Business Benefits by Aligning IT best practices

Executive Summary

Since the Sarbanes-Oxley Act (Sarbanes-Oxley or SOX) was signed into law in 2002, many companies have adopted some IT practices to comply the regulation. In this paper, I will discuss overall IT best practices and the business benefits by aligning them. After introducing the SOX and the internal control framework called COSO’s Internal Control briefly, I will discuss three international IT best practices (CobiT, ITIL, and ISO 17799) and the best way to implement the best practices. In the end, I will write about the business benefits from understanding SOX and aligning the IT best practices. The Following figure shows the relationship among SOX and its control frameworks mentioned in this paper.

(Source: CIO guide to SOX, Reymann Group Inc., Jan 2005)
I. Background

IT best practices have become significant due to following reasons:

- Business managers and boards require better returns from IT investments, which are generally increasing.
- Companies need to meet regulatory requirements for IT controls in areas such as privacy and financial reporting and in specific sectors such as finance, pharmaceutical and healthcare.
- Companies need to select service providers and outsource and acquire management of service.
- IT-related risks such as network security get complex and serious.
- IT governance initiatives including adoption of control frameworks and best practices to help monitor and improve critical IT activities.
- Companies need to optimize costs by following standardized approaches.
- Well-regarded frameworks grow mature and their consequent acceptance increases.

The growth in the use of standards and best practices creates demands for implementation guidance new challenges including creating awareness of the business purpose and the benefits of these practices and aligning them to suit each company. Therefore, I would like to explain the business purpose and benefits of IT best practices and good ways of implement and align the practices.

(Source: GITI & OGC, Aligning COBIT, ITIL and ISO17799 for the Business Benefit, 2005)
II. Overview of SOA and COSO frameworks

1. The Sarbanes-Oxley Act of 2002 (SOX)

The Sarbanes-Oxley Act (Sarbanes-Oxley or SOX) signed into law in 2002 represents the most dramatic change to federal securities law since the 1930’s. The SOX applies to all publicly traded companies, and is the federal government’s response to accounting scandals involving businesses like Enron. The purpose of Sarbanes-Oxley is to make sure that the board of publicly held companies takes responsibility for reporting accurate financial reports to the public. Sarbanes-Oxley also affects accounting firms and their auditing standards.

A few important contents of Sarbanes-Oxley are as follows:

- Sarbanes-Oxley requires the board of directors to be made up of five members who have a proven ability to review and comprehend financial documents. Of the five members, two must be either a Certified Public Accountant (CPA) or must have been a CPA. The other three must not be CPAs, nor can they be retired CPAs. Each of the five financially literate board members must serve a five-year term.

- The Board is responsible for adopting auditing, internal control and ethical standards for the company. The Board must adopt standards for evaluating public accounting firms and must require the firm keep accurate records supporting audit findings for a period of
The Board must ensure each audit is approved by a second partner. The Board must develop internal controls in keeping with revised audit standards in order for the public accounting firm to evaluate the company’s compliance with said internal controls.

- The Chief Financial Officer and the Chief Executive Officer must provide a letter stating the financial data they have provided the auditors is accurate. This letter must be provided to the auditing firm before the audit can be approved, and must be included with the published audit. Company executives and staff must not withhold financial information from the auditors, or attempt to influence the audit findings in any way.

Loans may not be issued to a director or executive officer of a publicly held company.


2. COSO’s Internal Control - Integrated Framework

Issued in 1992 by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), this Framework has long served as a blueprint for establishing internal controls that is designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.
COSO’s report outlines 26 fundamental principles associated with the five key components of internal control as follows:

(Source: Putting COSO’s Theory into Practice, THE INSTITUTE OF INTERNAL AUDITORS, 2005)

1) Control Environment

The Control environment is the foundation for all other components of control and sets the tone of an organization, influencing the control consciousness of its people. The factors included in the environment are Integrity and ethical values, Competence of people, HR practices, Management’s operating philosophy, The way authority and responsibility are assigned, and The attention and direction provided by the board.

2) Risk Assessment

The major principles related to the achievement of control objectives at the risk assessment level are the importance of financial reporting objectives, the identification and analysis of financial reporting risks, and the assessment of fraud risk
3) Control Activities

Control activities are policies/procedures that ensure management directives are carried out. They occur throughout the organization, at all levels and in all functions and help ensure that necessary actions are taken to address risks. The activities include approvals, authorizations, verifications, recommendations, performance reviews, asset security, and segregation of duties.

4) Information and communication

Pertinent information is identified, captured and communicated in a timeframe that allows people to carry out their responsibilities. This information includes internal and externally information about events, activities and conditions necessary for informed business decision-making and external reporting. Flow to information needs to allow for successful control from instructions on responsibilities to summary of findings for management action.

5) Monitoring

Effective monitoring comprises ongoing monitoring, separate evaluations, and reporting deficiencies. As a key component of the small-business control structure, monitoring confirms that all five components are in place, properly designed, and functioning effectively. Smaller businesses can reduce the cost and effort of monitoring by building it into processes.

(Source: Putting COSO’s Theory into Practice, THE INSTITUTE OF INTERNAL AUDITORS, 2005)
III. Overview of IT best practices for information trust

1. COBIT

COBIT (The Control Objectives for Information and related Technology) is a set of best practices (framework) for information (IT) management created by ISACA and ITGI in 1992. COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company. The first edition was published in 1996 and the fourth edition in December 2005. It has more recently found favor due to external developments, especially after the Enron scandal with the subsequent passage of the Sarbanes-Oxley Act.

The COBIT framework is based on the following principles: to provide the information that the enterprise requires to achieve its objectives, the enterprise needs to manage and control IT resources using a structured set of processes to deliver the required information services.

(Source: COBIT 4.0, IT Governance Institute, 2005, p12)
The COBIT framework has the four domains containing a set of 34 generic processes depicted in the following picture, managing IT resources to convey information to the business according to the business and governance requirement:

**Overall COBIT Framework**

(Source: COBIT 4.0, ITGI, 2005, P25)
The details of the four domains are as follows:

1) **Planning & Organization** – This domain covers strategy and tactics, and includes the identification of the way how IT can best contribute to the achievement of an organization’s business objectives. Furthermore, the realization of the strategic vision needs to be planned, communicated and managed for different perspectives. This domain also includes the development of a proper organization and technical infrastructure.

2) **Acquisition & Implementation** – To realize the IT strategy, IT solutions need to be identified, developed or acquired, and implemented. Changes to and maintenance of existing systems are also covered by this domain.

3) **Delivery & Support** – This domain is concerned with the actual delivery of required services, which may include computer operations, information security, operational continuity, and training. In order to deliver of services, necessary support processes must be set up and are also included in this domain.

4) **Monitoring** – All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management’s oversight of the organization’s control process and independent assurance provided by the internal and external audit or obtained from alternative sources.

(Source: COSO and Information Technology—integration of standards, PricewaterhouseCoopers, 2007, p9-13)
2. ITIL

IT service management is concerned with delivering and supporting IT services that are appropriate to the business requirements of the organization. ITIL provides a comprehensive, consistent and coherent set of best practices for IT service management and related processes, promoting a quality approach for achieving business effectiveness and efficiency in the use of IT. The core operational processes of IT service management are described within the two ITIL publications: Service Support and Service Delivery.

(Source: Intro to ITIL, Protiviti, 2007)

The processes of service support described in ITIL are Incident management, Problem management, Configuration management, Change management, Release management, and Service desk function. The processes of service delivery described in ITIL are Capacity
management, Availability management, Financial management for IT services, Service level
management, and IT service continuity management.

3. ISO 17799

The ISO and IEC, which have established a joint technical committee, the ISO/IEC JTC 1, published the international standard in 2000. The ISO 17799 provides information to responsible parties for implementing information security within an organization. It can be seen as a basis for developing security standards and management practices within an organization to improve reliability on information security in inter-organizational relationships.
The standard was published in 2000 in its first edition, which was updated in June 2005. It can be classified as current best practice in the subject area of information security management systems. The guiding principles are the initial point when implementing information security. They rely on either legal requirements or generally accepted best practices. Measures based on legal requirements include Protection and nondisclosure of personal data, Protection of internal information, and Protection of intellectual property rights. Best practices mentioned are Information security policy, Assignment of responsibility for information security, Problem escalation, Business continuity management.

When implementing a system for information security management several critical success factors are to be considered as follows:

- The security policy, its objectives and activities reflect the business objectives.
- The implementation considers cultural aspects of the organization.
- Open support from and engagement of senior management are required.
- Risk assessment and risk management is required.
- Effective marketing of security targets all personnel, including members of management.
- The security policy and security measures are communicated to contracted third parties.
- Users are trained in an adequate manner.
- A comprehensive and balanced system for performance measurement is available, which supports continuous improvement by giving feedback.

(Source: GITI & OGC, Aligning COBIT, ITIL and ISO17799 for the Business Benefit, 2005)
IV. Case Study

To illustrate how relevant modern IT general controls is to corporate financial statement processing functions, consider the following characteristics of a typical large corporation:

- The company maintains multiple national offices and distribution centers linked via WAN and VPN connections.
- All accounting, supply chain, and fulfillment operations are fully integrated via a modern, distributed ERP system that feeds financial information back to a centralized mainframe in the home office for financial processing and reporting.
- The company has internally developed an e-commerce website that generates most of its total sales orders. A high percentage of its purchasing and EDI operations are also conducted via secure trading-partner websites maintained by vendors or independent third-party service providers.
- The company distributes the majority of its internal financial reporting documentation electronically to all business units in real time via secured intranet websites and e-mailed PDF report attachments.

For a company like this, attention should be paid to the following specialized IT general and application level control areas: 1) Networking infrastructure, 2) ERP configuration and business continuity, 3) Web-based application development considerations, and third-party reliance, and 4) Paperless Financial Reporting Systems.
1) **Network infrastructure** - A thorough analysis of IT controls in this area would include a review of firewall configuration parameters, network intrusion detection and monitoring provisions, network performance monitoring activities, network configuration and administration functions, data classification and encryption standards, e-mail and antivirus filtering provisions, business continuity provisions, and critical third-party service provider reliability.

2) **ERP configuration and business continuity** - Modern ERP and accounting systems are capable of fully automating and integrating many highly complex business processes and centrally regulating and monitoring a broad array of financial and accounting system controls. No two vendors’ ERP or accounting applications are alike, and many can be extensively customized to support specialized vertical industry requirements.

3) **Web-based application development considerations, and third-party reliance** - When analyzing web-based application development, auditors should focus on the methodology the company is employing to monitor and regulate website development and maintenance.

4) **Paperless Financial Reporting Systems**

Implementing real-time financial management and paperless reporting systems can dramatically enhance the efficiency of an enterprise’s operations. While helping makes companies more nimble, the increasing adoption of these technologies has robbed auditors of ready access to the paper trails that have traditionally supported their analysis and testing of internal controls.

(Source: http://www.nysscpa.org/cpajournal/2004/1204/essentials/p52.htm)
V. Implementation of the Best Practices

The best practices adopted have to be consistent with the risk management and control framework, appropriate for the organization, and integrated with other methods and practices that are being used. For best practices to be effective, the use of a common language and a standardized approach oriented toward real business requirements is best. For this purpose, we need to do several tasks as follows:

1) Tailoring

Every organization needs to tailor the use of standards and practices, such as those examined in this document, to suit its individual requirements. All three can play a very useful part—COBIT and ISO 17799 helping to define what should be done and ITIL providing the how for service management aspects.

2) Prioritizing

To avoid costly and unfocused implementations of standards and best practices, organizations need to prioritize where and how to use standards and practices. The organization needs an effective action plan that suits its particular circumstances and needs.

3) Planning

With this mandate and direction in place, management then can initiate and put into action an implementation approach. To help management decide where to begin and to ensure that the
implementation process delivers positive results where they are needed most, the following steps are suggested:

- Step 1: Set up an organizational framework (ideally as part of the IT governance initiative)
- Step 2: Align IT strategy with business goals.

4) Avoiding Pitfalls

There are also some obvious, but pragmatic, rules that management ought to follow:

- Treat the implementation initiative as a project activity with a series of phases.
- Remember that implementation involves cultural change as well as new processes.
- Make sure there is a clear understanding of the objectives and Manage expectation.
- Focus first on where it is easiest to make changes and deliver improvements and build from there one step at a time.
- Obtain top management buy-in and ownership.
- Avoid the initiative becoming perceived as a purely bureaucratic exercise.
- Avoid the unfocused checklist approach.

5) Aligning best practices

IT best practices need to be aligned to business requirements and integrated with one another and with internal procedures. COBIT can be used at the highest level, providing an overall control framework based on an IT process model that should generically suit every organization. Specific practices and standards such as ITIL and ISO 17799 cover discrete areas and can be mapped to the COBIT framework, thus providing a hierarchy of guidance materials.

(Source: GITI & OGC, Aligning COBIT, ITIL and ISO17799 for the Business Benefit, 2005)
VI. Business Benefits through the Best Practices

1) Best Practices and Standards Help Enable Effective Governance of IT Activities

Increasingly, the use of standards and best practices is being driven by business requirements for improved performance, value transparency and increased control over IT activities. As every organization tries to deliver value from IT while managing an increasingly complex range of IT-related risks, the effective use of best practices can help to avoid re-inventing wheels, optimize the use of scarce IT resources and reduce the occurrence of major IT risks such as Project failures, Wasted investments, Security breaches, System crashes, Failures by service providers to understand and meet customer requirements.

2) An IT Management Framework Is Needed

Organizations wishing to adopt IT best practices need an effective management framework that provides an overall consistent approach and is likely to ensure successful outcomes when using IT to support the enterprise’s strategy. As IT governance gains momentum and acceptance, IT best practices will increasingly be aligned to business and governance requirements rather than technical requirements.

3) Best Practices Provide Many Other Benefits

- Avoiding re-inventing wheels and Reducing dependency on technology experts
- Increasing the potential to utilize less-experienced staff if properly trained
- Making it easier to leverage external assistance
• Overcoming vertical silos and nonconforming behaviors

• Reducing risks and errors, and Improving quality and the ability to manage and monitor

• Increasing standardization leading to cost reduction

• Improving trust and confidence from management and partners

• Creating respect from regulators and other external reviewers

• Safeguarding and proving value.

(Source: GITI & OGC, Aligning COBIT, ITIL and ISO17799 for the Business Benefit, 2005)

VII. Conclusion

I have discussed the internal control framework (COSO’s Internal Control- Integrated Framework) and its three international IT control frameworks including COBIT, ITIL, and ISO 17799 to meet the regulatory requirement for IT controls (SOX). I have also discussed the best way to implement the IT control frameworks to realize the Internal Control framework into the organizations and the business benefits from implementing and aligning the best practices.

While writing this paper, I have learned a few important aspects of implementing best practices:

• COBIT can be used as an overall control framework to decide how to adopt other IT best practices.

• To implement the best practices effectively, we need to do several tasks such as Tailoring, Prioritizing, Planning, Avoiding pitfalls, and Aligning IT best practices.

• The effective adoption of best practices can provide organizations with many business benefits such as effective governance of IT activities and improving the ability to manage.
References


- CIO guide to SOX, Reymann Group Inc., Jan 2005

- IT Control Objectives for Sarbanes-Oxley, GITI, 2006

- COSO’s Internal Control - Integrated Framework, COSO, 2004

- COSO and Information Technology–integration of standards, PWC, 2007

- Introduction to IT Governance, Michael J. Shaw, 2007

- COBIT 4.0, IT Governance Institute, 2005

- Intro to ITIL, Andrew Smith, Protiviti, 2007

- GITI & OGC, Aligning COBIT, ITIL and ISO17799 for the Business Benefit, 2005

- Sarbanes-Oxley Compliance for Nonaccelerated Filers, Solving the Internal Control Puzzle, Sid M. Edelstein, 2004