Comparing different information security standards: COBIT vs. ISO 27001

Varun Arora
Carnegie Mellon University, Qatar
varora@qatar.cmu.edu

ABSTRACT
In this paper, the manager's dilemma of choosing a security standard's framework is identified and two popular standards are compared for overlap and differences.

Categories and Subject Descriptors
K.6.2 [**Management of Computing and Information Systems**]: Installation management – *benchmarks.*

K.6.1 [**Project and People Management**]: Project and people management – *Strategic information systems planning.*

General Terms
Management, Measurement, Performance, Security, Standardization

Keywords
Keywords are your own designated keywords.

1. INTRODUCTION

The management of information security, or information security governance, has become a cause for concern for management of large scale organizations only in the past decade. What was earlier considered a minor set of activities of the information systems (IS) department of such organizations is now being given adequate attention. Many organizations are realizing the need for hiring individuals and making small teams of professionals who focus on information security management. In other cases, risk management departments of these organizations are dedicating human resources for focusing on setting security standards – while working closely with the IS and IT departments in its implementation.

Nevertheless, according to Andrew Jaquith's article "Creating meaningful information security metrics", the investment of companies in information security has stalled significantly despite the golden period between 2002 and 2007. A security analyst might argue that this is due to the lack of ability of managers to identify the need to allocate big budgets to information security needs of the organization. On the other hand, it is known that decision makers in the management are on a crunch with budgets – and aren't fully convinced to spend much money in security. Sadly, and as Jaquith best puts it, "victories are taken for granted and go unnoticed, but failures are embarrassingly public" (Jaquith, 2010).

Despite the falling investment in security planning and implementation in organizations, the increasing realization of the management that there must be better focus on information security is causing them make decisions in favor of complying to certain set of international standards. There may be two simple reasons for this:

1. Industry globalization and need for being on the same platform with international competition in the view of clients demanding secure, reliable and integral data services
2. Many regulations require a risk-based approach to management of information security

These regulations are the key driving factor for organizations to plan for standards which set a series of benchmarks and allow organizations to design a schema of metrics to compare against these benchmarks.

2. INFORMATION SECURITY STANDARDS

The frameworks of standards on information systems management may conveniently be broken down into the following two groups:

- Information Security standards
- IS Governance standards

Examples of standards focusing solely on security include ISO 27000 series (earlier known as ISO/IEC 17799), NIST 800 series, SOX, ISF SOGP, Risk IT, etc. Popular IT governance/service quality standards include COBIT, COSO, ITIL, etc.

Clearly, these two groups of standards aren't mutually exclusive of each other. Some of the popular IT governance and management frameworks such COBIT have tried to encompass aspects of security, but haven't gone into much depth. Basie von Solms (2005), in his paper "Information Security governance: COBIT or ISO 17799 or both?", notes that COBIT lays down good guidance on what needs to be implemented in terms of information security measures, but doesn't really elaborate on how this needs to be done. In the same way, many of the standards' frameworks which focus primarily on information security governance do not provide adequate knowledge/guidance on how these security measures fit into a larger framework of IS Management and processes.

Choosing the correct framework of standards for IS governance and information security and compliance with best industry practices has become the new dilemma of managers doing long-term planning for IS in large organizations. The large number of promising frameworks pose a fairly difficult challenge to managers in terms of the choice they offer. As mentioned previously, no single standards framework is a completely exhaustive option – and so, a manager is expected to examine a number of standards' frameworks and analyze what suits his needs before he/she decides to begin the process of working on processes, mechanisms and quality. Also, he/she needs to consider if the set of standards he/she chooses has adequate focus on information security or is there a need to go beyond and extend his framework to a hybrid of more standards.

In the following sections, two of the most popularly implemented frameworks, COBIT and ISO 27000 series are compared in their scope applicability, and it is concluded by basic suggestions on their use in organizations.

3. COBIT or ISO 27001?

In trying to understand whether an organization should implement any of these two frameworks, we must realize that while COBIT and ISO 27001 are different in many aspects, they do have some overlap and similarities. It is a particularly difficult decision for the manager, as he/she is required to deeply read through and understand which objectives are similar but worded differently in the two frameworks, and which objectives, that may look very identical in their scope, and vastly different due a minor difference in wording the objective.

As it turns out, there is more than just the above mentioned factor for an organization to choose a preferred framework. These include: alignment with the goals and objectives of the organization, relationships with other organizations following common standards, ability to accomplish objectives with existing infrastructure and smaller budgets, risk-assessment and risk-management, training of employees, and many more.

3.1 COBIT

COBIT is a high-level IT governance and management framework. It focuses on the broader decisions in IT management and does not dwell into technical details. It is a framework of best practices in managing resources, infrastructure, processes, responsibilities, controls, etc.

COBIT contains 34 IT processes, each with high-level control objectives (COs) and a set of detailed control objectives (DCOs). In total, there is a sum of 318 DCOs defined for these processes.

It is a good solution when managers are looking for a framework which serves as an integrated solution within itself, rather than having to be implemented along with other IT governance frameworks.

However, its biggest short-coming is that it does not give “how-to” guidelines to accomplish the control objectives. This is not preferred when the thrust in on correct implementation of security controls.

3.2 ISO 27001

ISO 27000 series is a family of IS management standards. It is the set of standards in this family that focuses on Information Systems Management (ISM). Initially known as the BS7799 standard, this was included in the set of ISO standards when ISO decided to include ISMS standards as one of the set of ISO standards. As a result of this, the standards' name/number was adopted and it was called the ISO17799:2005 series.

To bring the Information Security Management Systems (ISMS) standard BS7799-2 in line with other IS standards, this standard was included in the ISO 27000 series as ISO 27001.

ISO 27001 defines methods and practices of implementing information security in organizations with detailed steps on how these implemented. They aim to provide reliable and secure communication and data exchange in organizations. Also, it stresses on a risk approach to accomplishing its objectives.

This standard dives deep into ways to implement its sub-objectives. This puts managers who are looking for clarifications on implementation, at an advantage. However, it fails to achieve the goal of integrating into a larger system. It is standalone in its nature, and does not work as a complete ISM solution.

Let us look into the how these two frameworks are different from each other in a number of areas:

	COBIT	ISO 27001
Focus	Business orientation and IT governance in its entirety	Implementation of security controls, stress on risk—management approach
Paradigm	Planning of IT Processes	Information security management system
Scope	Complete IT governance of organization, including security planning. It is an integrated solution.	Standalone guidance for security.
Structure	34 IT processes grouped in 4 domains: Plan and organize, Acquire and Implement, Deliver and support, Monitor	11 sections with 36 objectives which are further divided into sub-objectives
Organizational model	All stakeholders	Management, IS departments
Certification	Is not certifiable for organizations	Is certifiable

3.3 Mapping COBIT to ISO 27001

As seen above, neither COBIT nor ISO 27001 provides a complete integrated IT governance framework with well documented security guidance, when considered along. Managers looking to have such a solution do not have to compromise on anything, as these frameworks may not be used in isolation from each other.

A number of papers have identified a clear mapping between individual detailed objectives of each of these frameworks. In fact, there are very few objectives that do not have a clear mapping with the other standard. A comprehensive list of mapping can be seen in the following resources:

- COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT [1]
- 08-02 Control mapping (NIST 800-53 vs. ISO 17799 vs. COBIT 4.1) [6]
- Aligning COBIT, ITIL and ISO 17799 for Business Benefit: Management Summary [3]

This clear mapping between the themes of the sub-objectives and controls of COBIT and ISO 27001 might make us believe that the objectives in both these standards are comprised of the same security instructions and guidance. However, it is interesting to note that although the themes are the same, there are minor differences in the implementation requirements which drastically affect the planning and budgeting for implementing these standards.

Here is an example (without clear reference to the document sections or objectives):

There are objectives in both documents to protect data and back them up at frequent intervals. However, these are additional requirements in ISO 27001 which requires special attention. Apart from what is required in COBIT, this objective requires the organization to maintain off-site backups. This requires significantly larger investments and effort on the part of the organization.

Thus, a manager is expected to carefully understand all the objectives of the two documents despite having a clear representation of their mappings – as this will enable him/her to make a better decision on using these frameworks, in case he/she feels the need to use these in complement to each other.

4. COBIT 5

There has been a new advancement in the COBIT standard. COBIT has released a draft document of their newest revision of COBIT. It is called COBIT 5 and is known to have expanded a lot more on security objectives and how an organization can achieve them.

5. ACKNOWLEDGMENTS

Sincere thanks to Dr. Daniel Phelps, Assistant Teaching Professor, Carnegie Mellon University for his guidance. Also, thanks to Omar Sherin, Q-CERT, ictQatar for his valuable time and assistance.

6. REFERENCES

[1] IT Governance Institute, "Overview of International IT Guidance." *COBIT Mapping* 2 (2006): 8-15, 20-31. Print.

[2] vln Solms, Basie. "Information Security governance: COBIT or ISO 17799 or both?." *Computers and Security* 24 (2005): 99-104. Print.

[3] "Aligning COBIT, ITIL and ISO 17799 for Business Benefit: Management Summary." *IT Governance Institute* 1 (2005): 5-62. Print.

[4] Jaquith, Andrew. "Creating meaningful information security metrics." *Information Security Magazine* 1 Mar. 2010: -. Print.

[5] Aylward, Anton J. "COBIT for ISO270001 Users | Concepts, Myths and Misconceptions." The Fourth Canadian ISO 17799/ISO 27001 Conference. Systems Integrity, Toronto. Toronto. 30 Nov. 2006. Lecture.

[6] "08-02 Control mapping (NIST 800-53 vs ISO 17799 vs COBIT 4.1)." *Open Security Architecture*. N.p., n.d. Web. 28 Mar. 2010. <http://www.opensecurityarchitecture.org/cms/library/08_02_control-catalogue/256-08-02-control-mapping>.

[7] "Mapping COBIT 4.1, ISO 27002 : 2005 and NIST SP 800-53 Rev 2 | SAIJE Thoughts." *SAIJE THOUGHTS*. N.p., n.d. Web. 28 Mar. 2010. <http://blog.saije.net/2008/01/23/must-ado-about-mapping/>.

[8] "ISO 27000 - An Introduction to ISO 27001 / ISO27001." *ISO 27000 - ISO 27001 and ISO 27002 Standards*. N.p., n.d. Web. 28 Mar. 2010. <http://www.27000.org/iso-27001.htm>.