Corporate Governance, Internal Control and Compliance

Christer Magnusson

September 2007

SVENSKT NÄRINGSLIV
CONFEDERATION OF SWEDISH ENTERPRISE

- From an Information Security Perspective

The report is commissioned by the Confederation of Swedish Enterprise and the Swedish Risk Management and Security organization, NSD, and written by Dr. Christer Magnusson. It is based on a research project at SecLab at the Department of Computer and Systems Sciences at Stockholm University and the Royal Institute of Technology. The report gives us the opportunity to take part in the development in Corporate Governance and IT security. NSD's reference group for the project has contributed with their valuable experience. It consisted of Ms. Ingrid Mogensén, CISO of Electrolux, Mr. Magnus Ek, CSO of the Vattenfall Group, Colonel Hans Dahlqvist, Rote Consult, and Mr. Tommy Svensson, Head of Security at the Confederation of Swedish Enterprise and the Executive secretary at the Swedish Risk Management and Security organization, NSD.

Göran Norén

Confederation of Swedish Enterprise

My ambitious master student, Mr. Kerem Kocaer, who graduated from the international information security masters program at the Royal Institute of Technology, was of great importance to conduct and complete the project. We have done our best to verify the facts and figures in the report. However, any mistakes in this report are of course my own; should you find any, please let me know.

Christer Magnusson

Executive Summary

Corporate Governance, the system that directs and controls corporations, shall provide transparency, accountability and control of the entity's processes to the different stakeholders. The need to guarantee transparency to companies' stakeholders increased substantially after the U.S. Congress enacted Sarbanes-Oxley Act (SOX) on July 30, 2002. The most discussed section of SOX is Section 404. It calls for creation and maintenance of viable internal controls defined as a broad concept extending beyond the accounting function of a company.

The U.S. Securities and Exchange Commission requires companies to base their assessment on a suitable and recognized internal control framework (i.e. COSO-ERM). A challenge is to integrate COSO-ERM with other standards and frameworks, as for instance, the Service Management standard ISO 20000, the Information Security standard ISO 27001 and in-house developed frameworks (for example a Security Architecture).

COSO-ERM, ISO 20000 and ISO 27001 provide guidance for their solo implementation. Although they overlap in some topics, there is an inevitable gap between them due to the fact that they aim towards different goals. Thus, integrating them becomes a challenge since there is a lack of information when it comes to their collaborative use. This situation causes confusion and difficulty in most organizations where several of these standards have to be implemented simultaneously.

The most appropriate option in order to identify the IT gaps between COSO-ERM, ISO 20000, ISO 27001 and the Security Architecture is to use the framework COBIT as the "Plumber". The Plumber approach "tailors" a selection of COBIT controls to pre-existing standards and frameworks. Unnecessary work can consequently be avoided; COBIT is only utilized when there are detected gaps between COSO-ERM, ISO 20000, ISO 27001, and an internal framework as a Security Architecture.

No area of U.S. SOX has generated more controversy than Section 404 (covering creation and maintenance of viable internal controls). One reason is the harsh criminal penalties that Section 404 imposes, if it is "more than a remote likelihood" that a material misstatement could occur. Today, there are strong commercial forces behind suggested changes of SOX and Section 404. They will see a change in the probability threshold for the detection of control weaknesses from "more than remote likelihood" to "reasonably possible" that a material misstatement could occur. The recommendation is that scoping materiality is generally defined, as before SOX, in terms of a five percent pre-tax income threshold.

Another proposal is that the auditor attestation should not require the auditor to report separately on management's own internal control assessment process; i.e. a return to the same procedures as before SOX. Moreover, for lower risk components of financial processes and other areas, "…such as certain elements of the information technology environment", management and the auditor should be allowed to use a multi-year rotational testing approach within an annual attestation.

This is a change to the pre-SOX modus operandi of auditing, when auditors' main focus was on controls in financial applications. The final example of the recommendations is another example on auditing as it used to be: "…allow auditors to use more judgment and risk based control testing in their attestation, as opposed to repeating tests similar to those used in management's assessment of internal controls."

The odds seem to be in favor of a change of SOX and Section 404. However**,** the debate will continue between promoters of principle based rules (i.e. voluntary guidelines) versus compulsory regulations (i.e. SOX). The outcome will have a significant impact on Corporate Governance, ERM, Compliance, and Information Security.

Regardless the outcome of the "SOX battle", there seems to be a widespread acceptance for COSO-ERM. One reason is the need for an "umbrella" for the myriad of regulations companies are facing (with or without SOX). Moreover, COSO-ERM is an umbrella that needs support from standards and frameworks as ISO 20000 and ISO 27001 to deliver compliance in IT and application infrastructures. To facilitate that, the "Plumber" COBIT may be called in.

Introduction

Arguing that the purpose of a business is to increase shareholder value, the need to guarantee transparency of processes to the different stakeholders of the organization becomes evident[1]. This gave rise to the concept of Corporate Governance, which can be defined as the system that directs and controls corporations; it shall provide transparency, accountability and control of the entity's processes to the different stakeholders. Due to the importance of IT for business, Corporate Governance and IT Governance are interrelated. Information Security Management and Service Management are also two important parts of the overall governance system.

The need to guarantee transparency to companies' stakeholders increased substantially after the U.S. Congress enacted Sarbanes-Oxley Act (SOX) in July 30, 2002. The objective with the legislation was to reinstall confidence in U.S. equity markets after the Enron scandal and the misconduct committed by Enron's auditor, Arthur Andersen. Other, now infamous, companies such as WorldCom, Tyco, Riggs Banks, Fannie Mae, ImClone, HealthSouth, and Marsh & McLennan followed. In Europe, the stakeholders in Ahold, Parmala and Skandia had their share of rough management.

SOX was developed under the supervision of Senator Paul Sarbanes (Democrat, at that time chairman of the Committee on Banking, Housing and Urban Affairs in the Senate), and Representative Michael Oxley (Republican, the Financial Services Committee chair in the House).

The most discussed and controversial part of SOX is Section 404. It calls for creation and maintenance of viable internal controls defined as, "…a broad concept that extends beyond the accounting function of a company"[2]. Accordingly, internal controls include policies, procedure, training programs, and other processes beyond financial controls. Moreover, companies must document and test the adequacy of these internal process controls, and their auditors must attest them.

A - or "The" - reason behind the controversy of Section 404 is that the Chief Executive Officers (CEOs) and the Chief Financial Officers (CFOs) are personally and criminally liable for the quality and effectiveness of their organization's internal controls[3]. However, that has significantly boosted the executive management commitment to and involvement in Corporate Governance, at least for all public issuers subject to the U.S. Securities and Exchange Commission (SEC) registration; these companies must comply with Section 404 from 2004[4]. Compliance with SOX is also controlled and enforced by the SEC.

[1] Wheelen, T., Strategic Management and Business Policy, Prentice Hall, 2004.

[2] SEC's Final Rule: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports.

[3] SEC's Final Rule: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports.

[4] Dead-line for foreign filers (as the Company in this report) was July 15, 2006. Dead-line for small companies - with less than $75 million of market capitalization - is December 15, 2007 for Section 404(a) management assessment. Implementation of auditor attestation for small companies, Section 404(b), is a year later. Investment companies are completely except from Section 404.

Requiring management assessment and auditor attestation of internal controls had not been subjected to extensive public scrutiny prior to SOX. "Congress was essentially drawing on a blank slate when it enacted Section 404, or asking the SEC and the PCAOB to do so"[5]. The solution came from the Committee of Sponsoring Organizations' (COSO) for the understanding of internal controls.

The SEC requires companies to base their assessment on a suitable and recognized internal control framework (i.e. COSO). COSO is also referred to and accepted by the Public Company Accounting Oversight Board (PCAOB) which monitors auditors of public companies to protect the interests of investors in the preparation of audit reports. Today COSO's concept of internal controls and Enterprise Risk Management, COSO-ERM, is gaining acceptance as a global standard.

A challenge is to integrate COSO-ERM with other standards and frameworks as the Service Management standard ISO 20000, the Information Security standard ISO 27001 and in-house developed frameworks (for example a Security Architecture). COSO-ERM, ISO 20000 and ISO 27001 provide guidance for their solo implementation. Although they overlap in some topics, there is an inevitable gap between them due to the fact that they aim towards different goals. Thus, integrating them becomes a challenge since there is a lack of information when it comes to their collaborative use. This situation causes confusion and difficulty in most companies where several of these standards have to be implemented simultaneously.

The primary objective with the report is to investigate if the framework COBIT may facilitate the integration with COSO-ERM and the other standards and frameworks, or not. The latest developments regarding SOX and the possible consequences of these developments for Corporate Governance, Compliance, ERM and Information Security will also be discussed.

This report applies a research methodology based on the hermeneutic philosophy which emphasizes the importance of understanding and interpreting texts within their context and by reference to the whole. The "hermeneutic circle", describing this process, refers to the idea that one's understanding of the text as a whole is established by reference to the individual parts and one's understanding of each individual part by reference to the whole. This circular dependence of interpretation stresses the importance of analyzing texts within their context.

The report bases itself on qualitative data obtained through literature review and a study of the conditions and the business context of the fictive Company. Five main standards and frameworks constitute the background of the study: the COSO-ERM framework, the ISO/IEC 20000 standard, the ISO/IEC 27001 standard (with the supporting ISO/IEC 17799 standard), the Security Architecture in the Company, and the COBIT framework.

[5] INTERIM REPORT OF THE COMMITTEE ON CAPITAL MARKETS REGULATION, November 30, 2006.

Following the hermeneutic circle principle, each text is analyzed in two steps: an individual study to understand and present the text and an interpretation of the text according to its relation with the other standards and frameworks. Figure 1 illustrates the main steps followed during this research.

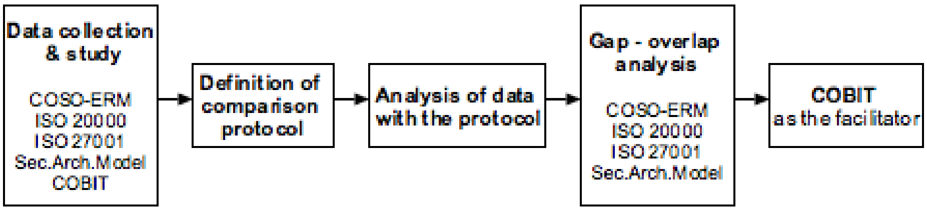


Figure 1: Steps followed during the research

Firstly, COSO-ERM, ISO 20000, ISO 27001, the Security Architecture and COBIT are studied individually to understand their purpose and content. Then, a set of criteria (the protocol) is defined to compare these standards and frameworks. After analyzing the collected data according to the protocol, another analysis is performed to identify the gaps and overlaps between COSO-ERM, ISO 20000, ISO 27001 and the Security Architecture. Finally, the usage of COBIT as a facilitator for the integration is discussed.

After this “Introduction” and the following presentation of “The Company”, the report presents 5 Sections and Conclusions. Section I, “Standards and Frameworks”, presents the four standards and frameworks that need to be integrated: COSO-ERM, ISO 20000, ISO 27001, and the Security Architecture, as well as the potential integrator, COBIT. Section II, “Comparing the Standards and Frameworks”, introduces the “Comparison protocol”, followed by a protocol analysis of COSO-ERM, ISO 20000, ISO 27001, and the Security Architecture. The results are analyzed in the “Gap – overlap analysis” in Section III. Section IV discusses the different options of using COBIT. Moreover, it adds COBIT to the gap - overlap analysis (performed in the previous section for the other standards and frameworks). The objective is to choose the most appropriate option of COBIT as a possible integrator. A summary of the two reports, considered to be most important forces behind the suggested changes of SOX, is presented in Section V. Finally, Conclusions are made.

The Company

This fictive, but fairly realistic company is the global leader (based on revenue) in their industry group. It is listed at one of the U.S. stock exchanges. It was already listed in the United States before SOX was enacted. Since the company is owned by 300 or more U.S. shareholders, it cannot exit from the U.S.marketplace and thereby avoid SOX.

The company has a strong balance sheet. However, the company faced the challenge with integrations costs after massive acquisitions around the globe. As a result, the company has recently become a target for Private Equity companies. The first item on their agenda would be to increase the leverage of the company and to sell out parts of the company. This has further increased the pressure on the primary target of the company: to deliver the highest possible shareholder returns (change in share price and dividends relative industry peer group). The giant has one single value driver for its business units: Economic Value Added (EVA). However, the liability that follows a public issuer subject to SEC registration highlights Corporate Governance, besides EVA.

The framework for Corporate Governance and control of risk in the company is based on COSO-ERM. The framework is an integrated part in the CEO's contract with the heads of the business units (BU). The head of each BU has signed a formal risk contract with the CEO, which is evaluated by the CEO and CFO before interim and annual reports to the market. The contract stipulates risk appetite and risk tolerance for the BUs'. The total risk of the company is decided by the board of directors. The development of the aggregated risk appetite is a permanent item on the agenda at the board meetings.

The high attention from the executive management (and the board of directors) is understandable, especially when it comes to Section 404 of SOX. The reason is that the CEO and CFO certification requirements in Section 302 of SOX apply to Section 404 reporting. Moreover, Section 906, covering criminal sanctions against CEOs and CFOs being aware of material misrepresentations of financial information, might also apply to Section 404 reporting.

Section 404 requires of the company (as for all issuers of public securities subject to SEC registration) to publish "an assessment . . . of the effectiveness of the internal control structure and procedures of the issuer for financial reporting"[6] in their annual report. The executives must state whether the controls are effective and note any significant deficiencies or material weaknesses in internal controls.

A "material weakness" exists if there is more than a remote likelihood that a material misstatement of the interim or annual financial statements will not be prevented or detected[7]. Management and auditors are also obliged to look for "significant deficiencies," which can be the evidence of a material weakness. Management and auditors may conclude that the company's internal control over financial reporting is effective if there are one or more material weaknesses in the company's internal control over the financial reporting.

"Significant deficiencies" are deficiencies resulting in more than a remote likelihood that a misstatement of the company's interim or annual financial statements will not be prevented or detected.

Section 404 (b) requires of the company's external auditor to attest to, and report on, the assessment made by the management of the issuer of the control environment.

[6] Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745.

[7] Auditing Standard No.2 (AS2) required by Section 404.

Auditors need to provide reasonable assurance that no material weaknesses exist in the company's internal control over financial reporting.[8] They must reach an independent conclusion about the effectiveness of internal controls. Specifically, an auditor must obtain the principal evidence for this independent judgment on the basis of his or her own work. An auditor can rely on the work of others (including work by internal auditors) only to the extent consistent with forming an independent view.

The company faces a dilemma: how to be compliant without reducing operational efficiencies and thereby competitiveness. Adding to the dilemma are the acquisitions of companies previously made. How could these be integrated successfully with the company's own IT infrastructure, Enterprise Resource Planning (ERP), Customer Relationship Management, Logistics, and Financial systems? The lack of a coherent IT and application infrastructure is the reason why financial data from these disparate application systems are keyed in manually into spreadsheets at the head office (with insufficient security, no version control, poor or nonexistent documentation, and no independent testing of the usually highly complex spreadsheets). As a result, at least one time, errors have resulted in publicly known misstatement in the company's financial reporting.

SOX require changes in the IT infrastructure and the application systems. Internal controls needs to be implemented systematically both in the IT infrastructure and the application system. An example of a requirement that needs to be in place to improve internal controls is the technology for Segregation Of Duties (SOD). The technology to enforce SOD must be installed and implemented in the whole business chain, ranging from system administrators of vital server parks to ERP systems used by business executives. Another objective for internal control is to assure accountability and traceability of operations. Handling (and normalization) of log data from different system environments is an essential part to achieve this control objective.

The company has outsourced some parts of its IT and application infrastructure to different partners. According to SOX, management is still liable for outsourced operations that may affect the financial performance of the company. However, SOX Section 404 accepts the Statement of Auditing Standards No. 70 (SAS 70) from outsourcing companies. Therefore the company requires a SAS 70 Type II (covers internal controls for a minimum period of six months) from its outsourcing partners[9]. Still, the company needs to stipulate in the Service Level Agreements (SLA's) the security requirements and controls that should be in place.

The Information Security standard ISO 27001 and the in-house developed Security Architecture together with the Service Management standard ISO 20000 are the means the company has chosen to try reaching a coherent internal (and external) control and security structure under the umbrella of COSO-ERM.

[8] PCAOB Bylaws and Rules – Auditing Standard No. 2, 2006.

[9] www.SAS70.com.

How can the company, however, bring these four (COSO-ERM, ISO 20000, ISO 27001 and the Security Architecture) components together towards the goal of Corporate Governance? The Chief Security Officer and the Chief Compliance Officer suggest to the executives to investigate if the framework COBIT can facilitate the integration of these components, or not. The project is approved and the result will be presented in the following sections.

Section I. Standards and Frameworks

Several standards and frameworks were created by international bodies to help companies understand, implement and comply with requirements in different areas, such as corporate governance, IT governance, risk management, IT service management and information security. In addition, companies often have their own "ways of working" by using their internal models or frameworks. The following section presents the framework COSO-ERM, the standards ISO 20000 and ISO 27001 standards, and the frameworks the Security Architecture and COBIT.

COSO-ERM

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) was formed in 1985 to make recommendations on how companies and auditors should identify and attack fraudulent financial reporting. COSO consist of the American Institute of Certified Public Accountants, the American Accounting Association, Financial Executives International, the Institute of Management Accountants, and the Institute of Internal Auditors.[10]

COSO-ERM (Enterprise Risk Management - Integrated Framework) is the resulting framework of a project initiated and published by COSO (developed by PricewaterhouseCoopers). It expands on COSO's "Internal Control – Integrated Framework", published in 1992, by providing a greater focus based on the broader subject of Enterprise Risk Management.[11]

The framework's main audience is the board of directors and the senior management. However, it contains information about ERM that is potentially useful to many others, including internal auditors, other entity personnel, external regulators, professional organizations and educators.

Its goal is to "provide direction to evaluate and enhance the effectiveness of enterprise risk management"[12]. This is achieved by providing guidance to help companies build effective systems for identifying, measuring, prioritizing and responding to risk.

The framework addresses the essential concepts, principles and components of ERM, provides a common ERM language to communicate more effectively and discusses the roles and responsibilities of the people inside and outside or the organization related to ERM. COSO-ERM also gives the organization the possibility to assess its ERM process against a commonly agreed standard, helping it to strengthen the ERM and move towards its established objectives.

[10] www.COSO.org.

[11] The Institute of Internal Auditors, 1, COSO Releases New ERM Framework, 2007.

[12] Enterprise Risk Management - Integrated Framework: Executive Summary and Framework (COSO-ERM), The Committee of Sponsoring Organizations of the Treadway Commission (COSO), PricewaterhouseCoopers, 2004.

The purpose of a business is to increase shareholder value. COSO-ERM builds itself on this premise, aiming for value creation through reaching the optimal balance between growth, returns, uncertainties, risks and opportunities. According to COSO-ERM, the optimal balance can be reached with the following capabilities encompassed in ERM:

- Aligning risk appetite and strategy: Risk appetite is defined as the amount of risk an entity is willing to accept in pursuit of value and is directly related to strategy. Effective ERM requires management to evaluate strategic alternatives and set high level objectives in line with the entity's risk appetite.
- Enhancing risk response decisions: Effective ERM will help the entity to take rigorous decisions when choosing between the risk responses (avoid, reduce, share and accept).
- Reducing operational surprises and losses: ERM enhances the entity's capability to identify potential events and establish responses, reducing surprises and associated costs or losses.
- Identifying and managing multiple and cross-enterprise risks: Treating individual risks is not enough as risks are often interrelated. Thus, a holistic cross-enterprise view over the risks is a requirement for effective ERM.
- Seizing opportunities: Events can be either risks, in which case they have to be assessed and treated, or opportunities, in which case they must be fed back to the strategy setting phase. Hence, merely looking at "risks" is not sufficient; management should consider the full range of potential events to be able to identify opportunities.
- Improving deployment of capital: Capital allocation is a key element for value creation. Obtaining information on risks allows the entity to better assess its needs for capital and to effectively allocate capital.

COSO defines Enterprise Risk Management as follows:

"Enterprise Risk Management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives"[13].

This definition emphasizes the following keys elements:

- ERM is a process. It is a dynamic, continuous or iterative interplay of actions. ERM is not just another activity; it is built into the infrastructure and is a part of the entity. The integration of ERM into basic activities allows the enterprise to avoid unnecessary procedures and costs.

[13] Enterprise Risk Management – Integrated Framework: Executive Summary and Framework (COSO-ERM), The Committee of Sponsoring Organizations of the Treadway Commission (COSO), PricewaterhouseCoopers, 2004.

- ERM is effected by people at every level of the enterprise, from the board of directors to the lower level personnel, and affects peoples' actions. ERM helps people understand the entity's strategy, objectives and risks related to those.
- ERM is applied in strategy setting, helping management to select the entity's strategy and objectives.
- ERM is applied at every level and unit of the entity, considering the entire scope of activities. Thus, it is necessary to obtain a portfolio view of risks and to consider the interrelation between risks.
- ERM is designed to manage risks within the entity's risk appetite. Operating in line with its risk appetite and within its risk tolerance ensures that the organization is moving towards its objectives.
- ERM provides reasonable (not absolute) assurance that the entity's objectives will be achieved.
- ERM is geared to the achievement of the objectives. It is a tool to each of the goals, not the goal itself.

The COSO-ERM framework is illustrated in Figure 2, showing its three dimensions: objectives, components and entity units. ERM is said to be effective when the eight components are present and functioning effectively in each of the four objectives, providing reasonable assurance to management about the achievement of the objectives.

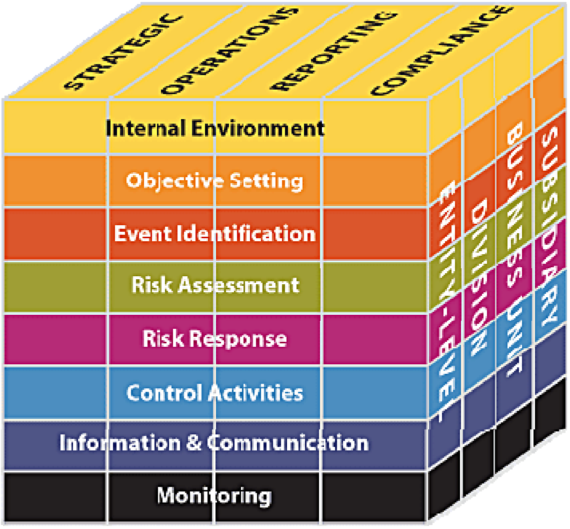


Figure 2: COSO-ERM

An entity's objectives, representing what the entity tries to achieve, are derived from its strategic goals and can be categorized under the following four types of objectives:

- Strategic objectives: high level goals, aligned with and supporting the entity's mission.
- Operations objectives: effective and efficient use of the entity's resources.
- Reporting objectives: reliability of the entity's reporting.
- Compliance objectives: the entity's compliance with applicable laws and regulations.

On the other dimension, COSO-ERM points out eight components of ERM:

- Internal Environment: representing the entity's discipline and structure. It is influenced by the history and culture of the organization. It comprises very important issues that define how risk is observed and addressed. These include the risk management philosophy, risk appetite, commitment to competence, responsibilities, human resource standards, etc.
- Objective Setting: precondition for the risk assessment components (event identification, risk assessment, risk response). This component ensures that strategic objectives are set in line with the entity's mission, that all objectives are understandable, measurable and consistent with the entity's risk appetite.
- Event Identification: all events, whether internal or external, risk or opportunity, are identified and forwarded to the right components. Events can result from internal factors such as the personnel or the technology, and external factors such as economic or political events.
- Risk Assessment: risks, both inherent and residual, identified in the previous component are assessed in terms of their likelihood and impact, using internal and external data sources and qualitative or quantitative techniques. A portfolio view of risks is adopted, analyzing the interrelationships of events during the assessment.
- Risk Response: the objective is to bring the residual risks within the desired risk tolerances, the responses or combinations of responses are chosen, planned and implemented using a portfolio perspective.
- Control Activities: to ensure that risk responses are conducted correctly, different types of controls (policies, procedures, mechanisms, etc.) are installed.
- Information & Communication: represents the need for information systems that acquire, manage and distribute relevant information to allow the management of risks and the achievement of objectives. This component also includes effective communication, both internal and external.
- Monitoring: The effectiveness of ERM should be verified by monitoring through ongoing activities and separate evaluations. Monitoring results should be reported to the right people.

Since ERM is a dynamic, iterative process, the components are closely related and affect each other.

Besides the components, COSO-ERM states the establishment of roles and responsibilities as a general requirement for effective ERM. Hence, the framework includes a discussion about the roles and responsibilities of entity personnel at different levels and external parties such as outsourcing partners, legislators and regulators, external auditors, financial analysts.

ISO/IEC 20000

The Information Technology Infrastructure Library (ITIL) is a framework of best practices in the field of IT service management. It was published by the Central Computer and Telecommunications Agency (CCTA), now the British Office of Government Commerce (OGC). It consists of eight books (recently supplemented with guidelines for smaller IT units).[14]

The international standard that reflects ITIL's guidance for IT service management is ISO/IEC 20000, which is based on and replacing the earlier British standard BS 15000. It was published in December 2005 by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) and consists of two parts:

- ISO 20000-1 Specification "promotes the adoption of an integrated process approach to effectively deliver managed services to meet the business and customer requirements"[15]. It comprises the following topics:
  - Requirements for a management system
  - Planning and implementing service management
  - Planning and implementing new or changed services
  - Service delivery processes
  - Relationship processes
  - Control processes
  - Resolution processes
  - Release processes
- ISO 20000-2 Code of practice provides "best practices for service management processes within the scope of ISO 20000-1"[16]. It contains the same sections as part 1, providing guidance for each of them, except "Requirements for a management system" as part 2 does not impose any requirement.

Some of the most important processes included in the sections mentioned above are:

- Incident management

[14] COBIT Mapping – Mapping of ITIL with COBIT 4.0, pp.16, 17, IT Governance Institute, 2007b, 2007.

[15] Information Technology – Service Management – Part 1: Specification (ISO/IEC 20000-1:2005), International Organization for Standardization, 2005b, 2005.

[16] Information Technology – Service Management – Part 2: Code of Practice (ISO/IEC 20000-2:2005), International Organization for Standardization, 2005b, 2005.

- Change management
- Problem management
- Service level management
- Service continuity and availability management
- Configuration management
- Release management
- Security management

ISO 20000 targets people in the organization that are responsible for IT service management. This includes the Head of Operations as the primary audience, and the Chief Information Officer (CIO), the Business Process Owner, the Head of Development, the Head of IT Administration, the Project Management Officer as the secondary audience.[17]

The goal of the publication is to guide organizations in delivering managed services to meet the business and customer requirements. The implementation of an effective service management system leads to improved quality, lower costs, greater flexibility and faster response.

ISO 20000 and ITIL are considered useful in improving the infrastructure to provide ongoing services through service management. However, they should not be seen as a comprehensive solution to all the IT issues and should be applied as a tool within the context of a broader organizational strategy[18].

Concerning security-specific controls, ISO 20000 references: ISO 17799 IT – Security techniques - Code of practice for information security management.

ISO/IEC 27001

ISO/IEC 27001[19], “Information technology - Security techniques - Information security management systems Requirements”, is an information security management system (ISMS) standard based on and replacing ISO/IEC 17799 part 2, and published in October 2005 by ISO and IEC. It was designed to be used together with ISO/IEC 17799:2005 (part 1), “Information Technology - Security techniques - Code of practice for information security management”, which contains an implementation guideline that can be used when designing the security controls required in ISO 27001.

The standard targets people in the organization who are responsible for the initiation, implementation or maintaining of information security. This includes the Chief Information Officer (CIO), the Chief Architect, the Head of Development, the Head

[17] COBIT Mapping – Mapping of ISO 17799:2005 with COBIT 4.0, pp.6, IT Governance Institute, 2007a, 2007.

[18] Meyer, D., What’s beneath all the buzz about ITIL?, pp.1, 2005.

[19] Information Technology – Security Techniques - Information Security Management Systems – Requirements, ISO/IEC 27001:2005, ISO and IEC 2005a ISO and IEC (2005a), 2005.

of IT Administration, Compliance, audit, risk and security people as the primary audience, and the Chief Executive Officer (CEO), the Business Executive, the Business Process Owner, the Head of Operations as the secondary audience[20].

The goal of ISO 27001 is to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of business risks"[21]. It guides the organization through the selection of adequate security controls. However, ISO 27001 is not enough by itself; ISO 17799:2005 is indispensable for the application of ISO 27001.

From a corporate governance perspective, ISO 27001 helps acquiring knowledge about the business activities via asset identification, business impact assessment, risk assessment, etc. ISO 27001 is not limited to IT. The standard covers information in its broader sense, independently of media, in all business processes and parts of an organization.

The Security Architecture

The Security Architecture is specifically designed for the fictive Company. Its primary audience is the security experts who have a good knowledge of security services and mechanisms. However, the first part of the architecture also contains information about the "costs for security", usually of concern for management.

The architecture's goal is to provide guidance for the installation of appropriate security services and mechanisms in order to reach uniform security by meeting weaknesses equivalently independently on the IT area.

The model behind the architecture starts from threats against, and weaknesses and vulnerabilities in different IT resources, aiming to design security services and mechanisms to reduce the vulnerabilities. The choice of security mechanisms and their strength depends on the security properties (confidentiality, integrity, availability) that must be protected and on the security level (1 to 4).

Security levels and services can be defined independently of an IT area, but security mechanisms are defined for a specific technical area. However, other than the IT-area-specific security mechanisms, there are also general mechanisms that cover all the areas.

Figure 3 illustrates the concepts of threat, weakness, vulnerability and countermeasure within a specific IT area. Threats exist in the external environment, independently of IT areas. However, there must be a weakness in the system which the threat can exploit to make the system vulnerable. Countermeasures in form of

[20] COBIT Mapping – Mapping of ISO 17799:2005 with COBIT 4.0, pp.6, IT Governance Institute, 2007a, 2007.

[21] Information Technology – Security Techniques – Information Security Management Systems – Requirements (ISO/IEC 27001:2005), International Organization for Standardization, 2005a, 2005.

security services and mechanisms within specific IT areas protect the systems' IT resources against the vulnerabilities. The strength of the counter measures depends on the security level; the higher the level, the lower the residual risk.

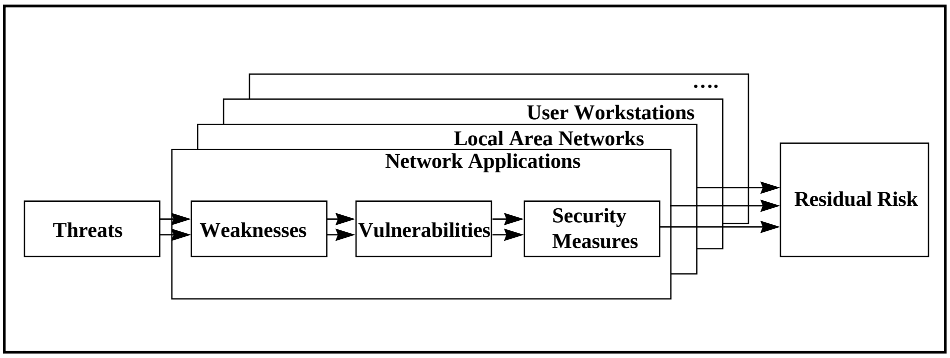


Figure 3: Threat, weakness, vulnerability and security measure

The grouping of resources in IT areas assumes the presence of uniform and consistent security levels between the different IT areas. If a weakness is not treated equivalently in all the areas, there will be a weak link which will cause potential vulnerabilities in the whole chain. Hence, the goal with defining the security levels independently of the IT areas is to have uniform security where no link is weaker than the other.[22]

The architecture presents in more detail the security properties (confidentiality, integrity, availability), the types of threats, the security services in different security areas (physical, logical, administrative), the IT areas (common IT, workstations, network applications, local networks, connections with external networks), the security levels and the security domains. The second part of the architecture includes a detailed description of the security mechanisms proposed.

COBIT

COBIT (Control Objectives for Information and related Technology) is a framework created by the Information Systems Audit and Control Foundation (ISACF) in 1996. The second edition was published in 1998, and the third in 2000 by the IT Governance Institute (ITGI). The latest version of COBIT, COBIT 4.0, was released in 2005.

COBIT addresses all types of organizations, public and private companies, and external assurance and advisory professionals. Within the organization, COBIT targets management (executive management and boards, business and IT management) as well as auditors and governance, assurance, control and security professionals. COBIT consists of several documents addressing different people:

[22] Magnusson, C., Security Architecture Model, GMTM, 2006.

While the Executive Overview, the Management Guidelines and the Framework are designed for management, the Detailed Control Objectives and Audit Guidelines are designed for IT, assurance and security people.

COBIT is a set of best practices for IT Governance. The objective is to guide its audience in maximizing the benefits gained from the use of IT systems while developing appropriate controls.. ITGI explains its mission as:

"To research, develop, publicize and promote an authoritative, up-to-date, internationally accepted IT governance control framework for adoption by enterprises and day-to-day use by business managers, IT professionals and assurance professionals"[23].

The framework supports IT governance by ensuring that:

- IT is aligned with the business
- IT enables the business and maximizes benefits
- IT resources are used responsibly
- IT risks are managed appropriately

The main characteristics of COBIT are: Business focus, Process orientation, Control based, and Measurement driven. These characteristics are elaborated on below.

Business-focused

IT systems support the business by providing the information that the organization needs to achieve its objectives. Hence, to "guarantee" that IT is fulfilling this role to deliver the required information services, COBIT states that IT resources should be managed and controlled using a set of processes. Figure 4 illustrates this principle.

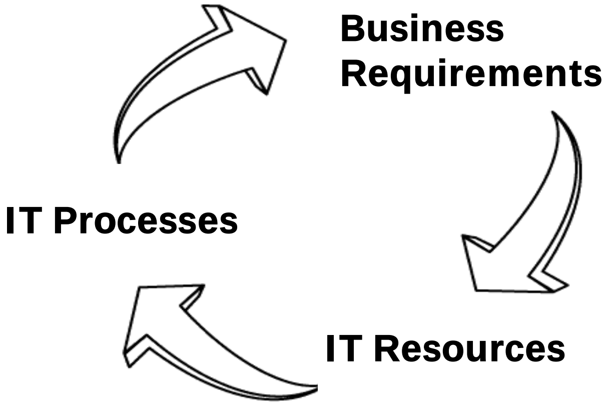


Figure 4: The basic principle of COBIT

[23] COBIT Mapping – Overview of International IT Guidance, pp.8, IT Governance Institute, 2006.

To ensure IT is aligned with business, COBIT introduces the following concepts:

– *The Information Criteria* must be complied with in order to support business objectives. The criterion encompasses quality, security and fiduciary of information and consists of the following properties:

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

– *Business goals and IT goals* should be clearly defined to be able to establish clear business requirements and metrics to measure the achievement of the goals. COBIT helps establish the link from the Enterprise strategy to the IT architecture.

– *IT resources*, defined by COBIT as:

- Applications
- Information
- Infrastructure
- People

For each of the high level controls provided by COBIT, the associated information criteria, goals and metrics, and resources are listed.

Process-oriented

COBIT follows a process model consisting of four phases:

1. Plan and Organize is the most important phase to establish the link between IT and business objectives. It ensures that IT is aligned with business, resources are used in an optimal way, IT objectives are communicated throughout the organization, risks are managed and IT systems satisfy the required quality.
2. Acquire and Implement is concerned with the identification, development or acquirement, implementation and integration of IT solutions in order to realize the IT strategy previously developed. This phase also covers changes and maintenance of existing systems.
3. Deliver and Support mainly covers the delivery and support of services, the optimization of costs and the management of security.

4. Monitor and Evaluate ensures that the processes are constantly monitored and evaluated. It is also concerned with improving the performance, providing regulatory compliance and governance.

Controls-based

COBIT defines controls as "policies, procedures, practices, organizational structures to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected"[24]. COBIT provides high-level control objectives, each of them containing detailed control objectives, together with generic control requirements that are applied to all the processes. COBIT is concerned with "General IT controls", and not "Application controls" which are the responsibility of the business process owner. However, it provides a recommended list of application controls dealing with the origination/authorization, input, processing, output and boundary of data.

Measurement-driven

COBIT provides tools for measuring the capability and the performance of processes. These are maturity models ("Where we are, Where the industry is, Where we want to go") to measure capability, and IT goals and metrics, process goals and metrics, and process performance metrics to measure performance. Key Goal Indicators (KGI) and Key Performance Indicators (KPI) are used for this purpose.

Figure 5 illustrates the basic principle of the COBIT framework: "IT resources are managed by IT processes to achieve IT goals that respond to the business requirements"[25].

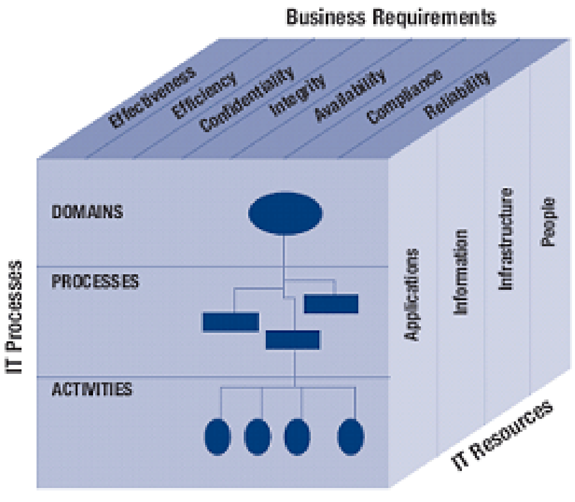


Figure 5: COBIT Framework principle

[24] Control Objectives for Information and Related Technology, COBIT 4.0, IT Governance Institute, 2005.

[25] Control Objectives for Information and Related Technology, COBIT 4.0, IT Governance Institute, 2005.

The framework provides 34 processes - high level objectives - containing a total of 215 control objectives. For each of the processes, COBIT explains the related information criteria, IT resources, inputs and outputs, a RACI chart explaining roles and responsibilities, goals and metrics, and maturity characteristics to measure the capability and performance of processes.

Section II. Comparing the Standards and the Frameworks

Section I gave an overview of the COSO-ERM framework, the ISO 20000 and ISO 27001 standards and the Company's Security Architecture. These focus on different, but related topics that are relevant for the achievement of corporate governance. Hence, to reach the goal of corporate governance, they need to be used simultaneously. However, to be able to realize their integration, they must be compared in order to understand their interrelationship and find the potential gaps and overlaps between them.

Comparison Protocol

To be able to efficiently compare the different standards and frameworks, a set of comparison criteria, the so-called "comparison protocol", was created. The goal of the protocol is to encompass the most important aspects of the standards and frameworks that are to be integrated: COSO-ERM, ISO 20000, ISO 27001 and the Security Architecture. It is not meant to be an exhaustive list of all the aspects covered by the standards and frameworks but to provide a general understanding of their fundamentals aspects.

The protocol begins by questioning the audience and the abstraction level of the standards and frameworks, and continues with criteria covering several aspects of COSO-ERM, ISO 20000 and ISO 27001. COSO-ERM forms the basis of the protocol with its eight components, due to its highest level of abstraction compared to the others, and the relevancy of its components towards reaching corporate governance. As a result, criteria 3 to 8 are derived from the COSO-ERM components. However, some of them are modified and enhanced by complimentary questions from other standards, or contain a grouping of COSO-ERM components, such as the "Risk analysis approach" criterion which maps to the "Event identification", "Risk assessment" and "Risk response" components.

The protocol continues with criteria compiled from the ISO 20000 and ISO 27001 standards. The Security Architecture does not contribute to the formation of the protocol because of its lower level of abstraction; it is more of a supporting model for satisfying security controls set by ISO 27001.

The protocol consists of the following comparison criteria:

1. Audience

This criterion compares the audience of the standards and frameworks, resulting in an overall view of the people involved in corporate governance works.

2. Abstraction level

Analyzing the abstraction level of the standards and frameworks helps to position them in relation to each other, giving an overview scheme of how they can fit together. The main focus here is to understand how broad the covered area is in relation to how much detail that is covered by the area.

3. Objective

First, the general objectives of the document are defined. Then, these objectives are compared with the four objectives defined by COSO-ERM (strategic, operations, reporting, compliance objectives) to see how much and from which perspective they support corporate governance.

4. Internal Environment

This criterion is based on COSO-ERM's Internal Environment component. It also includes discussion points from the Information and Communication component and from the Roles and Responsibilities section of COSO-ERM. It is concerned with the following topics:

- Risk appetite
- Management commitment
- Competence, awareness, training
- Internal communication
- Internal roles and responsibilities

5. Risk Analysis

The risk analysis approaches of the different documents are examined. The following questions are posed:

- Is a risk analysis approach specified?
- Are both risks and opportunities considered?
- What are the mentioned risk assessment steps?
- What risk responses are proposed?
- Is a risk analysis methodology specified?

6. Control Activities

This part of the protocol covers the standards' and frameworks' type of controls, the area they relate to, and whether the standards and frameworks provide a list of controls.

7. Monitoring and Improvement

The monitoring and improvement approaches are analyzed, answering the questions "What is monitored and improved" and "How is the monitoring and improvement realized".

8. Documentation and Reporting

Documentation and reporting requirements as well as processes are analyzed to compare the audience and abstraction level of documents.

9. Budgeting and Return on Investment

This criterion analyzes how the standards and frameworks are concerned with budgeting and accounting issues in order to compare their approach to the terms “cost” and “return on investment”.

10. External Relationships

As organizations are largely influenced by their external environment, measures should be taken to control this environment. This criterion examines what the standards and frameworks say about the entities’ relationships with external parties.

11. Incident Management

Incident management is an important issue since services could be reduced or interrupted because of incidents. The documents are analyzed to compare their approach to deal with incidents.

12. Release Management

This protocol criterion analyzes what the standards say about the release of applications, and what controls they provide to ensure proper releases.

13. Control Management

Control management encompasses “configuration management” which is the management of all items and assets in the organization, and “change management” which deals with changes that should be handled in an appropriate way.

Below, COSO-ERM, ISO 20000, ISO 27001, the Security Architecture, and COBIT are analyzed in detail, according to the comparison protocol.

COSO-ERM

1. Audience

This framework’s main audience is the board of directors and the senior management of the organization. However, it contains information about ERM that is potentially useful to many others, including:

- Internal: Besides board of directors, the senior management, internal auditors, other entity personnel
- External: Regulators, professional organizations, educators.

2. Abstraction Level

The report is on a very high abstraction level. It is mainly a management and control framework, and does not address specific IT requirements. However, its key concepts and definitions can be used by IT Governance efforts to address IT issues.

3. Objective

- Goals:

  – Provide direction to evaluate and enhance the effectiveness of enterprise risk management.

  – A common language to communicate more effectively; the possibility to assess the entity's ERM process against a standard, to strengthen it and to move towards established goals; increased understanding of ERM by legislators and regulators.

- The COSO-ERM Objectives are: strategic, operational, reporting, and compliance (explained in the previous section).

4. Internal Environment

- According to COSO-ERM, the risk management philosophy of the entity is influenced by its internal environment (discipline, structure, history, culture, etc.) and is mainly reflected by its risk appetite.
- COSO-ERM defines risk appetite as the "guidepost in strategy setting", and explains that "ERM helps management to select a strategy consistent with its risk appetite. Management aligns the organization, people, processes, infrastructure and resources to enable the entity to stay within its risk appetite. Risk tolerances are aligned with the risk appetite."
- COSO-ERM emphasizes the importance of Management Involvement and Commitment: "The attitude and concern of management for effective risk management must be definitive and clear, and permeate the organization. The board of directors must perform its oversight responsibilities."
- COSO-ERM mentions briefly the need of an "ongoing education process" under the section "Human Resource Standards". Human resource practices should, among other responsibilities (hiring, counseling, compensating, etc.), install training policies. Also, COSO-ERM defines the ERM as a process effecting and affected by all the entity personnel's actions. Hence, the people must be made aware of the connection between their actions and the ERM process.
- COSO-ERM lists the following requirements for internal communication:

  – clear and effective communication from management to personnel (about the importance of ERM, entity objectives, risk appetite and tolerance, common risk language, roles and responsibilities).

– open communication channels, normal and separate communication lines, willingness to listen.

- With regard to internal roles and responsibilities, COSO-ERM contains an important chapter, stating that every individual in the entity contributes by effecting or supporting ERM. The report includes a section for each of the following parties, explaining their roles and responsibilities: The Board of directors, the management, the risk officer, the financial executives, and the internal auditors.

5. Risk Analysis

- COSO-ERM's risk analysis approach is reflected in three of its components: Event identification, Risk assessment and Risk response, supplemented with the component "Control activities", which ensure that the risk responses are carried out.

  Event identification is the first step where management identifies potential events that, if they occur, might have positive effects (opportunities) or negative effects (risks) on the entity. Opportunities are fed back into the "objective setting" component, while risks are fed to the following "risk assessment" and "risk response" components. During the risk assessment process, management assesses the identified events usually considering likelihood and impact of both the inherent and residual risks.

  Management determines, in the risk response phase, whether to avoid, reduce, share or accept the risks, taking an entity-wide cost-effective perspective to bring the residual risk within the entity's risk appetite.

- COSO-ERM lists the main basic requirements (the "what") to analyze risks and opportunities. It is on a high level and does not explain how to conduct risk analysis (the "how").

6. Control Activities

COSO-ERM defines control activities as policies and procedures to help ensure that management's risk responses are carried out properly and timely. It mentions some examples of different categories and types of controls, including management controls ("segregation of duties", "security management", etc.) and more specific IT controls ("physical controls"), just to illustrate the range of controls, not to provide any list. Furthermore, it emphasizes that controls should be entity-specific.

7. Monitoring and Improvement

- Monitoring is one of the eight components of COSO-ERM and a key issue to assess the presence and effectiveness of the ERM components over time. It is realized through real-time, dynamic ongoing activities built into normal operations or through separate evaluations with variable scope and frequency. These can be performed by internal auditors (self-assessment) or by external auditors.

- COSO-ERM defines the evaluation as a process in itself and explains the basic rules to follow without enforcing a specific approach or methodology.
- Separate evaluations differ by scope and frequency. Higher-priority risk areas and responses are evaluated more often. Evaluation of the entire ERM is needed less frequently and may be prompted by some events such as a major strategy change or a change in the political or economic situation, etc.
- Identified problems or opportunities should be reported and communicated to the right people (identified by "who needs which protocols").
- The framework also gives examples of monitoring methods, such as checklists, questionnaires, flowcharts, benchmarks, etc.

8. Documentation and Reporting

- In COSO-ERM, reporting is considered as one of the key elements for effective ERM. Hence, it is placed as one of the four objectives. The report mentions that reliable reporting supports management's decision making and monitoring activities, and is usually mandatory for external dissemination. As reporting can be considered being within the entity's control, ERM can be expected to provide reasonable assurance that reliable reporting is achieved.
- The framework does not contain a separate chapter about documentation requirements or methods, but it refers to it in some places, e.g. the Monitoring component, stating "an appropriate level of documentation usually makes evaluation more effective and efficient".

9. Budgeting and Return on Investment

- ERM permits the entity to reduce costs and losses of resources, to seize opportunities, and to improve deployment of capital, hence helping management to achieve the entity's profitability targets. Therefore, return on investment (ROI) is a key driver for COSO's enterprise risk management framework.
- COSO-ERM emphasizes the importance of making a cost-benefit analysis when choosing risk responses.

10. External Relationships

- COSO-ERM requires appropriate communication with external parties such as customers, suppliers, business partners, stakeholders, regulators, financial analysts, etc.
- COSO-ERM states that external parties contribute by actions or by providing information. Thus, it contains a chapter explaining the roles and responsibilities of each of the following external parties: external auditors,

legislators and regulators, parties interacting with the entity, outsource service providers, financial analysts, bond rating agencies, news media.

11-13. Incident, Release and Control Management

COSO-ERM does not deal with these management issues.

ISO 20000

1. Audience

The target audiences of ISO 20000 are those responsible for IT service management in the organization, including:

- The Head of Operations as the primary audience.
- The Chief Information Officer (CIO), the Business Process Owners, the Head of Development, the Head of IT Administration, the Project Management Office as the secondary audience.

2. Abstraction Level

ISO 20000 and ITIL provide best practices and guidelines for service management. The standard is on a high abstraction level, focusing on IT and services at management level, without technical specifications.

3. Objective

- Goals:

  – Deliver managed services to meet business and customer requirements.

  – Improved quality, lower costs, greater flexibility, and faster response.
- COSO-ERM objectives:
  - Delivering managed services to customers is mandatory for most companies in order to achieve their high-level strategic goals. ISO 20000's main focus is not on strategic goals, but on service management, which is a tool to attain these strategic goals.
  - Effective service management can be done through effective resource management. ISO 20000 deals with the use of the entity's resources in several places, and thus helps the company to achieve its operations' objective.
  - ISO 20000 addresses the reporting objective directly as it contains a "service reporting" process explaining general reporting requirements. Besides, different processes also state their reporting requirements, such as the "Configuration status accounting and reporting" clause under the "configuration management" process.

  - The compliance with laws and regulations is not addressed by this standard, since ISO 20000 only concerns the compliance with the agreed service levels.

4. Internal Environment

- ISO 20000 includes a section “Management responsibility” in the chapter “Requirements for a management system”, explaining that management shall provide evidence of its commitment to the development, implementation and improvement of the service management capability. The report states management’s main responsibilities. Moreover, it demonstrates the need to assign a senior level manager as responsible and accountable for the service management processes.
- Competence, awareness and training are addressed in a separate section (3.3) in the “Requirements for a management system” chapter. Moreover, training is mentioned in other places as part of a process. For example, “6.6.6 Controls” under “Information security management” in “Service delivery processes” mentions “staff with significant security roles should receive information security training”.
- ISO 20000 does not use the terms risk appetite or risk acceptance. However, in the security management process, it refers to the ISO 17799 standard; i.e. it uses the same concepts and terminology.
- ISO 20000 does not discuss internal communication.
- Concerning internal roles and responsibilities, “Allocation of roles and responsibilities” is one of the steps included in “4.2 Implement service management and provide the services”. The same step is also included in other chapters such as chapter 5 “planning and implementing new or changed services” and 4.4 “continual improvement”. The standard also advises to appoint someone responsible for important tasks. These prove that ISO 20000 emphasizes on internal roles and responsibilities in several places. However, besides management, it does not specify the roles and responsibilities of other entity personnel, like COSO-ERM.

5. Risk Analysis

- ISO 20000-1 links to ISO 17799 as a guidance on information security management. Thus, the standard does not discuss risk analysis in greater detail, just a section in ISO 20000-2 under the “Information security management” chapter. This section is on a very high level and mentions only the most important points without going far into the “what to do” and “how to do” discussion. The points mentioned are:

  – The need to identify and classify information assets,

  – Best practices about risk assessment,

  – How risks should be assessed (nature, likelihood, impact, experience)

– Which properties the risks threaten (confidentiality, integrity, availability, physical damage to service providing equipments)

– Some management controls for security.

- ISO 20000's risk analysis considers only static risks, and does not mention the steps to follow (identify, evaluate, etc.). The points mentioned above indicate that it follows ISO 17799's advices and favors, like ISO 17799, an asset-based risk analysis methodology.
- Because of its importance for service continuity, availability is given a special focus throughout the standard, compared to the other security properties (confidentiality and integrity).
- Briefly, ISO 20000's risk analysis approach is a set of simplified guidelines ("what to do") that follow ISO 17799 and does not go into detail on "how to do" aspects.

6. Control Activities

ISO 20000 presents processes to control service management. It does not contain a list of controls, like ISO 27001 and COBIT. These are management best practices and do not contain any technical details. Concerning security specific controls, ISO 20000 refers to ISO 17799.

7. Monitoring and Improvement

ISO 20000 follows the PDCA model for planning, implementing, monitoring and improving the service management. Chapter 4 in the standard, "Planning and implementing service management", describes these steps

- Section 4.3 "Monitoring, measuring, reviewing" states the need for monitoring the processes and measuring their efficiency, to review the service management requirements and its implementation and maintenance, to audit processes and record the findings of all the above.
- Section 4.4 "Continual improvement" states the need for a published policy for service improvement and to manage all suggested improvements. It also lists some activities to deal with improvements.

8. Documentation and Reporting

- Chapter 3.2 "Documentation requirements" explains the need for documentation, what aspects the documentation should include and what documents should be considered as evidence for service management planning. It states the need for a process to create and manage documents.
- Reporting is considered very important, as we can understand from this statement in chapter 6.2 "Service reporting": "The success of all service management processes is dependent on the use of the information provided in service reports." Service reporting is a process under the category of "service delivery processes". It covers reporting to customers and internal

management. Moreover, reports should contain all measurable aspects of the service, with current and historical analysis. ISO 20000 further distinguishes three types of reports: reactive (what happened), proactive (what can happen) and forward scheduled reports (what will happen) and lists what they should include. Reporting is also covered separately under other processes, such as the clause “Change management reporting, analysis and actions” under the “Change management” process.

9. Budgeting and Return on Investment

The chapter 6.4 “Budgeting and accounting for IT services” discusses the need for policies and processes (budgeting and accounting) to handle cost related issues, in order to be able to deliver services. Besides, ISO 20000 states that decisions about service provision should be based on cost effectiveness comparisons.

10. External Relationships

- Chapter 7 “Relationship processes” discusses the management of relationships with customers and suppliers, based on how to understand the customer and how to manage suppliers. Its focus is on the establishment of Service Level Agreements.
- Communication with external parties is also explained in the chapter “Relationship processes”.
- ISO 20000 does not contain a discussion about the roles and responsibilities of external parties.

11. Incident Management

ISO 20000 deals with “incidents” in chapter 8.2 “Incident management”, in a broader sense than ISO 27001, not limiting itself to security incidents. The goal is to restore agreed service to customers as soon as possible. The chapter describes the need to record incidents, establish procedures to deal with them, inform the customer, and provide necessary access to the staff responsible for incident management.

12. Release Management

Chapter 10 deals with “Release process”, explaining the basic requirements: the need for a policy, planning releases and roll-outs, using in-house or external software, and verifying and accepting releases, etc.

13. Control Management

- ISO 20000 deals with “Configuration management” in chapter 9.1. It states that all configuration items (assets) should be identified and defined, controlled, recorded, verified, and audited.

- ISO 20000 presents best practices for managing changes in its “change management” process in order to ensure that all changes are assessed, approved, implemented and reviewed in a controlled manner.

ISO 27001

1. Audience

The report targets people in the organization who are responsible for the initiation, implementation or maintaining of information security. This includes:

- The Chief Information Officer (CIO), the Chief Architect, the Head of Development, the Head of IT Administration, Compliance, audit, risk and security people as the primary audience; and
- The Chief Executive Officer (CEO), the Business Executive, the Business Process Owner, and the Head of Operations as the secondary audience.

2. Abstraction Level

ISO 27001 is on a relatively high abstraction level, defining the requirements for an Information Security Management System. ISO 17799:2005, also on a quite high abstraction level, provides implementation guidance for ISO 27001 that can be used when designing controls. They are concerned about security-specific management guidelines, without any technical specification. Hence, it is considered to be on a lower abstraction level than COSO-ERM.

3. Objective

- Goals:

  – Provide a “Guideline for implementing information security”.

  – The standard aims at providing a model for establishing, implementing, operating, reviewing, maintaining and improving a documented Information Security Management System within the context of business risks.

- COSO-ERM Objectives:

  – ISO 27001’s objective is focused on implementing security and not on the broader strategic high-level goals. However, ultimately information security should enable business objectives, and may also be a tool towards reaching strategic objectives.

  – ISO 27001 is concerned about the security of assets (e.g. category 9.2 “Equipment security” to prevent loss, theft or damage of assets) and their secure use. This helps the entity to reach its operations objectives.

  – ISO 27001 contributes to the reporting objective by reporting security events and weaknesses, and to the compliance objective with the control category “A.15 Compliance”.

4. Internal Environment

ISO 27001 deals with internal environment issues as presented below:

- The importance of management involvement and commitment is explained in "Control 6.1.1 Management commitment to information security". This control is under the category "Internal organization", dealing with the management security within the organization. In addition, in chapter 5 the report includes "Management responsibility" that states that management should provide evidence of its commitment to the whole process.
- This chapter also deals with training and awareness under the "Section 5.2.2 Training, awareness and competence". Moreover, the control categories 8.1 "Prior to employment" and 8.2 "During employment" ensure that employees always have the required level of knowledge and skills to conduct the ISMS. Control category 8.2 states that management is responsible that "…an adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities should be provided to all employees".
- In ISO 27001, the risk appetite and risk tolerance concepts are translated as "risk acceptance criteria", which has to be defined during the "Establish the ISMS" phase.
- Internal communication is analyzed from a security perspective, dealing with the reporting of security events, in control 13.1 "Reporting information security events and weaknesses".
- Apart from the management roles and responsibilities, the controls presented in the standard address other roles and responsibilities in the internal organization. Categories 7.1 "Responsibility for assets", 8.2 "During employment", 10.1 "Operational procedures and responsibilities", 11.3 "User responsibilities" are some of the categories that contain controls with regard to roles and responsibilities.

5. Risk Analysis

- Defining the risk assessment approach of the organization is one of the first steps in establishing and managing the ISMS. This includes:

  – Identifying a risk assessment methodology,

  – Develop risk acceptance criteria and identify the acceptable risk levels
- Then, with the chosen methodology, the main steps to follow are:

  – Identify risks: Asset -> threat -> vulnerability -> impact on asset

  – Analyze and evaluate risks: Business impact, likelihood -> "level" of risk

  – Identify and evaluate treatment options: Control, accept, avoid, and transfer

  – Select control objectives and controls for treatment

- After management approval, the decisions are implemented in the next phase “Implement and operate the ISMS”.
- ISO 27001 does not mandate any specific methodology. Like COSO-ERM, it tells “what” has to be done, and not “how” to do it. The “what” of these two standards are similar in general; however there are some differences:

  – COSO-ERM uses an event-based risk identification approach where the risk assessment starts by finding events, while ISO 27001 uses asset-based risk identification where the process starts by identifying assets and threats related to them.

  – COSO-ERM looks at both risks (events with a negative result) and opportunities (events with positive results), while ISO 27001 is focused on static risks that threaten the security of assets.

  – The risk evaluation and response phases of the two standards propose the same approach with the same evaluation criteria (impact and likelihood) and the same responses.

6. Control Activities

The standard presents an annex of 133 controls classified under 39 categories under 11 security control clauses. These are completely security-oriented controls, describing what has to be done to obtain good security. It provides management with guidelines but not with technical specifications, services or mechanisms. For example, control 12.2.3 suggests to “identify requirements for authenticity and integrity and acquire and implement appropriate controls”, but it does not specify any method or algorithm to use for this purpose.

7. Monitoring and Improvement

- The last two steps of the PDCA model for ISO 27001 are “Monitor and review the ISMS” and “Maintain and improve the ISMS” which are explained in detail in the report.

  – Monitoring and reviewing includes installing procedures to execute monitoring and reviewing, performing reviews of the effectiveness of the ISMS and the controls, reviewing the risk assessment and risk acceptance levels. These should be supported by regular internal audits and management reviews of the ISMS explained further in two different chapters.

  – The Maintain and improve step includes implementing the improvements that were identified in the previous step, communicating them to the interested parties and ensuring that they will reach their objectives.

- The standard includes a chapter about internal ISMS audits, with information on what should be done and recommending ISO 19011:2002 (Guidelines for quality and/or environmental management systems auditing) as an audit guideline. It also includes the chapter “Management review of the ISMS” stating the desired inputs and outputs of this review.
- The report also contains the chapter “ISMS improvement” dictating the need of continued improvement by corrective and preventive actions. Both corrective and preventive actions should follow this basic procedure: Identify nonconformities -> Evaluate the need for action -> Determine and implement the action -> Record results -> Review the action. The priority of preventive actions should be based on risk assessments.

8. Documentation and Reporting

- Chapter 4.3 “Documentation requirements” explains what the ISMS documentation should include, and how documents and records should be controlled. The extent of documentation can differ from one organization to another, and documents and records can be in any form of medium.
- ISO 27001 is concerned with the reporting of security related issues. The controls A.13.1.1 “Reporting information security events” and A.13.1.2 “Reporting security weaknesses” deal with this duty.

9. Budgeting and Return on Investment

Under “Chapter 5.2 Resource management”, management is held responsible for providing resources necessary for everything related to the ISMS. As for the rest, the report does not contain any cost-related discussions. It does not mention the costs related to ISMS, the cost implications of security, or the return on investment from security and ISMS.

10. External Relationships

- External relationships are very important from a security point of view. Hence, ISO 27001 contains many controls addressing this issue. Category 6.2, “External parties”, deals with identifying risks related to external parties, addressing security with customers and 3rd party agreements. Also, control 11.4.2 deals with “User authentication for external connections”, and 10.8 with “Exchange of information” with external entities.
- Communication with external parties is covered in particular in the control category “External parties”.
- Management has to consider feedback from external parties during the “management review of the ISMS”, thus influencing the improvement of the ISMS. External parties (“Interested parties”) are considered as an input to the PDCA process model of ISO 27001.
- ISO 27001 does not explicitly list the roles and responsibilities of external parties.

11. Incident Management

Incident management is addressed in ISO 27001 by the Category 13.2 “Management of Information Security Incidents and Improvement”. Controls state the need to establish responsibilities and procedures, learn from security incidents, and collect evidence.

12. Release Management

ISO 27001 does not deal with release management.

13. Control Management

- Configuration management is addressed in ISO 27001 under the clause 7 “Asset Management”, which contains the categories “Responsibility for assets” and “Information classification”. A “configuration item” of ISO 20000 is called an “asset” in this standard. These categories contain controls to keep an inventory of assets, assign owners, define acceptable use, classify information, label and handle it.

- ISO 27001 contains the control A.10.1.2 “Change management”, stating that changes to information processing facilities and systems should be controlled. Its requirements are basically the same, but not as detailed, as ISO 20000. ISO 27001 emphasizes that security impacts should be part of the assessment of potential impacts of the change.

The Security Architecture

1. Audience

The architecture addresses security experts. However, the first part of the architecture also contains information about the “costs for security”, usually of concern to management.

2. Abstraction Level

The architecture consists of two parts: the first part describes the model on a fairly high abstraction level; and the second part contains the technical description of the security services and mechanisms. When comparing with the other standards, the Security Architecture is technically on a lower level.

3. Objective

- Goal: Install appropriate services and mechanisms in order to reach uniform security by meeting weaknesses equivalently, independently of the IT area.
- COSO-ERM Objectives: The model informs how to provide security to the entity to reach its high level goals. It is not linked by itself to the COSO-

ERM strategic, operational, reporting and compliance objectives, but it provides the low level support to reach each of them.

4. Internal Environment

The Security Architecture contains the security service "Organization and Administration" dealing with the following internal environment issues:

- Management commitment
- Competence, awareness, training
- Internal roles and responsibilities

5. Risk Analysis

The architecture does not include a risk analysis approach. It focuses on addressing the risks that have been previously identified. Its success depends on a good risk analysis methodology. (For example, the determination of the security domain is done following the results of risk analysis in the organization.)

6. Control Activities

- The architecture includes physical, logical and administrative security services and mechanisms. These meet threats from the same three areas (physical, logical, administrative).
- Services can protect one or more of the security properties (CIA).
- Services and mechanisms from different areas can be combined, and sometimes should be, to provide more cost-effective solutions.
- Mechanisms aim for prevention, restoration, detection, warning or restoration.
- The architecture defines rules for communication between security domains to prevent a domain from communicating on a domain on a higher level.

7. Monitoring and Improvement

The Security Architecture deals with the monitoring of its security mechanisms in the security service "Organizational and administrative security management".

8. Documentation and Reporting

The Security Architecture requires the documentation and reporting of security mechanisms.

9. Budgeting and Return on Investment

The architecture includes the chapter, "Costs for security", highlighting the following:

- Risk management is about weighting the costs for security against the costs of possible damages.
- The four security levels help to make cost-effective RM decisions.
- It distinguished between two types of costs:

  - Direct costs: the cost of buying, developing, installing, administrating, training and maintaining of security mechanisms.

  - Indirect costs: Security vs Flexibility, i.e. the effect of security services on the organization’s flexibility.

10. External Relationships

The Security Architecture does not discuss external relationships although the provided services and mechanisms are dealing with the control of risks originating from the external environment.

11. Incident Management

The Security Architecture deals with incident management in the security service “Organization and administration”.

12. Release Management

The Security Architecture does not discuss release management.

13. Control Management

The Security Architecture deals with control management issues in its security service “Organization and administration”:

- Configuration management is handled in “Installation and configuration”.
- Change management is handled in “Installation and configuration”, but is limited to patch management.

COBIT

1. Audience

COBIT addresses all types of organizations, public and private companies, and external assurance and advisory professionals. Within the organization, COBIT supports management (executive management and boards, business and IT management) as well as auditors and governance, assurance, control and security professionals. The primary and secondary audiences are:

- The Business executive, the Chief Information Officer, the Business process owner, compliance, audit, risk and security people are the primary audience.
- The Chief Executive Officer, the Chief Financial Officer, the Heads of Operations, the Chief architect, the Head of development, the Head of IT

administration, and the Project management office are the secondary audience.

2. Abstraction Level

COBIT is a framework for IT Governance, presenting “control objectives for IT”. Accordingly, it deals with a very large spectrum of IT-related tasks, focusing on IT management duties. The control objectives aim to list tasks to be completed, being as complete as possible, but not providing any technical specification. It is consequently on a high abstraction level compared to the other standards except COSO-ERM. However, COBIT is focused on IT governance while COSO-ERM is concerned with corporate governance, which is a broader concept.

3. Objective

- Goals:

  – The COBIT mission is “to research, develop, publicize and promote an authoritative, up-to-date, internationally accepted IT governance control framework for adoption by enterprises and day-to-day use by business managers, IT professionals and assurance professionals”

  – A framework for IT Governance, so that IT is aligned with the business, enables the business and maximizes benefits, uses resources in a responsible way, and manages risks appropriately.

  – Main characteristics: business-focused, process-oriented, controls-based, and measurement-driven.

- COSO-ERM Objectives:

  – COBIT is based on the principle of providing the information the organization needs to achieve its high-level objectives. Hence, it does not deal with strategic goals directly, but aims to align IT governance objectives with high level strategic (business) objectives. In other terms, it deals with “strategic IT goals”.

  – COBIT deals directly with the efficient and responsible use of IT resources and is therefore directly supporting COSO-ERM’s operations objective.

  – Documentation and reporting are not objectives or controls by themselves, but documentation and reporting requirements are clearly stated for each process, thus complying with the reporting objective of COSO-ERM.

  – COBIT contains a high level objective “ME3[26] Ensure Regulatory Compliance” that deals directly with COSO-ERM’s compliance objective.

4. Internal Environment

- Management roles and responsibilities are explained separately in each high level objective in a RACI[27] chart showing who is Responsible for,

[26] Monitor and Evaluate phase.

Accountable for, Consulted and/or Informed of each activity. Other than that, COBIT does not contain a section explaining management commitment.

- Control objective PO9[28] "Assess and manage IT risks" goal is to align risks to an acceptable level of tolerance. The concept of risk appetite and tolerance are a part of the framework.
- Competence, awareness and training are dealt with in two places in COBIT. First, PO6 "Communicate Management Aims and Direction" states the need to ensure that awareness and understanding of business and IT objectives and direction are communicated throughout the enterprise. Secondly, PO7.4 "Personnel Training" is another control to maintain the knowledge, skills, abilities and security awareness of entity personnel.
- Internal communication is covered in several points:

  – Each high-level control has a "RACI chart" explaining who must be consulted or informed about the process.

  – Some controls state explicitly the need to communicate some information. For instance, PO6 "Communicate Management Aims and Direction" is all about communication, while PO4.6 "Roles and responsibilities" mentions that roles and responsibilities have to be communicated.

  – Communication is also part of the Maturity Attribute Table measuring the communication in the entity with a scale from 1 (Sporadic communication) to 5 (Proactive communication based on trends, mature communication techniques, integrated communication tools)
- Roles and Responsibilities is a generic control requirement, i.e.it has to be applied to all the processes in the framework. This control states that unambiguous roles, activities and responsibilities have to be defined for each COBIT process for its efficient execution. Also, generic control PC1 "Process owner" necessitates that every process has an owner. Moreover, some processes have detailed control objectives about this issue, such as PO4 containing PO4.6 "Roles and Responsibilities", or these detailed control objectives mention, among other requirements, the need to define and communicate roles and responsibilities.

5. Risk Analysis

The COBIT's risk analysis approach is presented in the high level control objective PO9 "Assess and Manage IT Risks", which promotes the creation and maintenance of a risk management framework. According to this, the main steps are:

- Create and integrate the risk management framework with the business and operational risk management framework. Align with the organizations risk appetite and tolerance.

[27] Responsible, Accountable, Consulted, Informed.

[28] Plan and Organize phase.

- Establish risk context (for each risk assessment, define the internal and external context, the goal and the risk evaluation criteria).
- Identify events (threat and vulnerability). Determine the nature of the impact (positive, negative).
- Assess risks: likelihood and impact, inherent and residual risks, portfolio view.
- Risk response: avoid, reduce, share or accept. Cost-effective control decisions.
- Implement, maintain and monitor risk action plan.

The definition of the risk analysis approach is almost the same as COSO-ERM's. It considers both risks and opportunities and proposes the same responses. Again, it does not specify any risk methodology, but it states the requirements. However, it proposes useful ways of measuring the effectiveness of the risk management framework.

6. Control Activities

- COBIT distinguishes between two kinds of controls: general IT controls in IT processes and services, as security, change management, systems development; and application controls in business process applications, as authorization, segregation of duties, completeness.
- COBIT IT processes cover general IT controls, not application controls. However, it provides a list of recommended application control objectives. The list contains 18 controls under five categories: Data origination/ authorization controls, data input controls, data processing controls, data output controls, and boundary controls.
- The rest of COBIT deals with general controls, presenting 34 high-level objectives (or processes) containing 215 control objectives, categorized under four domains: Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS), Monitor and Evaluate (ME). These are defined as "the minimum requirements for effective control of the process" and contain "policies, procedures, practices and organizational structures to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected".
- Besides the 215 control objectives, COBIT also presents six "general control requirements" that apply to each of the processes together with the other controls. These are PC1, Process Owner; PC2, Repeatability; PC3, Goals and Objectives; PC4, Roles and Responsibilities; PC5, Process Performance; and PC6, Policy, Plans and Procedures.
- These controls include some high-level control objectives related to security. Examples are PO9, Assess and manage IT risks, and DS5, Ensure systems security. Other high-level control objectives also include controls that are related to security. PO7.4 covers "Personnel Training" for security awareness

of entity personnel, and PO4.8, “Responsibility for Risk, security and compliance”.

7. Monitoring and Improvement

One of the four characteristics of COBIT is that it is measurement-driven. Measurement is realized at two levels: Maturity models and performance measurement:

- Maturity models measure the capability (and not the performance) of processes with a scale of five maturity levels supplemented with maturity attributes. The levels help the entity understand “where they are”, “where the industry is” and “where they want to go”. The report contains, for each high-level control objective (each process), a maturity model describing what the organization should be capable to do at each level (in relation to that process activities).
- Performance measurement is realized in three levels: IT Goals and Metrics, Process goals and metrics, and Activity goals and metrics (process performance). The high-level control objective’s performance is measured with Key Goal Indicators and Key Performance Indicators provided by COBIT for each process.
- The COBIT Framework includes a phase in the whole cycle (corresponding to a process domain), named “Monitor and Evaluate” that manages the monitoring and evaluation of IT performance and internal control, ensuring regulatory compliance and providing IT governance.
- Processes and controls are improved by utilizing maturity models and performance measurement, while the improvement of the organization’s IT governance follows from the monitoring and evaluation phase. However, it is clear that these two issues are related.

8. Documentation and Reporting

- COBIT does not contain a separate chapter explaining the documentation or reporting requirements. However, for each high-level control objective a list of outputs to other processes is provided with information what should be documentated or reported for each process. For instance PO5, “Manage the IT investment”, lists cost and benefits reports as an output for other processes.
- The detailed control objectives state documentation and reporting requirements, if specifically needed. For example PO 5.4, “Cost management”, states that costs should be monitored and reported, while PO9.6, “Maintenance and monitoring of a risk action plan,” requires that any deviations from the execution of the plan should be reported to the executive management.

9. Budgeting and Return on Investment

- Budgeting is handled in the following control objectives: PO5, Manage the IT investment; AI5, Procure IT resources; and DS6, Identify and Allocate costs.
- COBIT analyses the return of investment by posing the question "How far should we go, and is the cost justified by the benefit?". The response is provided in the Management Guidelines of COBIT, addressing management concerns such as:

  – What are the indicators of good performance? (Performance measurement)

  – What are the critical success factors for control? (IT control profiling)

  – What are the risks of not achieving objectives? (Awareness)

  – What do others do? (Benchmarking)

  COBIT Management Guidelines helps answering these questions by defining maturity models (benchmarking), performance indicators and critical success factors for each high level control objective.

10. External Relationships

- DS1, "Define and manage service levels", defines the needs for effective communication and documentation regarding services and agreed service levels with customers. It includes controls of: defining a framework for service level management, defining services, defining service level agreements, ensuring the operation of level agreements, monitoring and reporting service level achievements, and reviewing SLAs and contracts.
- DS2, "Manage third-party services", is another process addressing the management of suppliers. It covers identifying relations, managing relationships, managing supplier risks, and monitoring supplier performance.
- Also, DS5 "Ensure systems security", covers external relationships from a security point of view, stating needs for identity management and user account management concerning external users.
- ME2.6, "Internal control at third parties", is another example of a control of external relationships, assessing the status of external parties' internal controls.

11. Incident Management

COBIT deals with incident management in the process DS8, "Manage Service desk and incidents". The requirements stated are to establish: a service desk, a system to register customer queries, procedures to handle incident escalation, procedures for incident closure, and reports about trends to enable measurement and improvement.

12. Release Management

AI7, “Install and Accredit solutions and changes”, includes the control “Software release”. It sets the requirements to fulfill before releasing a product, including sign-off, packaging, testing, distributing, etc.

13. Control Management

- The high level control objective AI6, “Manage Changes”, deals with everything related to change management. It states that all changes, including emergency maintenance and patches, should be logged, assessed, and authorized prior to implementation. All changes shall be reviewed afterwards.
- Objective DS9, “Manage the configuration”, requires the establishment of a repository for configuration items, identifying and maintaining them, and reviewing their integrity status.

Section III. Gap-overlap analysis

Based on the results of the protocol analysis in the previous section, this section identifies the relation between COSO-ERM, ISO 20000, ISO 27001 and Security Architecture in terms of gaps and overlaps.

1. Audience

The audience for the framework and standards differ. COSO-ERM's target group is primarily the board of directors and the senior management. ISO 20000's and ISO 27001's primary audiences are service and security managers respectively. The Security Architecture requires technical competence, and its main audience is security system engineers. (See figure 6.)

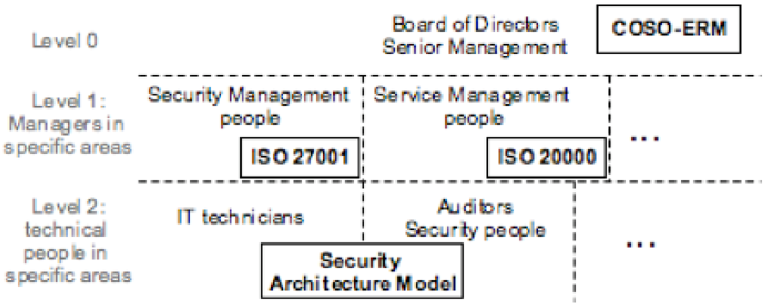

Level 0
Board of Directors
Senior Management
COSO-ERM
Level 1: Managers in specific areas
Security Management people
ISO 27001
Service Management people
ISO 20000
...
Level 2: technical people in specific areas
IT technicians
Auditors
Security people
Security Architecture Model
...

Figure 6: Audiences

A well defined audience is important. For example, senior managers will probably not read ISO standards. However, most Chief Information Security Officers (CISO) appreciate the need to have at least some understanding of ISO 27001. Nevertheless, only a few will spend time on technical details in the architecture. After the CISO have decided on the appropriate risk responses in ISO 27001 (in dialogue with line managers and the senior management), the implementation of security services and mechanisms in the Security Architecture is left to security engineers to be decided on. Higher levels require feedback of the results from lower levels, but they are probably less interested in operational and technical details.

2. Abstraction Level

The abstraction level of the standards and frameworks are illustrated in two dimensions (see figure 7). The horizontal axis refers to the broadness of the documents: how broad is the addressed subject? The vertical axis refers to its profundity: how detailed is the document in terms of technical or operational profundity?

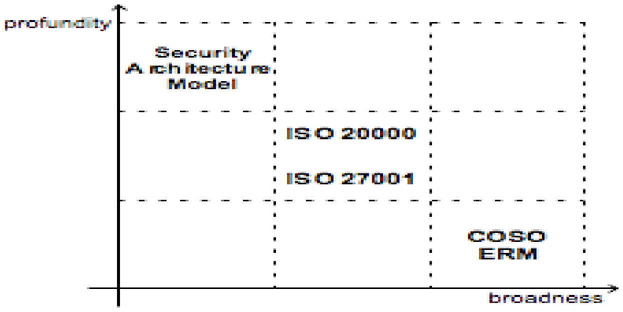


Figure 7: Abstraction levels

COSO-ERM covers the broadest area of corporate governance but does not provide technical or operational guidance. ISO 27001 and ISO 20000 are more specific in their areas, security management and service management, and provide implementation guidance. Hence, there is a gap between the very high level of abstraction of COSO-ERM and the lower level of abstraction of ISO 20000 and ISO 27001. COSO-ERM and the Security Architecture are in the both extremes of the graph; a “hand-shake” between them would by no means be possible.

3. Objective

As COSO-ERM is on a higher level, the other standards objectives do often not map directly to the four objectives, but support them in their specific field. For example, to be able to reach the high level strategic goals, it is required (of the Company) to reach the “Services management goals” (ISO 20000), and “Security goals” (ISO 27001 and the Security Architecture). There is a natural gap between their main objectives, but combining them allows getting closer to the COSO-ERM objectives. However, what is further required is a low level mapping between COSO-ERM objectives and controls and processes presented by the other standards. For example, the “Reporting” objective of COSO-ERM could be translated to reporting controls in specific topics, such as ISO 27001’s “Reporting of information security events” and ISO 20000’s “Service reporting”.

4. Internal Environment

Risk appetite (or “risk acceptance criteria”) is analyzed in COSO-ERM and ISO 27001. They use the same definition and emphasize its importance. All standards and frameworks express the importance of “Management Commitment”. The standards and frameworks cover “Competence, Awareness, and Training”. For instance, both ISO 27001 and ISO 20000 cover “competence, awareness, and training” requirements within each standards area of competence. All standards and frameworks cover “Internal Communication”, except ISO 20000, as its focus is on communication with external parties, customers and suppliers.

“Internal Roles and Responsibilities” are defined in COSO-ERM, ISO 20000 and ISO 27001, underlining the roles and responsibilities of entity personnel for the correct functioning of the management systems. The Security Architecture contains, in its security service “Organization and Administration”, the necessary services and mechanisms to support the implementation of these requirements set by the other standards. (See table 1.)

	COSO-ERM	ISO 20000	ISO 27001	Sec. Arch.
Risk appetite	Yes	No	Yes	No
Management Commitment	Yes	Yes	Yes	Yes
Competence, Awareness, Training	Yes	Yes	Yes	Yes
Internal Communication	Yes	No	Yes	Yes
Internal Roles & Responsibilities	Yes	Yes	Yes	Yes

Table 1: Internal Environment

5. Risk Analysis

Table 2 summarizes the answers to the following questions:

– Does the framework or standard provide a risk analysis approach?

– Does it specify a risk analysis methodology?

– Does it consider risks or opportunities (or both)?

– Are risks identified from the assets perspective or from events?

	COSO-ERM	ISO 20000	ISO 27001	Sec. Arch.
Approach description	Yes	No	Yes	No
Specific methodology	No	No	No	No
Risks/Opportunities	Both	No	Risks	No
Assets/Events	Event	No	Asset	No

Table 2: Risk Analysis

COSO-ERM and ISO 27001 are the two standards that contain sections about risk analysis. They both align with the risk appetite and propose the same risk responses and risk assessment steps. However, there are important differences between their risk analysis approaches. ISO 27001 considers risks while COSO-ERM considers both risks and opportunities. The reason is probably that information security (ISO 27001) is a static risk by nature. COSO-ERM has a dynamic risk approach covering both “opportunities “and “risks”.

Another difference is ISO 27001's "asset-based" risk identification compared to COSO-ERM's "event-based" identification of risk. This difference emanates from the different audiences. COSO-ERM is at business level, dealing with events that may result in both risks and opportunities. Opportunities can be identified from events, but hardly from assets. ISO 27001, on the other hand, is at information systems level, protecting information assets.

Neither COSO-ERM nor ISO 27001 specify a methodology for risk assessment; they account for the basic steps and leave the choice to the organization. While the Security Architecture does not contain a risk analysis approach, it bases its decisions (such as the determination of security domains, the 4 security levels) on results from risk assessments.

6. Control Activities

Table 3 summarizes the answers to the following questions:

– Does the framework or standard address High Level Measures (HLM) or Technical Services and Mechanisms (TSM)?

– Which area (general, services, or security) do the controls relate to?

– Does the framework or standard provide an exhaustive list of controls for its area?

	COSO-ERM	ISO 20000	ISO 27001	Sec. Arch.
HLM or TSM	HLM	HLM	HLM	TSM
Area	General	Services	Security	Security
List of controls	No	Yes	Yes	Yes

Table 3: Control Activities

Together, ISO 20000, ISO 27001 and the Security Architecture provide IT services and security controls, including HLM and TSM. They do not conflict; on the contrary, they complement each other. Nevertheless, corporate governance goals are best translated with COSO-ERM objectives. To be able to "control governance", there must be a link between the objectives and controls from the service and security areas to COSO-ERM. Since COSO-ERM does not provide a list of controls, the "link" is missing.

The Company can, of course, implement ISO 20000 and ISO 27001, and obtain acceptable assurance for its service and security management. However, this will not assure the fulfillment of the COSO-ERM (and SOX, Section 404) objectives.

7. Monitoring and Improvement

Monitoring is one of the eight components in COSO-ERM, while ISO 27001 and ISO 20000 consider it as a phase in their model cycle. COSO-ERM monitors its eight components. ISO 20000 monitors its service management processes, ISO 27001 monitors its Information Security Management System (ISMS), and the Security Architecture monitors its security mechanisms. (See table 4.)

	COSO-ERM	ISO 20000	ISO 27001	Sec. Arch.
Monitoring and Improvement	Components	Processes	ISMS	Mechanism

Table 4: Monitoring

By constant surveillance, the Company can detect problems, correct and improve the controls or processes in each of the frameworks and standards. The challenge is to monitor the whole Company. Separately monitoring of the different standards and framework is not a solution. COSO-ERM does not provide any benchmarking tools; there is a need for a tool to measure the whole organization's capability and to monitor its high level objectives.

8. Documentation and Reporting

COSO-ERM proposes to document without stating requirements, but both ISO 20000 and ISO 27001 contain a section in their report describing the documentation requirements. (See table 5.)

Reporting is one of the four objectives of COSO-ERM. Reporting processes in ISO 20000 must be in written form. ISO 27001 uses the word "reporting" embedded in two controls: "reporting information security events" and "reporting information security weaknesses". None require a written report. The Security Architecture requires documentation and reporting concerning the security mechanisms. (See table 5.)

	COSO-ERM	ISO 20000	ISO 27001	Sec. Arch.
Documentation	No	Yes	Yes	Yes
Reporting	Yes	Yes	Yes	Yes

Table 5: Documentation and Reporting

The different standards and frameworks have different requirements concerning documentation and reporting, and there is no single approach to unite them.

9. Budgeting and Return On Investment

Table 6 summarizes the answers to the following questions:

– Is budgeting and costs managed by a process, and have responsibilities for investments and operative costs been assigned?

– Is Return on Investment (ROI) covered?

– Is it possible for management to measure ROI?

	COSO-ERM	ISO 20000	ISO 27001	Sec.Arch
Budget	No	Yes	Yes	No
ROI discussion	Yes	No	No	Yes
ROI calculation	No	No	No	No

Table 6: Budgeting and ROI

COSO-ERM and the Security Architecture are “ROI-aware”. They present ROI as a driver for management decisions. However, none of them outline a way for management to calculate or measure ROI.

ISO 20000 defines the process “Budgeting and accounting”, which manages issues related to budgeting and costs. ISO 27001 does not include separately defined processes. Instead it is included, to some extent, in the provision of resources, in “Resource management”, as a management responsibility. The difference in approach for cost management, together with the absence of a central point for budget control, is confusing (for the Company).

10. External Relationships

COSO-ERM mentions two aspects of relationships with external parties: the communication itself, and the roles and responsibilities for the communication. COSO-ERM states the need for good communication with external parties, such as customers, suppliers, business partners, stakeholders, regulators, and financial analysts. Nevertheless, COSO-ERM does not provide any help or guidance on how to realize this requirement. Roles and responsibilities are however covered in a separate chapter. These discussions provide guidance for an organization (as the Company) in understanding the needs, but the organization still needs to install controls to ensure that these requirements are met.

ISO 20000 and ISO 27001 provide some of these controls. ISO 20000 provides processes to manage the communication regarding services with customers and suppliers. ISO 27001 elaborates on the relationships on security issues with customers and suppliers. (See table 7.)

	COSO-ERM	ISO 20000	ISO 27001	Sec. Arch.
Communication	No	Yes	Yes	No
Roles & Responsibilities	Yes	No	No	No

Table 7: External Relationships

11. Incident Management

ISO 27001 elaborates on the relationships on security issues with customers and suppliers. However, both ISO 27001 and the Security Architecture focus exclusively on security incidents, while ISO 20000 deals with incidents on a broader level. ISO

20000 encompasses all kinds of incidents that might interrupt the agreed service level.

An almost complete incident and security management system would be the result of integration between ISO 20000 and 27001, supported by mechanisms from the Security Architecture. Nevertheless, there is still a gap to COSO-ERM. (See table 8.)

	COSO-ERM	ISO 20000	ISO 27001	Sec. Arch.
Incident Management	No	Yes	Yes	Yes

Table 8: Incident Management

12. Release Management

ISO 20000 is the only standard covering release management (see table 9).

	COSO-ERM	ISO 20000	ISO 27001	Sec. Arch.
Release Management	No	Yes	No	No

Table 9: Release Management

13. Control Management

Table 10 shows which standards and frameworks that cover the two control management issues: configuration management and change management.

	COSO-ERM	ISO 20000	ISO 27001	Sec. Arch.
Configuration	No	Yes	Yes	Yes
Change	No	Yes	Yes	Yes

Table 10: Control Management

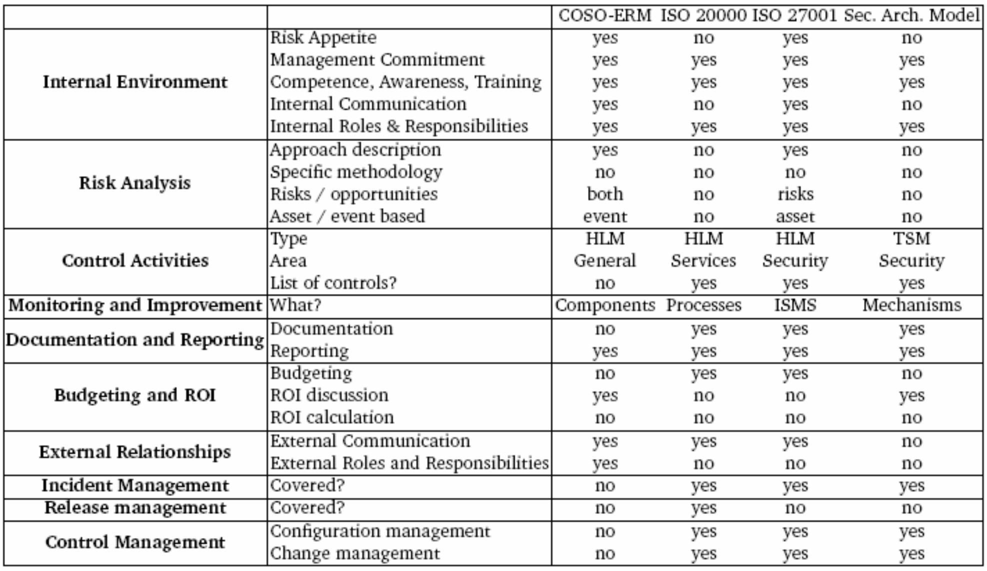
ISO 20000 and ISO 27001 do not conflict in their configuration management requirements, but ISO 27001 includes the need to assign responsibilities for assets.

ISO 27001 states the same change management requirements as ISO 20000, but less detailed, emphasizing that security impacts should be taken into consideration when estimating the impact of change.

The Security Architecture analyzes configuration and change management in the security service “Organization and Administration”, under the “Installation and Configuration” section. However, change management is limited to “patch management”.

14. Summary

A summary of the Gap – overlap analysis is presented in table 11.



		COSO-ERM	ISO 20000	ISO 27001	Sec. Arch. Model
Internal Environment	Risk Appetite	yes	no	yes	no
	Management Commitment	yes	yes	yes	yes
	Competence, Awareness, Training	yes	yes	yes	yes
	Internal Communication	yes	no	yes	no
	Internal Roles & Responsibilities	yes	yes	yes	yes
Risk Analysis	Approach description	yes	no	yes	no
	Specific methodology	no	no	no	no
	Risks / opportunities	both	no	risks	no
	Asset / event based	event	no	asset	no
Control Activities	Type	HLM	HLM	HLM	TSM
	Area	General	Services	Security	Security
	List of controls?	no	yes	yes	yes
Monitoring and Improvement	What?	Components	Processes	ISMS	Mechanisms
Documentation and Reporting	Documentation	no	yes	yes	yes
	Reporting	yes	yes	yes	yes
Budgeting and ROI	Budgeting	no	yes	yes	no
	ROI discussion	yes	no	no	yes
	ROI calculation	no	no	no	no
External Relationships	External Communication	yes	yes	yes	no
	External Roles and Responsibilities	yes	no	no	no
Incident Management	Covered?	no	yes	yes	yes
Release management	Covered?	no	yes	no	no
Control Management	Configuration management	no	yes	yes	yes
	Change management	no	yes	yes	yes

Table 11: Summary

Section IV. COBIT as a potential facilitator

When using COBIT, there is often a misunderstanding that COBIT should either be implemented entirely or not at all. This is addressed by COBIT Implementation Tool Set: “COBIT is a framework that must be tailored to the organization. For example, COBITs IT processes must be compared to the organization’s existing processes, the organization’s risks must be reviewed, and responsibilities for the IT processes must be established. Organizations will in many cases need to customize this general set of guidelines to their specific environment.”[29]

The Company has two options, besides the “all” or “nothing” approaches, one of which is utilizing COBIT to implement the “Architectural view” in the Company. As indicated by the expression “architect”, COBIT provides the high level foundation for the other IT frameworks and standards; it is the first framework to be implemented with controls selected to meet the enterprise IT strategies derived from COSO-ERM objectives.

After the COBIT architecture is laid out, processes and controls from ISO 20000 and ISO 27001 are selected and mapped to COBIT controls. The next phase is to implement the standards by applying the best practices. Finally, the technical security services and mechanisms from the Security Architecture are implemented.

The second option is to use COBIT as the” Plumber”. It is then used as a tool to do the plumbing between the pre-existing standards. COBIT will provide:

- A checklist to ensure that no process requiring control has been overlooked, and to identify missing controls,
- A collection of globally accepted controls to formulate enterprise policies,
- A means of promoting other standards that already exist in the organization.

With the Plumber approach a selection of COBIT controls are “tailored” to pre-existing standards and frameworks. By applying this approach, unnecessary work can be avoided; COBIT is utilized only when there are detected gaps between COSO-ERM, ISO 20000, ISO 27001, and the Security Architecture.

To conclude, the Company has four options:

- Not to chose COBIT at all,
- Implement 100 % of COBIT,
- Using COBIT as the “architect”,
- Using COBIT as the “plumber”

[29] COBIT Implementation Tool Set, IT Governance Institute, 2005a, 2005.

To select the best option for the Company, a Gap – overlap analysis of COBIT is conducted below.

Gap-overlap analysis

1. Audience

COBIT differs from the other standards and frameworks. It provides several different reports to different audiences such as: Management Guidelines for senior managers; Audit Guideline for auditors; and a Framework for managers in charge of implementing COBIT.

Since ISO 27001 and ISO 20000 do not provide a "Management summary", senior managers are not able to understand what they should expect from these standards without reading the whole document (which is not likely). COBIT can help to close this gap with the Management Guidelines. It will provide senior managers with a tool to measure performance of the standards controls and their cost effectiveness.

2. Abstraction Level

COBIT is positioned between COSO-ERM and the standards and the architecture. It covers a much broader area (IT governance) than ISO 20000 (Service management), ISO 27001 (Security management) and the Security Architecture (Security services and mechanisms), but not surprisingly with less profundity than the standards and the architecture. (See figure 8.)

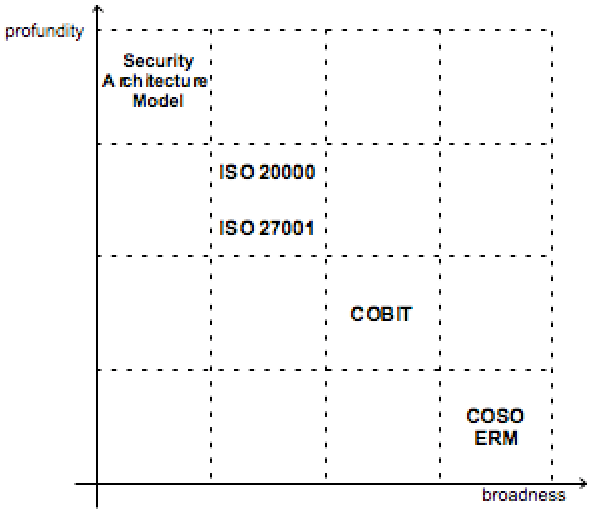


Figure 8: Abstraction Level

COBIT does not replace ISO 20000, ISO 27001, and the Security Architecture; it is not profound enough to be able to do that. Nevertheless, COBIT fulfills an obvious link between them and COSO-ERM.

3. Objectives

COBIT can be utilized as middle layers between COSO-ERM and the ISO standards. It can translate COSO-ERM objectives into more concrete controls or processes and facilitate the handshake with the standard by applying COBIT controls.

COBIT may directly integrate the Security Architecture with COSO-ERM without ISO 27001. However, this will not be done without considerable effort due to the difference between their level of abstraction, audience and objectives. It is therefore recommended that ISO 27001 is used as a layer between COBIT and the Security Architecture.

There is one significant limitation with COBIT. It is limited to IT governance. COBIT does not cover the full scope of COSO-ERM. Moreover, ISO 27001 is broader than just IT. That is the reason why there must also be a direct link between COSO-ERM and ISO 27001. (See figure 9.)

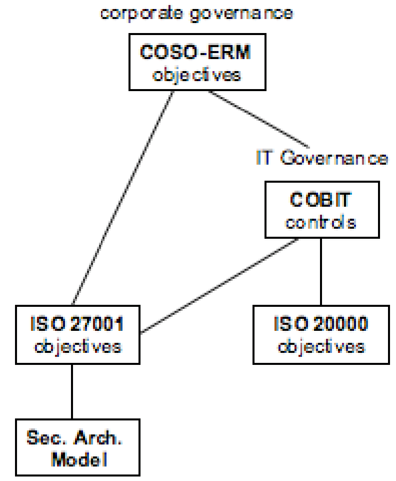


Figure 9: Linking the Frameworks and Standards

4. Internal Environment

COBIT introduces several useful tools for the “Internal environment”. The RACI chart defines, for each high level control objective, the people who are Responsible, Accountable, Consulted and Informed (RACI), introducing a consistent approach for internal roles and responsibilities.

Furthermore, “Roles and responsibilities” is a generic control requirement applied to all the processes in the framework. It requires that roles, activities and responsibilities are clearly defined for each control objective. COBIT adds another generic control, PC1, “Process owner”, requiring of every process to have an appointed owner. “Internal communication” is a part of the Maturity Attribute Table, and measures the communication capability of an organization.

There are overlaps between COBIT and the other frameworks and standards, as for instance "Management Commitment" (see table 12, pages 57). Implementing COBIT may provide consistent management of and add quality to "Management Commitment", but it may also require quite a few additional resources. The decision to adopt these COBIT requirements or not needs to be considered carefully.

5. Risk Analysis

As stated in the Gap – overlap analysis in Section III, COSO-ERM and ISO 27001 differ in risk analysis approach concerning the identification of risks (COSO-ERM is event-based, and ISO 27001 is asset-based) and their consideration of opportunities. COSO-ERM has a dynamic perspective on opportunities compared with ISO 27001, by identifying the events that could create value (as well as risks) for business. ISO 27001 is restricted to static risks.

COBIT defines risk identification in the same way as COSO-ERM, considering opportunities as well as risks, and using an event-based approach to be able to identify opportunities. The COBIT controls provide, in its risk identification, the requirements on IT systems and thereby facilitate the integration of ISO 27001 with COSO-ERM.

6. Control Activities

COBIT provides an extensive list of controls of IT, including the more specific areas like security and services, which also covers most of COSO-ERM requirements. COBIT can be used as the handshake between the COSO-ERM objectives and the controls and processes of ISO 20000 and ISO 27001[30]. This will provide reasonable assurance that COSO-ERM objectives are fulfilled. Moreover, COBIT can become a tool (a checklist) to identify gaps in the IT governance framework.

7. Monitoring and Improvement

COBIT can be used as the overall monitoring tool to assess the IT performance of COSO-ERM, ISO 20000, ISO 27001 and the Security Architecture. COBITs' methods and tools will facilitate the understanding of process performance. Moreover, the Maturity Models can help the enterprise evaluating them and to decide on future maturity goals, as well as a benchmarking tool to other organizations.

8. Documentation and Reporting

ISO 20000, ISO 27001 and the Security Architecture state all their documentation and reporting requirements. These should of course be followed to ensure compliance. COBIT may add value to these separate processes by its "inputs - outputs" table. It may provide a coherent oversight of reporting and documentation. However, implementing the table will require significant effort; it may not be cost effective.

[30] Regarding the Security Architecture, see the discussion in "3. Objectives".

9. Budgeting and Return on Investment

Budget is covered by the ISO 20000 and ISO 27001 standards, but not by the Security Architecture. If the Security Architecture is used without the higher level support of ISO 27001, COBIT could be used to control budgeting issues for the architecture.

In contrast to the other frameworks and standards, COBIT provides a way to at least estimate Return On Investment (ROI), probably one of the most important issues for the senior management. COBIT's "Management Guidelines" tries to provide management with the tools to answer the question: "How far should we go, and is the cost justified by the benefit?" The tools provided by COBIT are the maturity models, performance indicators and critical success factors (also referred to in the "Monitoring and Improvement" section).

10. External Relationships

COBIT might be used as a negotiator between ISO 20000, ISO 27001 and the Security Architecture and to establish the link between COSO- ERM and these standards. For instance, both ISO 20000 and ISO 27001 cover "External Communication, which is also an important requirement from COSO-ERM in "External Relationships".

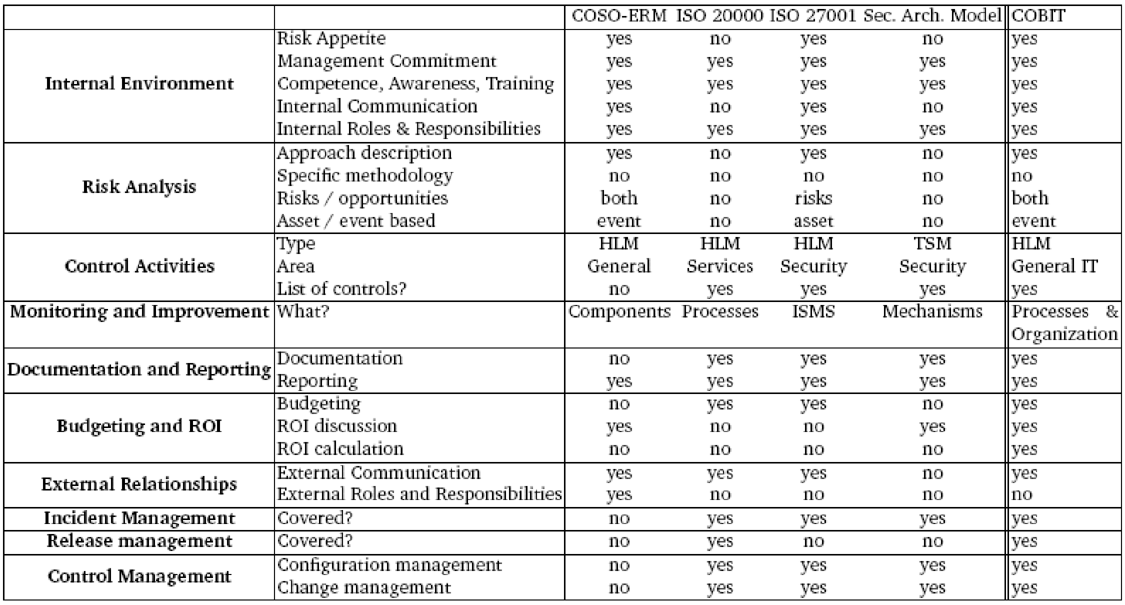
COBIT may set the control objectives, DS1, "Define and manage service levels", defining the needs for the effective communication and documentation regarding services and agreed service levels with customers. Moreover, DS5, "Ensure systems security", may be used for covering external communication regarding security.

11. Incident, Release and Control Management

Requirements for IT Incident, Release and Control management are not specified in COSO-ERM, although they are important parts of corporate governance. These requirements are covered in ISO 20000, ISO 27001, and the Security Architecture. COBIT can do the "IT-plumbing" between COSO-ERM and the standards and the architecture.

The Company's decision

The Company might choose the option to implement "100% COBIT". However, several subjects are already covered by the other standards and frameworks (see table 12); it is obvious that it would not be cost effective for the Company to implement the total framework of COBIT.



		COSO-ERM	ISO 20000	ISO 27001	Sec. Arch. Model	COBIT
Internal Environment	Risk Appetite	yes	no	yes	no	yes
	Management Commitment	yes	yes	yes	yes	yes
	Competence, Awareness, Training	yes	yes	yes	yes	yes
	Internal Communication	yes	no	yes	no	yes
	Internal Roles & Responsibilities	yes	yes	yes	yes	yes
Risk Analysis	Approach description	yes	no	yes	no	yes
	Specific methodology	no	no	no	no	no
	Risks / opportunities	both	no	risks	no	both
	Asset / event based	event	no	asset	no	event
Control Activities	Type	HLM	HLM	HLM	TSM	HLM
	Area	General	Services	Security	Security	General IT
	List of controls?	no	yes	yes	yes	yes
Monitoring and Improvement	What?	Components	Processes	ISMS	Mechanisms	Processes & Organization
Documentation and Reporting	Documentation	no	yes	yes	yes	yes
	Reporting	yes	yes	yes	yes	yes
Budgeting and ROI	Budgeting	no	yes	yes	no	yes
	ROI discussion	yes	no	no	yes	yes
	ROI calculation	no	no	no	no	yes
External Relationships	External Communication	yes	yes	yes	no	yes
	External Roles and Responsibilities	yes	no	no	no	no
Incident Management	Covered?	no	yes	yes	yes	yes
Release management	Covered?	no	yes	no	no	yes
Control Management	Configuration management	no	yes	yes	yes	yes
	Change management	no	yes	yes	yes	yes

Table 12: Gap - Overlap Analysis

The remaining implementation options, the architectural view and the Plumber, are both more viable and efficient solutions than 100 % COBIT, proposing two different approaches. Since the Company, as many other organizations, already has the required standards and frameworks, the architectural view would take a great deal of efforts and resources to implement; it would almost certainly require substantial administrative re-engineering of the existing standards and framework. The benefits would not outweigh the costs for the architectural view.

Even if the other standards or frameworks are not previously implemented, the architectural view may not be the most appropriate solution. A reason is that ISO 27001 covers a broader perspective (information security) than COBIT (IT security). Accordingly, the architectural view will not control the full spectrum of security aspects that are required of COSO-ERM.

For the Company the most appropriate option is the “Plumber” in order to identify the IT gaps between COSO-ERM, ISO 20000, ISO 27001 and the Security Architecture.

Section V. The SOX Battle

The need to guarantee transparency to companies' stakeholders increased substantially after the U.S. Congress enacted the Sarbanes-Oxley Act (SOX) on July 30, 2002. The aim with the legislation was to reinstall confidence in U.S. equity markets after the Enron scandal and the misconduct committed by Enron's auditor, Arthur Andersen.

The most discussed and controversial part of SOX is Section 404. It calls for creation and maintenance of viable internal controls defined as, "…a broad concept that extends beyond the accounting function of a company"[31]. Accordingly, internal controls include policies, procedures, training programs, and other processes beyond financial controls. Moreover, companies must document and test the adequacy of these internal process controls, and their auditors must attest them.

A - or "The" - reason behind the controversy of Section 404 is that Chief Executive Officers (CEOs) and Chief Financial Officers (CFOs) are personally and criminally liable for the quality and effectiveness of their organization's internal controls[32]. However, that has significantly boosted the executive management commitment to and involvement in Corporate Governance, at least for all public issuers subject to the U.S. SEC registration; these companies must comply with Section 404 from 2004[33]. Compliance to SOX is controlled and enforced by the SEC.

There are strong commercial forces behind the suggested changes of SOX. A summary of the two reports that are considered to be the most important in this context is presented in this section. The reports are: "Interim report of the Committee on Capital Markets Regulation"; and "Sustaining New York's and the US' Global Financial Service Leadership".

Interim report of the Committee on Capital Markets Regulation[34]

When Henry Paulson, former President and CEO of Goldman Sachs, was appointed Treasury Secretary one of the first issues he may have had on his agenda was to promote the Committee on Capital Markets Regulation, announced on September 12, 2006. The Committee composes of 22 corporate and financial leaders from the investor community, business, finance, law, accounting, and academia. Its members include the former Chairman and CEO of NASDAQ, the President and Co-COO of NYSE, the CEO of PricewaterhouseCoopers, and the CEO of Deloitte.

[31] SEC's Final Rule: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports.

[32] SEC's Final Rule: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports.

[33] Dead-line for foreign filers (as the Company in this report) was July 15, 2006. Dead-line for small companies - with less than $75 million of market capitalization - is December 15, 2007 for Section 404(a) management assessment. Implementation of auditor attestation for small companies, Section 404(b), is a year later. Investment companies are completely except from Section 404.

[34] INTERIM REPORT OF THE COMMITTEE ON CAPITAL MARKETS REGULATION, November 30, 2006.

The Committee's proclaimed purpose, "… is to explore a range of issues related to maintaining and improving the competitiveness of the U.S. capital markets". The objective, "… is to recommend policy changes that should be made, or areas of research that should be pursued, to preserve and enhance the balance between efficient and competitive capital markets and shareholder protection".

The Committee states in its interim report November 30, 2006, that: "Regulatory intensity almost inevitably increases after periods of market euphoria and the subsequent market collapse". The question they raise is: "Has the shift in intensity gone too far?"

The question above is, of course, rhetoric: it has already gone too far. The report on 152 pages explains why, and elaborates on the consequences of too much of Corporate Governance (and liability risks) for the U.S.. An example is the international market for Initial Public Offerings (IPO), a market usually dominated by the U.S. This has changed drastically according to the report: "As measured by value of IPOs, the U.S. share declined from 50 percent in 2000 to 5 percent in 2005. Measured by number of IPOs, the decline is from 37 percent in 2000 to 10 percent in 2005." The Committee states that, "…certainly one important factor contributing to this trend is the growth of U.S. regulatory compliance costs and liability risks compared to other developed and respected market centers".

Another effect of SOX is the move from the public to the private market: "In 2005, approximately 90 percent of the volume of international equity issues in the United States was done in the private market, compared with about a 50-50 split between the public and private markets in 1995." The Committee concludes that the regulatory and litigation burden is an important factor in the choice between public and private markets: "The decision to "go private" or to access the private equity markets is a further suggestion of the regulatory and liability costs and burdens of accessing the public U.S."

The Committee has investigated the cost of implementing Section 404. The price tag was $4.36 million for an average company in 2004. The total compliance cost was estimated at $15-20 billion in 2004. Although this cost is decreasing, the Committee concludes that new entrants into the U.S. public markets will still face this large initial cost.

An indication of a cornerstone in Committee's recommendations is the quote in the report of Mr. Ed Balls, Economic Secretary to the U.K. Treasury: "Our system of principles and risk-based regulation provides our financial services with a huge competitive advantage and is regarded as the best in the world."

The Committee's four key recommendations are in the following order[35]:

"1. Regulatory Process. We conclude that the SEC and self-regulatory organizations ("SROs") should engage in a more risk-based process, focused explicitly on the

[35] Of the total of 4 recommendations are recommendations 2 and 3 excluded since they are outside the scope of Corporate Governance.

costs and benefits of regulation. To the extent possible, regulations should rely on principles-based rules and guidance, rather than the current regime of detailed prescriptive rules. We also recommend better coordination among national regulators and between federal and state authorities.

4. Implementation of Sarbanes-Oxley. We recommend no statutory changes in the Sarbanes-Oxley Act, including Section 404. Investors have benefited from the stronger internal controls, greater transparency, and elevated accountability that have resulted from this new law. However, we do believe that the implementation of SOX 404 by the SEC and the PCAOB, together with the prospect of catastrophic liability faced by auditors, has produced a regime that is overly expensive. The same benefits can be produced at lower cost. We conclude that there need to be changes to SOX 404 implementation, including [A] a redefinition of materiality, [B] more guidance from the PCAOB, and [C] multi-year rotational testing permitted within an annual attestation."

The Committee elaborates on the recommended changes to SOX Section 404:

A. "Redefine" Material Weakness. The starting point for reform should be to revise the scope and materiality standards in Auditing Standard No. 2[36] ("AS2") to ensure that reviews are truly risk-based and focus on significant control weaknesses.

The Committee recommends that the definition of materiality in AS2 be revised as follows: "A material weakness exists if it is reasonably possible that a misstatement, which would be material to the annual financial statements, will not be prevented or detected." The Committee's proposed formulation would change the probability threshold for the detection of control weaknesses from AS2's existing "more than remote likelihood" standard to "reasonably possible" that a material misstatement could occur.

The Committee recommends, therefore, that the SEC revise its guidance on materiality for financial reporting so that scoping materiality is generally defined, as it was traditionally, in terms of a five percent pre-tax income threshold."

B. "Develop Enhanced PCAOB and SEC Guidance. The Committee recommends that the SEC and PCAOB further enhance guidance by:

- clarifying and permitting greater judgment as to the auditor's role in understanding and evaluating management's assessment process;
- confirming that auditors, in attesting to management's assessment, are not required to perform similar assessments to those needed in issuing their own opinions;
- . reinforcing the appropriateness of the auditor's use of judgment throughout the audit of internal controls over financial reporting, including in the evaluation of strong indicators of material weakness;
- clarifying that the auditor attestation does not require the auditor to report separately on management's own internal control assessment process; and

[36] The Auditing Standard for SOX.

- incorporating the frequently-asked questions guidance into the text of AS2[37]."

C. "Permit Multi-Year Rotational Testing and Increased Reliance on Work of Others. Critical components of financial processes and higher risk areas such as procedures for preparing the annual financial statements and related disclosures should be tested each year. For lower risk components of financial processes and other areas, such as certain elements of the information technology environment, management and the auditor should be allowed to use a multi-year rotational testing approach within an annual attestation.

The SEC and PCAOB also should confirm that auditors may increase reliance on the work of others and give guidance to both management and auditors regarding the auditor's maximum reliance on inputs from existing sources in performing their control work (for example, inputs from internal auditors and management). Such guidance would help eliminate redundancies and allow auditors to use more judgment and risk based control testing in their attestation, as opposed to repeating tests similar to those used in management's assessment of internal controls."

The Committee's four key recommendations are proposed to the following audience: "Due to the importance of these issues, we recommend that the President direct his Working Group on Financial Markets to examine the legal and regulatory concerns we raise and to propose whatever reforms it views necessary and appropriate."

Sustaining New York's and the US' Global Financial Service Leadership[38]

On January 22, 2007, New York City Mayor Republican[39] Michael R. Bloomberg and Democratic US Senator Charles E. Schumer released a report that to a large extent confirmed the recommendations in the "Paulson Report". The 134 pages report provides, as the previous report, analyses of market conditions in the U.S. and abroad. The authors of the report (McKiney & Co.) interviewed more than 50 leaders from the financial services industry, consumer groups, and other stakeholders to reach the following conclusions:

"The findings are quite clear: First, our regulatory framework is a thicket of complicated rules, rather than a streamlined set of commonly understood principles, as is the case in the United Kingdom and elsewhere. The flawed implementation of the 2002 Sarbanes-Oxley Act (SOX), which produced far heavier costs than

[37] The Auditing Standard of SOX.

[38] Sustaining New York's and the US' Global Financial Service Leadership, January 22, 2007.

[39] He has recently converted to Independent.

expected, has only aggravated the situation, as has the continued requirement that foreign companies conform to U.S. accounting standards rather than the widely accepted – many would say superior – international standards. The time has come not only to re-examine implementation of SOX, but also to undertake broader reforms, using a principles based approach to eliminate duplication and inefficiencies in our regulatory system."

The consensus with the findings in the "Paulson Report" is obvious, they even quote Mr. Paulson: "… in the words of Treasury Secretary Henry Paulson, "that the internal control audit is top-down, risk-based and focused on what truly matters to the integrity of a company's financial statement"."

Conclusions

The immediate reason for the Company's interest in COBIT is to facilitate the implementation of the Sarbanes-Oxley Act (SOX). To become SOX compliant, the US Security and Exchange Committee (SEC) require companies to base their assessment on a suitable and recognized internal control framework, i.e. COSO. The challenge is to integrate COSO-ERM with the other standards of the Company, the Service Management standard, ISO 20000, the Information Security standard, ISO 27001, and the in-house developed Security Architecture.

COBIT will not replace the other standards. It is a middle layer between COSO-ERM and the standards. COBIT can translate COSO-ERM objectives into more concrete controls or processes to ISO 20000 and ISO 27001 by first matching them with the COBIT controls. COBIT can also directly integrate COSO-ERM with the Security Architecture, if ISO 27001 is not implemented (even though this is recommended). However, COBIT doesn't otherwise replace ISO 27001. The reason is that COBIT is limited to IT governance; it doesn't cover the full scope of either COSO-ERM or information security.

COBIT is not implemented in total with all its controls; it is "tailored" according to the environment of the Company and the pre-existing standards and architecture. This "Plumbing Approach" reduces unnecessary work and is thereby cost-effective; it is only used when there is a detected gap between COSO-ERM and the standards ISO 20000, ISO 27001 and the Security Architecture.

No area of U.S. SOX has generated more controversy than Section 404 (covering creation and maintenance of viable internal controls). A reason is the harsh criminal penalties that Section 404 imposes, if it is "more than a remote likelihood" that a material misstatement could occur.

The "Paulson Committee" will see a change in the probability threshold for the detection of control weaknesses from "more than remote likelihood" to "reasonably possible" that a material misstatement could occur. The recommendation is that scoping materiality is generally defined, as before SOX, in terms of a five percent pre-tax income threshold.

Another proposal is that the auditor attestation should not require the auditor to report separately on management's own internal control assessment process; i.e. back to the same procedures as before SOX.

Moreover, critical components of financial processes and higher risk areas should be tested each year. However, for lower risk components of financial processes and other areas, "…such as certain elements of the information technology environment", management and the auditor should be allowed to use a multi-year rotational testing approach within an annual attestation. This is a change to the pre-SOX modus operandi of auditing, when auditors' main focus was on controls in financial applications. Section 404 expanded that scope beyond financial controls to the IT and application infrastructure.

The final example of the recommendations is another example on auditing as it used to be: "…allow auditors to use more judgment and risk based control testing in their attestation, as opposed to repeating tests similar to those used in management's assessment of internal controls."

There are strong commercial forces behind the suggested changes, but also some names that are outside the financial and accounting industries. The most notable name is Governor Elliot Spitzer, the Democratic governor of New York, who as the state's attorney general prosecuted Wall Street firms and other companies for corporate securities fraud and earned more than $3.5 billion in penalties and settlements for the state. He has joined Mayor Bloomberg and Senator Schumer in calling for a reform of the Sarbanes-Oxley Act.[40]

The odds may be in favor of a change of SOX and Section 404. Business Week's guessed that, "regulators are now planning to loosen the rules, probably before the end of this year is out"[41]. However, there is some resistance; it is not the same consensus in the U.S. as when SOX passed the Senate unanimously and won easy approval in the House before it was signed by President Bush into law.

Critics stress high compliance costs (which totaled an estimated $15- 20 billion for issuers in 2004). Supporters emphasize the changed "tone at the top" among public companies when it comes to financial reporting, with a higher level of engagement from audit committees, CEOs, and CFOs on compliance. They also note the significant improvements in the control environment. Lately, the sub-prime meltdown and the risk of a global credit crunch have highlighted the consequences of lack of governance and transparence in the global financial industry. This may strengthen the "supporters" and weaken the "critics".

The two reports state as an example The City of London for the future of the U.S.; New York is governed by a rule-based-regulatory regime; London's regulators operate a principles-based-system that has an altogether lighter touch. But, the same role model, the City of London, was the target for the US SEC when it "launched an astonishing attack on the City's regulatory standards yesterday", according to The Times. Mr. Roel Campos, an SEC commissioner, compared London's junior AIM[42] market to a casino: "It is a losing proposition to tout lower standards as a way to promote your markets."[43]

The frustration Mr. Campos expressed might also be seen in the context of the development of the Alternative Investment Market (AIM), the British competitor to NASDAQ. AIM listed 870 new companies in the five year since 2001, while

[40] www.accountingweb.com.

[41] Business Week, January 29, 2007.

[42] Alternative Investment Market.

[43] The Times, Friday, March 9, 2007.

NASDAQ listed 526.[44] To make things worse from a US perspective, the combined IPO proceeds from listing on AIM and the LSE exceeded those on NASDAQ and the NYSE for the first time 2006.[45]

The debate will continue between promoters of principle based rules (i.e. voluntary guidelines) versus compulsory regulations (i.e. SOX). The outcome will have a significant impact on Corporate Governance, ERM, Compliance, and Information Security. However, there seems to be a widespread acceptance for COSO-ERM. One reason is the need for an "umbrella" for the myriad of regulations companies are facing regardless of SOX.

Just a few examples of existing regulations: the Health Insurance Portability Accountability Act, HIPAA (protects personal health information of individuals stored in electronic form); Basel II (regulate bank credit handling and operative risks); the Federal Information Security Management Act, FISMA (requires agencies to report on the state of their security readiness annually); the United States' Patriot Act (covering surveillance and investigative powers of law enforcement agencies in the US; the Gram-Leach-Bliley Financial Modernization Act, GLB Act. (ensure the security and privacy of customer information); and European Union regulations such as Solvency II (for improvements of insurers internal control) and other national laws concerned with internal control (as "Svensk kod för bolagsstyrning").

Several of these regulations are referring to COSO-ERM. Also governments base their governance on COSO-ERM. The US Office of Management and Budget issued Circular A-123, defining management's responsibility for internal control in federal agencies, based on COSO[46]. Our neighboring countries Norway and Finland apply COSO-ERM, and the Swedish government agencies will probably be required to implement COSO-ERM as of 2008[47].

Presently, COSO-ERM is the best alternative as an umbrella for regulations. However, it is an umbrella that needs support from standards and frameworks as ISO 20000 and ISO 27001 to deliver compliance in IT and application infrastructures. To facilitate this, the "Plumber" COBIT could be called in.

[44] The Times, Tuesday, March 13, 2007.

[45] The Times, Friday, March 9, 2007.

[46] Circular A-123, Federal Managers' Financial Act of 1982.

[47] Intern styrning och kontroll i staten, Departementsserien, Ds 2006:15, 2006.