

# **IT Governance, Information Trust, and Risk Management**

**IT security and risk management: ISO 17799**  
Madina Nurguzhina

Spring 2007

## Table of contents

<b>1. Introduction</b>	<b>3</b>
<b>2. COBIT versus ISO 17799 in IT Governance</b>	<b>5</b>
<b>2.1. COBIT 4.0</b>	<b>6</b>
<b>2.2. ISO 17799</b>	<b>8</b>
<b>3. Implementation of ISO 17799</b>	<b>11</b>
<b>3.1. ISO 17799's implementation example</b>	<b>12</b>
<b>3.2. Benefits of ISO17799</b>	<b>15</b>
<b>4. Conclusion</b>	<b>17</b>
<b>Reference</b>	<b>18</b>

## **1. Introduction**

In order to be compliant with current laws and regulations, to be competitive and successful a company in the big world must consider not only such things as profit, personnel, supply chain management, and so on, but also information technologies that play a very high role in aforementioned processes. Information is a very important element of every process within a company. If a company can successfully protect and manage information, it would contribute a lot into its business purposes as a whole.

In the global community there are many different types of standards and frameworks that help a company to manage and secure IT such as COSO, COBIT, ISO, ITIL and many others. In order to have a strong and sound IT governance, a company has to implement appropriate IT frameworks that would fit a company's main processes.

COSO is a very broad group of standards that includes different financial and auditing institutions' functions, while COBIT, ISO and ITIL are more specific and focuses more on IT security and risk management. As a part of my individual project, I want to narrow my search to COBIT and ISO standards. ISO standards are used globally more often than COBIT due to the fact that ISO fits more smoothly into different frameworks of most of the countries in terms of business processes since COBIT addresses standards only, while ISO concerns about both standards and processes (e.g. organizational security, personnel security, communications and operations management, business continuity management, and so on). I will show it in my report supporting my ideas with relevant cases and examples from certain companies.

Let us talk a little bit about COSO (the Committee of Sponsoring Organizations of the Treadway Commission) and its role in IT Governance. As was mentioned earlier COSO is a very broad set of standards (to be precise a private sector organization) that focuses not only on IT

Governance control and improvement, but also and mostly focuses on financial reporting' quality, internal control and corporate governance. This organization was formed in order to find out factors that lead to frauds in financial reporting as well as give recommendations how to prevent these factors for companies, auditors, educational institutions and so on. Among sponsoring organizations within the Committee there are "five major professional associations in the United States, the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the Institute of Internal Auditors, and the National Association of Accountants (now the Institute of Management Accountants)" (1). In spite of the fact that there is a sponsorship deal, the Commission is independent from all of the sponsoring organizations, and has representatives from industry, public accounting, the New York Stock Exchange, and different investment firms.

COSO defines Internal Control as "a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives" in such categories as effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations. IT Governance is part of internal control within the COSO framework. Therefore, different frameworks for IT security and management (COBIT, ITIL, ISO, and so on) should comply with COSO organization's rules and requirements. While COSO is generally accepted as the internal control framework for enterprises, COBIT, ISO and other similar frameworks are the generally accepted internal control frameworks for IT.

## **2. COBIT versus ISO 17799 in IT Governance**

Why information technologies are so important in business world? Why so many organizations care about IT Governance and spend so much money for IT frameworks' implementation in order to be compliant with different laws and regulations? In some companies information technology is the most valuable resource since it protects their assets from being harmed, it reduces risks of frauds either financial or informational, and it improves whole governance system in order to detect and prevent those risks and problems in future. Many business processes depend heavily on information technologies. Therefore, each company no matter how large it is has to take care of its IT security, and manage IT in such a way that every process within a company would run properly and smoothly not affecting the bottom line.

IT Governance is management's responsibility when the board of directors and managers must determine objectives of company's strategy, and try to install certain IT frameworks to fit this strategy and lead to a better position in business world.

As already has been mentioned there are many IT frameworks such as COBIT, ITIL, ISO that include and institutionalize good practices to make sure that management uses IT that supports their business objectives. Each framework helps to take advantage of all information technologies within a company, controlling them more efficiently, maximizing their usefulness, and thus leading a company to a competitive advantage.

Managers have to optimize available IT resources, infrastructure and people clearly understanding what combination of resources and what IT framework would be better for their organization and then decide what control, improvement system, and governance would be more appropriate in current environment.

Before we concentrated only on managerial aspects of Information Security; however, technical aspects as well as human are needed to be considered on managerial level. You can see IT Governance from different points of views: from different governance policies, standards and guidelines, managerial aspects as well as from human perspective such as training, ethics, creating culture, and so on. Therefore, to establish a very strong security management system management should combine all the components in one system. Here we can use two approaches when security is driven from “process security” perspective when a company refers to different standards, policies, and managerial aspects, and from “product security” perspective when a company tries to use only certified products (4). According to these researchers, information security system consists of following components – “standards, procedures, management system audits, certification and accreditation, codes of practice, process security and product security, assurance, and culture, ethical, social and legal issues”.

## **2.1. COBIT 4.0**

There are many IT frameworks and standards that address aforementioned problems. One of such IT frameworks is *Control Objectives for Information and related Technology* (COBIT) that helps managers to create a controllable and smooth structure using best practices of COBIT. However, COBIT practices are mostly focused on control than on execution. COBIT framework helps managers to make IT resources successful in terms of achieving business objectives and put internal control framework in right place. COBIT has a very good way to identify what IT resources are needed for certain business objectives, and to define what control objectives are needed to be considered.

COBIT is represented by a model with 34 processes that take care of assessing, creating, observing and planning of IT resources. COBIT help IT and business managers presenting a model to understand the processes that work in IT environment, thus, helping them to understand each others' points and match each others' interests. COBIT's objectives are created in such a way that they fit IT process providing a framework that connects IT governance requirements, IT processes and controls with business aspects.

According to COBIT 4.0 there are three levels of COBIT products: Executive management and boards, Business and IT management, and Governance, assurance, control and security professionals. Executives are more interested in "Board Briefing on IT Governance, 2nd Edition" (created to help top managers understand why it is so important to manage and secure IT, and what should they do to make it better). Business and technology managers are more interested in "Management Guidelines" (how to assign responsibility, measure performance, and benchmark, what amount of work should be done in IT control, costs versus benefit, and so on). Governance, assurance, control and security professionals are interested in "Framework" (how IT governance objectives and best practices are organized by IT domains and processes, and how they related to business requirements), "Control objectives" (generic best practices for IT activities), "Control Practices" (why and how to implement controls), "IT Assurance Guide" (a generic audit approach and supporting guidance for audits of IT processes), "IT Control Objectives for Sarbanes-Oxley" (how to ensure that IT environment using COBIT complies with policies and laws), "IT Governance Implementation Guide" (a generic guide for implementing IT governance), "COBIT Quickstart™" (guidelines for the smaller organization and for the larger enterprise to start), and "COBIT Security Baseline™" (crucial steps for implementing IT

security). Hence, this COBIT structure helps all members of IT governance to reduce the gap between their areas of interests with respect to requirements.

But here it is very important to know how to measure certain risks in order to detect and prevent them quickly and efficiently, and how to secure available IT resources. If we know this we can measure how well a company achieves its chosen objectives as well as comply with business environment. According to COBIT 4.0 Executive Overview companies use certain tools to measure those things such as dashboards, scorecards, and benchmarking. However, all of the tools need in turn indicators, measures and a scale for comparison. Thus, each enterprise has to define what kind of indicators, measures and comparison scale it is more appeal to use. There are certain models for these processes that are generally used namely: “the Software Engineering Institute’s Capability Maturity Model, the principles of Robert Kaplan and David Norton’s balanced business scorecard”, and so on (6). After a company decides what measurement is more appropriate it can start to develop action plans in order to match with desired objective level.

## **2.2. ISO 17799**

To measure performance is very important for IT security and management. Performance measurement is supported both by ISO and COBIT, and shows how well IT processes are executed to meet business requirements. Since it is very hard to measure information technologies’ costs and risks, they are very important for IT Governance. If a company has a good way to measure performance, it is much easier to measure all risks and costs of IT.

Let us talk now about ISO and its way to measure performance. ISO17799 is an internationally recognized IT security Management Standard published by International Organization of Standardization in December 2000. Since these standards are international, it

enables ISO to be implemented in various types of enterprises. ISO 17799 defines information as an asset that is variable and valuable. That is why IT governance should find more appropriate way to protect this asset in order to minimize costs of damage, maximize profits, thus, enabling business continuity. ISO complies with the main principles of IT security that are confidentiality (to ensure that IT is used only by those who authorized for access to IT), integrity (to provide accurate and complete information and processing methods), and availability (to ensure access to IT for those who authorized when needed).

ISO17799 is based on the British Standard 7799 and addresses the following control areas:

- Security policy
- Organizational security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- System development and maintenance
- Business continuity management
- Compliance

ISO17799 compare to COBIT and other security standards not only covers IT security, but also tries to define risks and vulnerabilities, and offers ways to control information security disregarding its level and control methods. However, ISO17799 is not a technology guide since it does not provide practical aspects of technical nature security problems. In spite of this fact ISO17799 tries to be as broad as possible to fit most of organizations and applications. That is

one of the reasons of ISO wide acceptance in global society. For example, small and medium companies do not need to follow the full list of controls presented by ISO17799, but only crucial to current situation and environment. ISO also helps many companies to create their own specific IT environment guidance. ISO17799 contrary to COBIT can fit enterprises of different sizes.

Generally ISO17799 standards more fit to high to maximum security levels. But when it is needed to address lower security level, a small size enterprise still can adapt and modify standards to fit its environment and security level. Regarding costs and efforts that an enterprise should put while implementing ISO17799, they usually depend on organizational quality level that is when a company is not well organized, more efforts and costs would be needed compare to those that better organized. However, one of the ISO17799 advantages is that it using its baseline security approach enables an enterprise to increase security level using existing resources with no additional costs.

### **3. Implementation of ISO 17799**

In this part of report ISO17799 best practices will be shown from two perspectives: Entrust Inc. and Lucent Technologies Inc. which research provided us with great amount of advice and examples from practice when they implement ISO17799.

Here is a set of general steps that an enterprise takes while implementing ISO17799. As we can see from ISO framework, at the very beginning stage the company that wants to have strong IT Governance in order to prevent itself from risks, harms and vulnerabilities should provide its management with precise directions regarding support for information security. When management first tries to assess and design a new security policy that would be compliant with chosen framework, it starts with a policy document that needed to be communicated to all employees in order to deploy new security system within the company. However, it is not enough just to create this policy once. It is very important to keep it always appropriate with changing environment's rules and make all the employees to be updated with new released information. Also management should always seek for advice and relevant information from inside and outside specialists who have sound knowledge in this area.

After management updates information, assesses current situation and starts to design and implement new policy for the company, another phase is launched that is employees' education. First of all, employees should sign an agreement that states their responsibility for information security. Then education itself starts. Not only employees should receive training, but also not always though third party companies that have direct involvement within the company's procedures. As part of the training employees should respond and report very quickly on observed or suspected security problems. There should be created a certain mechanism of calculating volume, amount of risks and harm as well as costs of such problems.

As quality standards in ISO family of standards ISO17799 is based on the same philosophy of continuous improvement that is we can make some conclusions such as it is better and cheaper to prevent something to happen than observe, suspect and find problems, and then try to fix them. According to ISO9000 a company should create a sound mechanism of detection and prevention of such security problems. If problems occur, well-trained employees should take quick steps to fix them at the very same place. If this is impossible, they have to report to upper level employees and try to fix them again. After problems occur employees also should let know others about this in order to make everybody aware of such occurrence possibility and let them detect and prevent such problems as soon as possible in their work places.

### **3.1. ISO 17799's implementation example**

Since Entrust, Inc. is a company that provides solutions for secure identity management, secure messaging and secure data (5) to other companies helping them to reach more customers, partners and employees in more efficient way, it is worth to consider their opinion about IT security and management.

Entrust chose ISO 17799 because of its good mix of international acceptance level and full comprehensiveness as well as it was dedicated “solely for information security practices within a business as a whole including IT exclusive, and is built around policy and process” (7). Before choosing ISO17799 Entrust made a huge search of relevant literature and practices. Entrust also referred to COBIT and COSO; however, after all Entrust decided that COBIT’s “comprehensiveness can make implementation onerous” (7). Also, COBIT compare to ISO17799 focuses more on efficiency and effectiveness of IT environment (CIO audience) rather than information security that linked to business issues. COSO was considered good internal

control framework as well as COBIT, but with minimal guidance due to not being up-to-date enough for security environment applications.

Making analogy with ISO quality standards and their way of managing and improving Entrust made process of ISO17799 implementation as easy as possible. Analogically to quality manager, information security manager observes situation, gives regular assessments, and then recommendations for improvement, afterwards business managers determine to what issues investments should be put in as well as their priority.

As we know ISO17799 has 10 control areas each of what has subset elements. To provide performance measurement Entrust rated each element according to Red-Yellow-Green scale that is High-Medium/Moderate-Low/Acceptable level of Risk. After summarizing all elements in their groups (security practices) Entrust got following table (5):

<b>Information Security Management Report</b>			
<b>Security Practices</b>	<b>Risk Level</b>		
(based on ISO17799 chapters)	<b>R</b>	<b>Y</b>	<b>G</b>
Security Policy	0	1	1
Organizational Security	1	3	1
Asset Classification and Control	1	0	2
Personnel Security	1	4	4
Physical and Environmental Security	2	4	12
Communications and Operations Management	2	10	20
Access Control	4	12	14
System Development and Maintenance	0	2	11
Business Continuity Management	1	2	2
Compliance	2	5	3
<b>TOTAL (*sample numbers only)</b>	<b>14</b>	<b>43</b>	<b>70</b>

The table clearly and concisely shows all risk levels in each control area (a company should make deployed table including risk levels for all 127 subsets within each chapter), and helps Board of Directors, CEO, CIO and business unit managers to quickly overview whole picture of information security in an enterprise, identify priority of issues with higher risk levels. Afterwards an enterprise can observe the progress using the same reporting chart using continuous improvement principle.

In further steps Entrust made review within business groups. Here is a fragment of matrix “business groups-information systems” with only four information systems:

<b>Function</b>	<b>Network</b>	<b>Computers</b>	<b>E-mail</b>	<b>ERP</b>
<b>Sales</b>	M	M	M	L
<b>Marketing</b>	H	L	H	H
<b>Customer Support</b>	H	M	H	M
<b>Operations</b>	H	M	H	M
<b>Development</b>	H	M	M	M
<b>HR</b>	H	M	H	H
<b>IS/IT</b>	H	M	H	H
<b>Professional Services</b>	M	L	M	M

This matrix shows an impact of a failure of main principles of Confidentiality, Integrity, and Availability for each system within each business group. For example, “H” in Marketing department–ERP system crossing in the matrix means that Marketing function would be seriously affected by a failure in ERP security system. Likewise, computers’ security failure would have lower impact on the same Marketing function.

There is also another lesson in measuring risk. Entrust offered a formula to describe a risk in a format that would be understood by everyone within a company:

### **Vulnerability x Threat x Impact**

They explained this formula using following example: “Inconsistent account disabling procedures [**vulnerability**] could allow a disgruntled ex-employee access to confidential information that could be deleted, modified or stolen [**threat**] resulting in lost productivity, erroneous reporting or loss of intellectual property [**impact**].”

As we can see this method of describing risk can be easily understood by stakeholders, thus, being more useful for IT governance.

These examples from Entrust company could be very good advice for those who want to implement Information security governance in their enterprises.

### **3.2. Benefits of ISO17799**

Another company Lucent Technologies provided their benefits of using ISO17799. Considering three main principles of confidentiality, integrity, and availability, as well as ISO’s best practices and guidelines to prevent and detect risks as soon as possible, from Lucent Technologies Inc. implementation experience ISO17799 offers a benchmark that helps to design strong information security as well as mechanism to manage security process. Therefore, ISO17799 is a comprehensive, broad information security process that gives enterprises benefits such as:

- An internationally recognized and well structured group of methods;
- A defined process to evaluate, implement, maintain, and manage information security;

- A set of policies, standards, procedures, and guidelines that well match with most of applications;

- Certification allows organizations to show their own security level as well as compare it with their trading partners' and competitors' information security level;

- Certification shows “due diligence” (3)

Also from Lucent Technologies Inc. perspective ISO17799 can be mandatory for those who require high level of assurance as well as non-mandatory, but a very useful marketing tool in terms of competition.

#### **4. Conclusion**

In this report it was shown how important to implement information security governance, as well as advantages of ISO17799 over other frameworks. COBIT is a good framework for assessing, managing and reducing IT business risks, but it lacks implementation details, while ISO17799 has them. However, each of frameworks has their own weaknesses and strengthens; e.g. ISO17799 has a complete level of security, but does not contain product-oriented measures. This requires using of some additional frameworks that would make a complete performance measurement.

In fact ISO17799 and COBIT have many common in some issues, and sometimes they complete each other. This shows us that their combination could be a very complete and comprehensive standard for any kind of enterprise and any application. In any situation if a company wants to implement Information Security Management, it should consider that chosen standard can cover national requirements, match their business and control objectives, and help to establish strong IT governance system; otherwise it will need to add some other frameworks, or make other adjustments for each specific IT environment.

In some cases an enterprise cannot implement some of the best practices within the standard because it does not fit some of business objectives or IT environment. In this case managers should show auditors who try to audit them against only best practices their business analysis that proves that these practices work against their business. Even though it is a standard that everybody has to follow to comply with requirements, each enterprise has to adjust standards to their specific situation.

To conclude, every framework or standard could be good for your enterprise, if you would find a good way of implementing, find only practices that would work for you and take only advantages of each framework. In some cases managers could consider combination of different frameworks and standards to make their information security strong and sound.

## References

1. Home page of the COSO website: <http://www.coso.org/>
2. Sh. Ladan, A. Yari, and H. Khodabandeh. “Combination of Information Security Standards to Cover National Requirements” // Transactions on Engineering, Computing and Technology. Volume 13, May 2006. ISSN 1305-5313.
3. Tom Carlson. “Information Security Management: Understanding ISO 17799”.
4. Jan Eloff, Mariki Eloff. “Information Security Management – A New Paradigm”.
5. “Implementing Information Security Governance” // Case study of Entrust Inc.
6. COBIT 4.0
7. Home page of Entrust Inc. [www.entrust.com](http://www.entrust.com)
8. Don Holden. “ISO17799 Security Standard: How Will It Fit with Other Standards?”