Computers & Security (2005) **24**, 99—104

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

Information Security governance: COBIT or ISO 17799 or both?

Basie von Solms*

Academy for Information Technology, University of Johannesburg, Johannesburg, South Africa

KEYWORDS
COBIT;
ISO 17799;
Information Technology governance;
Information Security governance;
Information Security;
Risk management;
Corporate governance;
IT audit

Abstract This paper investigates the co-existence of and complementary use of COBIT and ISO 17799 as reference frameworks for Information Security governance. The investigation is based on a mapping between COBIT and ISO 17799 which became available in 2004, and provides a level of 'synchronization' between these two frameworks.

Introduction

Information Security governance has become an established and recognized component of Corporate Governance, and specifically Information Technology governance,

'Corporate Governance consists of the set of policies and internal controls by which organizations, irrespective of size or form, are directed and managed. Information security governance is a subset of organizations' overall (corporate) governance program' (Information Security Governance — A Call to Action).

This realization is causing many companies world wide to establish environments for Information Security governance.

In this process of establishing such environments for Information Security governance, companies are realizing that is it preferable to follow some type of internationally recognized reference framework for establishing such an Information Security governance environment, rather than doing it ad hoc. There are several possible reference frameworks which can be used, and it is

* Tel.: +41 504 3604; fax: +41 504 9604.
E-mail address: basie@rau.ac.za

0167-4048/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2005.02.002

therefore prudent for such a company to evaluate and choose one or more.

The question companies are asking, is therefore: 'What is the best reference framework for an Information Security governance environment for our company?'

It is not the purpose of this paper to evaluate the different options, but rather to discuss two such possible frameworks, and investigate whether they can be used together as frameworks for Information Security governance, and whether there is any synergy in using them together.

The two options which will be investigated are COBIT (2000) and ISO 17799 (ISO/IEC 17799, 2000).

This paper will not compare these two options, but will rather reason that these two frameworks are complementary, and are actually very good choices as reference frameworks for Information Security governance. Used together, they provide a synergy which can be very beneficial to companies.

In next section, we will give a brief overview of COBIT, which will be followed by the section that will discuss the same for ISO 17799.

Then, we will discuss why they are complementary, and good to use together, followed by discussion on the mapping between these two frameworks.

Further, we will illustrate some scenarios where it can be very beneficial to use these two frameworks together to provide a comprehensive Information Security governance environment.

We will end with a summary in the last section.

The pros and cons of using COBIT for Information Security governance

COBIT positions itself as 'the tool for information technology governance' (COBIT, 2000). COBIT is therefore not exclusive to information security — it addresses Information Technology governance, and refers amongst many other issues, to information security.

COBIT divides Information Technology governance into 34 processes, and provides a high level Control Objective (CO) for each of these 34 processes.

Each CO is again divided into a set of Detailed Control Objectives (DCOs), which specify the way the high level CO must be managed, in more detail. In total, 316 DCOs are defined for the 34 processes. The rationale is that if each of these 34 processes is managed properly, proper Information Technology governance will result.

One of these 34 processes is DS 5, 'Ensure System Security'. The CO for this process is divided into 21 DCOs, e.g.

- DS 5.1 manage security measures,
- DS 5.2 identification, authentication and access,
- etc.

However, these 21 DCOs are not the only amongst 316 which are relevant to the Information Security governance. Within many of the other 33 processes are DCOs which are also related to Information Security governance — maybe a little more indirectly than the 21 of DS 5, but nevertheless important to Information Security governance.

The upside of using COBIT as an Information Security governance framework is that information security is 'integrated' into a larger or wider Information Technology governance framework, provided by the other 33 processes. Even if COBIT is used only for Information Security governance, it still provides the rest of the framework if the company later decides to base the rest of its Information Technology governance also on COBIT. The then existing Information Security governance framework will then fit seamlessly into the wider framework defined by COBIT.

The downside of using COBIT for Information Security governance is that it is not always very detailed in terms of 'how' to do certain things. The DCOs are more addressed to the 'what' must be done. In most cases some more detailed guideline for detailing precisely 'how' things must be done, will be needed.

Because of COBIT's history as being used by IT auditors, COBIT is in many cases preferred by IT auditors and IT Risk Managers as a framework of choice.

The pros and cons of using ISO 17799 for Information Security governance

ISO 17799 is exclusive to information security, and only addresses that issue.

ISO is divided into 10 sections, with 36 objectives. Each objective is again divided into sub-objectives.

The upside of using ISO 17799 for Information Security governance is that it is more detailed than COBIT, and provides much more guidance on precisely 'how' things must be done.

It will e.g. give guidance on what an Information Security Policy should look like in terms of structure and content.

Because of this more detailed, and maybe more 'technical' orientation of ISO 17799, it is in many

cases the framework of choice of IT managers and Information Security Managers.

The downside of using ISO for ISO 17799, is that it is very much a 'stand alone' guidance, not integrated into a wider framework for Information Technology governance.

Using both COBIT and ISO 17799 for Information Security governance

As indicated above, the upside of using COBIT is that COBIT positions Information Security governance within a wider Information Technology Governance framework, which is good because it provides an integrated platform (architecture/structure) for wider Information Technology governance.

The downside, however, is that the Information Security governance component of COBIT provides good guidance on the 'what' of Information Security governance, but is not very detailed as far as the 'how' is concerned.

The upside of ISO 17799, on the other hand is that it is much more detailed, providing much more direct guidelines on the 'how'. The downside is, however, that it is 'stand alone', and does not provide the wider platform provided by COBIT.

It therefore seems logical that to get the benefits of both the wider reference and integrated platform provided by COBIT, and the more detailed guidelines provided by ISO 17799, there can be a lot of benefit in using both together for Information Security governance.

The synergy of combing these two frameworks can be substantial.

To a certain extent these two frameworks naturally complement each other.

Use COBIT as a 'high' level reference framework in which Information Security governance is well positioned, and the 'what' is quite clear, and use ISO 17799 as a 'lower' leveled guideline specifically for InfSec in which the 'how' is more detailed.

In taking this (very good) decision, the problem is to determine how to integrate them — i.e. which DCOs of COBIT map to which elements of ISO 17799 and vica versa.

If this problem is not solved, it stays very difficult to provide a consistent reference framework, because of possible unclarity between which COBIT DCOs represent which ISO 17799 objectives and sub-objectives, and vica versa. It is like comparing apples with pears.

This unclarity, and often disagreement, will arise e.g. where the Risk Management Department (RMD) wants to use COBIT for wider Information Technology governance, and expects the Information Security Department (ITD) to accept that. However, the Information Security Department may have already decided to use ISO 17799, and is unwilling, and unhappy to change, especially if the RMD cannot inform the ISD which of the ISO 17799 controls they have already implemented, satisfy which COBIT DCOs required by the RMD. This situation is quite common, in that COBIT is generally preferred by the more 'non-technical' role players as far as information security is concerned (Risk Managers, auditors, etc.), while ISO 17799 is generally preferred by the more technical role players (InfSec Managers, Network Security Managers, etc.).

If this problem can be solved by 'building a bridge' between COBIT and ISO 17799, much 'richer' Information Technology governance and Information Security governance environments can be created, satisfying both the RMD and the ISD, and most probably also the Auditing Department who may be doing their auditing based on COBIT.

A very recent report by the IT Governance Institute solves precisely this problem, by providing a detailed mapping between COBIT's DCOs and ISO 17799 (COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT). This report will be discussed in more detail in the next section.

The implication of this mapping, and the subsequent richer complementary existence of COBIT and ISO 17799 will be discussed in section 'The complementary use of COBIT and ISO 17799 for Information Security governance'.

A mapping between COBIT and ISO 17799

In COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT, a detailed mapping between COBIT and ISO 17799 is provided.

Every COBIT DCO is investigated, and the corresponding, if any, ISO 17799 objectives and/or sub-objectives are indicated.

This clears up the unclarity referred to in the previous section.

Some examples are (quoted directly from COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT) as follows.

Example 1 (p. 99)

DS 5.3 security of online access to data

- COBIT DCO: In an online IT environment, IT management should implement procedures in line with the security policy that provides access security control based on the individual's demonstrated need to view, add, change or delete data.

ISO 17799 requirements (sub-objectives)

- Physical and logical access should be controlled (4.2.1.1).
- Access to data should be limited to authorized users and adequate protection should be implemented in application systems. Operating system software and other utility programs that could provide online access to data should be protected (9.6).

(The numbers in brackets indicate the specific clause in ISO 17799).

Example 2 (p. 100)

DS 5.6 user control of user accounts

- COBIT DCO: Users should systematically control the activity of their proper account(s). Information mechanisms should be in place to allow them to oversee normal activity as well as to be alerted to unusual activity in a timely manner.

ISO 17799 requirements (sub-objectives)

- Users should be aware of their responsibilities for maintaining access controls (9.3).
- Information regarding the previous logon (successful and unsuccessful) should be provided after successful logon (9.5.2).

Not all COBIT DCOs are necessarily mapped onto two ISO sub-objectives (bullet points) as in the two examples above.

COBIT DS 5.4 (User Account Management) is mapped to 13 different ISO 17799 sub-objectives.

By using this mapping documented in COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT, COBIT's Information Security governance requirements can now be closely linked and integrated with that of ISO 17799.

Unfortunately the mapping is only one directional, from COBIT to ISO 17799, and does not provide a mapping from ISO 17799 back to COBIT. Such a mapping would have been useful, but can be quite easily retraced from the provided mapping.

A formal ISO 17799 to COBIT mapping, based on COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT, is presently being formalized (COBIT/ISO Mapping, 2005). This project will provide an automated tool implementing a bi-directional mapping between COBIT and ISO 17799, based on COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT.

The RMD referred to above, can now implement their Information Security governance program based on COBIT's information security related DCOs, and can then precisely indicate to the ISD how these requirements map onto the control measures, based on ISO 17799, implemented by the ISD. Such an approach was always possible, but the lack of an 'official' mapping tended to cause disagreements between involved parties.

The mapping offered in COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT, does not only map the 21 DCOs of the high level Control Objective DS 5 of 'Ensuring System Security' to ISO 17799, but actually provides a mapping for all 316, of which some are of course empty. This indicates that ISO 17799 is 'wider' and more comprehensive than only DS 5 of COBIT, and again illustrates the absolute integration of Information Security governance in Information Technology governance.

Example 3 (p. 78)

AI 4.2 user procedures manual

- COBIT DCO: The organization's system development life cycle methodology should provide for the preparation and refreshment of adequate user procedures manuals as part of every information system development, implementation or modification project.

ISO 1799 requirement (sub-objective)

- Operating procedures and instructions for job execution should be documented (8.1.1).

Example 4 (p. 60)

PO 10.12 training plan

- COBIT DCO: The organization's project management framework should require that a training plan be created for every development, implementation and modification project.

ISO 17799 requirement (sub-objective)

- Not addressed in ISO 17799.

This mapping allows us now to compare apples with apples!

The way in which Information Security governance environments can be synchronized based on the mapping and the discussion above, will be discussed in the next section.

The complementary use of COBIT and ISO 17799 for Information Security governance

In this section we will discuss a number of scenarios where such complementary use of COBIT and ISO 177 can be very beneficial.

Scenario 1

Suppose the company does not have a comprehensive Information Technology governance plan, but the Information Security Department (ISD) had been proactive, and had started using ISO 17799 as an information security management guideline.

The Risk Management Department (RMD), or the Audit Department, or someone else, now decides to use COBIT as an enterprise wide IT Governance framework, and expects the ISD to follow suit.

The benefit of the complementary approach discussed above, is that the ISD does not have to change anything — using the mapping, they can now immediately inform the RMD or other, precisely which DCOs from COBIT have been implemented through ISO 17799. The RMD can carry on and create their enterprise wide plan with the knowledge that they know where Information Security governance fits in, and what has already been done.

Scenario 2

Suppose, as above, that the Information Security Department (ISD) had been proactive, and had started using ISO 17799 as an information security management guideline.

An IT audit is scheduled, and the auditors (internal or external) will be using COBIT as their IT audit framework.

Without the complementary approach discussed above, and without using the mapping, serious disagreement between the auditors and the ISD can arise, because of apples being compared with pears, or existing apples expected to be pears, even though they actually are apples, but just look like pears!

This scenario is not uncommon from the author's experience.

Using the mapping, the auditors can, from the beginning inform the ISD which ISO 17799 objectives and sub-objectives-driven control measures they will expect to be in place. The ISD also knows what they are in for.

Apples are compared with apples!

Scenario 3

The company had implemented an enterprise wide IT governance framework based on COBIT, and the ISD had subsequently also based their governance plan on the some COBIT DCOs (probably DS 5 and some more).

The ISD now decides to use ISO 17799, maybe because of its more detailed contents, or maybe because the company has decided to get officially certificated against ISO 17799, or for whatever reason.

Using the mapping, the ISD can now easily determine which of the ISO 17799 objectives and sub-objectives are already satisfied through their use of COBIT, and which must still be given attention.

Again a seamless move is possible.

Several more similar type of scenarios are possible, but those discussed above clearly makes the point.

Scenario 4

Company A, having an IT governance framework based on COBIT, takes over company B, who has an Information Security governance framework based on ISO 17799.

The benefit in the complementary approach, made possible by the mapping (COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT), should be clear.

Summary

The appearance of the mapping (COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT) has been timely, and will definitely help to make the very useful content provided by COBIT and the very useful content provided by ISO 17799, much more useful in implementing comprehensive and standardized Information Security governance environments.

References

An automated COBIT/ISO mapping. Masters project at the University of Johannesburg; 2005, <http://basie@rau.ac.za>.

COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT. USA: IT Governance Institute, <http://www.itgi.org>.

Control objectives for information and related technologies (COBIT). 3rd ed. USA: IT Governance Institute; 2000.
Information Security Governance — a call to action. National Cyber Security Summit Task Force, <http://www.technet.org/resources/InfoSecGov4_04.pdf>.
ISO/IEC 17799, Information technology — code of practice for information security management. Switzerland: International Organization for Standardization (ISO); 2000.

Prof SH (Basie) von Solms holds a PhD in Computer Science, and is the Head of Department of the Academy for Information Technology at the University of Johannesburg in Johannesburg, South Africa.

He has been lecturing in Computer Science and IT related fields since 1970.

Prof von Solms is specializes in research and consultancy in the area of Information Security. He has written more than 90 papers on this aspect — most of which were published internationally. Prof. S. H. von Solms also supervised more than 15 Ph. D. students and more than 45 Master students.

Prof von Solms is the present Vice-President of IFIP, the International Federation for Information Processing, and the immediate past Chairman of Technical Committee 11 (Information Security), of the IFIP. He is also a member of the General Assembly of IFIP.

He has given numerous papers, related to Information Security, at international conferences and is regularly invited to be a member of the Program Committees for international conferences.

Prof von Solms has been a consultant to industry on the subject of Information Security for the last 10 years.

He is a Member of the British Computer Society, a Fellow of the Computer Society of South Africa, and a SAATCA Certificated Auditor for ISO 17799, the international Code of Practice for Information Security Management.