Understanding the COSO and COBIT Frameworks and
What They Hold for AIS Compliance with Sarbanes-Oxley

Michael K. Dolan Jr.
Accounting Information Systems
6 April 2004
Table of Contents

Table of Contents

Introduction and Overview of Sarbanes-Oxley

Internal Control Frameworks

COSO’s “Internal Control – Integrated Framework”
COSO’s “Enterprise Risk Management Framework”
Control Objectives for Information and Related Technology (COBIT)
Practical Implications of COSO and COBIT on AIS

Conclusion

Appendix

Exhibit 1 - ERM Framework Components
Exhibit 2- COBIT Domains
Exhibit 3 - Maturity Models
Introduction and Overview of Sarbanes-Oxley

Enacted on July 30, 2002 after waves of corporate accounting scandals at companies like Enron and Worldcomm, Sarbanes-Oxley (hereafter “SOX”) was intended to “protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws…”¹ While SOX does not address accounting information systems directly, many of its provisions will have profound impacts on the systems corporations use for corporate reporting and daily operations. Sections 302 and 404(a) in particular put the onus on top level management to ensure the accuracy and reliability of corporate reports.

Public companies will be required to comply with SOX as of their fiscal year end after November 15, 2004 for accelerated filers (market capitalization over $75 million) and July 15, 2005 for non-accelerated filers.²

Section 302 requires CEOs and CFOs to sign off on accuracy of the company financial statements and periodic reports. The officers must certify a number of attestations that they have reviewed the financial report, the report is true and not misleading, and that the officer accepts responsibility for ensuring effecting disclosure controls. This section specifically addresses the users and systems in the company that generate financial reports for external parties.³

Section 404(a) requires companies to issue with their annual reports (i) an internal control report stating management’s responsibility for establishing and maintaining internal control over financial reporting, and (ii) an assessment of the

effectiveness of internal control. The SEC has recognized the COSO framework for establishing internal controls over financial reporting. Given the civil and criminal penalties for CEOs and CFOs, top management will have a lot riding on the information systems their company employs.

**Internal Control Frameworks**

When analyzing the requirements of SOX, it is inevitable to recognize the 1992 COSO framework being that it has been stamped with the seal of approval by the SEC. External auditors will also have to opine on a company's internal controls and will be using the COSO framework as their primary guide. COSO does not directly setup a framework for corporate information systems, however. SOX’s requirements will likely be implemented into a corporate IT system. In order to determine the internal control from an AIS perspective, companies and auditors will turn to the COBIT IT governance framework. Understanding these two frameworks and how they fit into an AIS internal control system will be essential for every organization under SOX.

**COSO’s “Internal Control – Integrated Framework”**

The COSO framework was published in 1992 as an independent private sector initiative. The framework identified the establishment of internal controls as a means for helping a company achieve control objectives. The COSO framework is the only framework to date having the SEC’s approval. COSO is also the underlying foundation of SAS 94 “The Effect of Information Technology on the

---

4 Id. at §404(a).
6 Id.
Auditor’s Consideration of Internal Controls in a Financial Statement Audit.”

Understanding the COSO framework will be essential to understanding the impact of SOX on a company’s IT and AIS systems.

The COSO framework sets up three key objectives:

1) Effectiveness and efficiency of operations
2) Reliability of Financial Reporting
3) Compliance with applicable laws and regulations

The path to achieving these objectives is comprised of five components for designing and benchmarking internal control:

- **Control Environment** – discipline and structure foundation of the company
- **Risk Assessment** – identification and analysis of risk
- **Control Activities** – policies, procedures, and technology used to achieve management of control and risk
- **Information and Communications** – information flow between management and employees
- **Monitoring** – continuous oversight of control by parties outside the process

Finally, the COSO framework extends responsibility for these objectives and components across all levels of the enterprise, business units, and other levels of

---

7 Greene, Fredric. “Compliance with Sarbanes-Oxley and SAS 94: The Critical Role …” Available at http://www.nysscpa.org/committees/emergingtech/sarbanes_act.htm
operations.\(^8\) The COSO framework is often summarized in a cube diagram recreated below.

![Figure 1 - Internal Control Framework](image)

COSO’s “Enterprise Risk Management Framework”

As of April 2004, COSO is finalizing the draft of a new Enterprise Risk Management Framework. This new framework incorporates and builds upon the 1992 Internal Control Framework. It includes three new components for objective setting, event identification, and risk response although all components are broader in their descriptions and application. The new framework is designed to promote three principles into an organization:

1) Help align risk appetite and strategy  
2) Make the risk appetite explicitly known in an organization and ensure alignment in actual practice  
3) Ensure effective risk-response decisions are being made

---

The new framework also includes a new objective for strategy. In the new framework, strategy becomes the baseline measure of a company’s risk management practices.\textsuperscript{9} The ERM framework has a new cubicle depiction included below. A table showing the descriptions of ERM Components is included as Exhibit 1.

\begin{figure}[h]
\centering
\includegraphics[width=0.8\textwidth]{ERM_Framework.png}
\caption{ERM Framework}
\end{figure}

\textbf{Control Objectives for Information and Related Technology (COBIT)}

The COBIT framework was developed by the IT Governance Institute (an outgrowth of ISACA) as a standard for IT security and control practices. The COBIT framework specifies IT governance as “a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise’s goals by adding value while balancing risk versus return over IT and its

processes.” The framework focuses on the structure linking IT processes, resources, and information to enterprise strategies and objectives. While the COBIT framework is focused on IT in general, it applies directly to a company’s AIS possibly the most important component of its overall IT system.

COBIT identifies 34 key IT Control Objectives and groups them under four categories or domains:

1) Planning and Organization
2) Acquisition and Implementation
3) Delivery and Support
4) Monitoring

Exhibit 2 contains a diagram detailing the domains and their respective IT processes. Each of the control objectives has a corresponding COBIT Audit Guideline for companies to review their practices against COBIT guidelines. Specifically, COBIT organizes control and measurement over IT processes into four areas:

- **Maturity Models** – help an organization map its progress to date versus the best in the industry or where it wants to be (See Exhibit 3)
- **Critical Success Factors** – define the most important management-oriented implementation guidelines to achieve control over and within its IT processes

---

• **Key Goal Indicators** – define measures that tell management – after the fact – whether an IT process has achieved its business requirements

• **Key Performance Indicators** – lead indicators that define measures of how well an IT process is performing in enabling the goal to be reached

COBIT also provides an implementation tool set describing the process of implementing COBIT into an organization. These real life implementation stories give companies an idea of what may lie ahead during an implementation.11

The COBIT framework fits together as domains of activity and processes. The COBIT domain has processes of business needs like the Delivery & Support domain has a business need for “Ensure System Security”. The business needs are described using Key Goal Indicators and then measured using Key Performance Indicators. Critical Success Factors facilitate the use of KGIs and KPIs. COBIT’s maturity model will allow the organization to assess whether its level of achievement is in a range from “non-existent” to “optimized.”12

While COSO says little if nothing about specific IT controls required to meet its Control Activities goals, COBIT provides this guidance. COBIT recognizes the COSO framework and builds upon COSO while focusing on real life IT aspects. These IT implications apply directly to a company’s AIS. The COBIT framework is not a separate framework, but provides a finer grain of detail.

---


under the COSO framework and is intended to be used alongside COSO. SOX requires a company’s external auditor to sign off on management’s assertions about internal control over financial reporting. The COBIT framework is well recognized as an IT control and external auditors will use COBIT to evaluate and test as part of their audit.\textsuperscript{13}

**Practical Implications of COSO and COBIT on AIS**

The COSO and COBIT frameworks taken together provide a fairly detailed path of what a SOX compliant AIS requires. There will be quite a few stakeholders in an organization when it comes to SOX compliance. Internal groups within an organization will have their priorities and external auditors will have their own priorities. In the end, however, both will now work off the same guide having COSO and COBIT generally accepted. An example of the practical implications of SOX on an AIS can be found using AIS application security.

One area of change that SOX will likely require for AIS is in application security. Using COSO, an organization will perform a *Risk Assessment* and analyze risks associated with data loss, modification, and disclosure. The organization will want to have control activities designed to protect and ensure confidentiality, integrity, and availability of the AIS.

Under COBIT, an organization will look at the *Planning and Organization* domain. Some processes under the *Planning and Organization* domain of the company’s AIS that are relevant to application security would include defining the information architecture (PO2), ensuring compliance with external requirements

(PO8), assessing risks (PO9), and managing projects (PO10) and quality (PO11). Planning and Organization would not be the only domain relevant to a company’s AIS. Under the domain of Delivery & Support, relevant business processes to application security would include defining and managing service levels (DS1), manage third-party services (DS2), ensure system security (DS5), manage problems, incidents (DS10) and data (DS11). Under the domain of Acquisition & Implementation, an organization would look at identify automated solutions (AI1), acquire and maintain application software (AI2), develop and maintain procedures (AI4), and manage changes (AI6). Finally, under the domain of Monitoring the organization would focus on monitoring the process (M1), assessing internal control adequacy (M2), and providing for independent audit of security (M4).\textsuperscript{14}

Narrowing down a business goal of AIS application security, the organization now has domains and respective business processes to focus on to ensure AIS application security. Each business process has procedures and detailed guidance within the COBIT framework documentation for the organization to follow in implementing each business process. The COSO and COBIT frameworks will work together and lead to the development of specific controls to implement internal control under SOX within an AIS. Other standards

\textsuperscript{14} COBIT Framework 3\textsuperscript{rd} Edition, p. 7. Available at https://www.isaca.org/Template.cfm?Section=Obtain_COBIT&CONTENTFILEID=1396&TEMPLATE=/MembersOnly.cfm
like ISO 17799 “Code of Practice for Information Security Management” may be implemented into a control process along the way as appropriate.15

In the end, using COSO and COBIT may lead a company to implement specific input controls such as dual-input (repetitive input) checking for errors including out of range values, overflow strings, and invalid characters. Processing controls within the AIS for application security could include checks on the order of processing programs and specific controls designed to handle processing halts or failures. Output controls for application security within the AIS could include checks on user rights for viewing the data being output, checks on whether the data itself is reasonable, and checks to make sure the data was fully processed before results are output.16

Conclusion

With COSO and COBIT as framework guides, companies and their external users of AIS data will have a common ground with which to work in meeting SOX requirements. COSO and COBIT will likewise drive a standardization of business processes as a result of each organizations analysis. The result is a set of frameworks that taken together provide the fundamental basis for internal control over an AIS.

The next question is whether the final result of COSO and COBIT actually further the original mandate of SOX. SOX under sections 302 and 404(a) requires management to sign off on the internal controls within the organization

16 Id.
and also in financial reporting. The COSO and COBIT frameworks provide an excellent foundation for internal control and thus do seem to give management a measure and a strategy for achieving control under SOX. With COSO and COBIT frameworks in place, a CEO or CFO should have the confidence in their organizations internal controls to sign off as required in SOX.

Some may debate whether SOX really would have precluded the occurrence of the accounting scandals of Enron and Worldcomm et al. It can be argued these scandals were the result of collusion between powers that would normally be separate (i.e. legal, accounting, and consulting). The more compelling arguments for COSO and COBIT are that they should move companies to make changes in their AIS and other IT systems that will provide checks and controls against collusion within the system. While an AIS cannot prevent collusion, a COSO and COBIT system with proper security and integrity controls could prevent collusion between employees and managers. The weakness that will always remain, however, is if the COBIT or COSO frameworks are implemented incorrectly.

In the end, it seems appropriate that COSO and COBIT together should govern an organization’s AIS and SOX compliance issues. It appears AIS compliance requires the use of both frameworks as they meld business and IT processes in a meaningful guide. It will be imperative for managers to grasp and implement both frameworks into their SOX compliance planning.
Appendix

Exhibit 1 - ERM Framework Components

- **Internal Environment**

- **Objective Setting**

- **Event Identification**

- **Risk Assessment**
  - Inherent and Residual Risk – Likelihood and Impact – Methodologies and Techniques – Correlation

- **Risk Response**
  - Identify Risk Responses – Evaluate Possible Risk Responses – Select Responses – Portfolio View

- **Control Activities**
  - Integration with Risk Response – Types of Control Activities – General Controls – Application Controls – Entity Specific

- **Information and Communication**
  - Information – Strategic and Integrated Systems – Communication

- **Monitoring**
  - Separate Evaluations – Ongoing Evaluations
COBIT IT Processes Defined Within the Four Domains

Exhibit 2- COBIT Domains

Maturity models are effective tools for determining the current status of an organization’s processes, their effectiveness at achieving business goals, and how they should evolve. Five levels make up a generic maturity model. The model reads from the base (1) up (i.e. to 5)

1) Initial – Software processes are ad hoc; there are few defined processes and success depends on individual effort.

2) Repeatable – Basic project management processes are established to track cost, schedule, and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.

3) Defined – The software process for both management and engineering activities is documented, standardized, and integrated into a standard software process for the organization. Projects use an approved, tailored version of the organization’s standard software process for developing and maintaining software.

4) Managed – Detailed measurements of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.

5) Optimizing – Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

---