and internal auditors to become friends!

6. MAPPING EXAMPLE: ACCESS CONTROL MAP

The following is an example of the proposed mapping. This example covers Access control as an objective, and was mapped from ISO to COBIT.

6.1 Objectives covered by both ISO and COBIT

6.1.1 Business requirements for access control (Section 10.1 of ISO 17799)

ISO objective: Control access to information. Access to information and business process should be controlled on the basis of business **and** security req.

ISO control: 10.1.1 ACCESS CONTROL POLICY: Business requirements for access control should be defined and documented.

Link to COBIT control objective: 5.2 Identification, Authentication and Access

Motivation for link between ISO and COBIT: Both ISO's and COBIT's controls and objectives for access control state that specific procedures need to be in place and that these procedures must be documented, in order to keep access mechanisms effective.

6.2 Objectives only covered by ISO

6.2.1 Network access control (Section 10.4 of ISO 17799)

ISO objective: Protection of networked services. Access to both internal and external networked services should be controlled

ISO control: 10.4.8 NETWORK ROUTING CONTROL: For shared networks, routing controls should be implemented to ensure that computer connections and information flows do not breach the access control policy of the business applications.

Link to COBIT control objective: No apparent link to COBIT

Motivation for link between ISO and COBIT: COBIT deals with access control in a broad manner, and although it seems that it's access control objectives cover all areas of access, it does not have a control objective specific to network access control.

6.3 Objectives only covered by COBIT

6.3.1 Firewall architecture and connections with public networks

COBIT objective: Adequate firewalls should be operative to protect against denial of service attacks and any unauthorised access to internal resources

COBIT control: Firewalls

Link to ISO control objective: No apparent link to ISO

Motivation for above link between ISO and COBIT: ISO doesn't have a specific objective referring to firewalls and the use of it, while COBIT has a specific control objective dedicated only to firewalls.

7. CONCLUSION

Besides synchronising the two frameworks, the use of the mapping will also reduce confusion and deviations that exist between IT and Audit. The fact that the mapping can provide IT and Audit with the links at the touch of a button, means that a lot of time can be saved when auditing and setting up the Information Security environment. In addition the "IS policy alignment tool" can prove to be beneficial in the drafting and reviewing of a company's policy with regards to the ISO 17799 and COBIT DS5 frameworks.

REFERENCES

1. ISO / IEC 17799:"Code of Practice for Information Security Management"
2. COBIT - Audit Guidelines, 3rd edition