

Risk Assessment in Sarbanes Oxley

Van A. Norris, Advanced Technology Institute, Charleston SC
Lisa R. Young, Bright Mind Solutions, Tampa FL

INTRODUCTION

Transitioning from a documentation culture focused on internal financial controls to a culture aware of business risks and the management of those risks is necessary to achieve lasting value from the compliance process. There is a real need to move away from a singular focus on financial controls to a process improvement and strategic model of risk management that includes all the controls necessary for the complete organization.

Enterprise Risk Management (ERM) has been designed to assist in making this transition. ERM properly implemented enables organizational management to effectively deal with uncertainty and associated risk and make an organization more valuable by creating a single view of all risks, internal and external, and an executive-level management strategy to deal with those risks. ERM has been viewed as the management of business risk, financial risk, operational risk and risk transfer to maximize a firm's value to owners and customers.

Several frameworks and methodologies have been developed to assist organizations in the ERM process. The OCTAVE¹ risk assessment methodology, COSO² framework for improving governance and enterprise risk management posture, and CobiT's³ information technology control framework are among the most popular with risk managers.

COSO, CobiT and Enterprise Risk Management

Over ten years ago, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued *Internal Control – Integrated Framework* to help businesses assess and enhance their internal control systems. That framework has since been incorporated into policy, rules, and regulations used by thousands of enterprises to achieve greater financial controls and prevent fraud.

In 2001, amid declining investor confidence caused by a series of high-profile corporate scandals, COSO initiated a project to produce a ERM framework that would be readily usable by management to evaluate and improve their organizations' governance and enterprise risk management posture.

¹ OCTAVE : Operationally Critical Threat, Asset, and Vulnerability Evaluation, www.cert.org/octave

² COSO : Committee of Sponsoring Organizations of the Treadway Commission

³ CobiT® : "Control Objectives for Information and related Technology" , Information System and Audit Control Association

The COSO ERM structure allows for a management framework with common language, concepts, and principles with clear guidance for management certification and audit attestation of the accuracy of financial accounting procedures and controls.⁴ The goal of ERM is to enable organizational management to effectively deal with uncertainty and associated risk and make an organization more valuable by creating a single view of all risks, internal and external, and an executive-level management strategy to deal with those risks.

Societal mandates for “sound management and honest financial reporting” resulted in governments imposing regulations forcing organizational leaders to make every effort to minimize reporting risks to their organizations. These regulations include the Basel II Accord⁵, Sarbanes Oxley (SOX)⁶, HIPAA⁷, and the Gramm-Leach-Bliley Act⁸. The Sarbanes Oxley regulation is considered by many to be one of the primary drivers of the adoption of ERM by organizations.

With the passage of the SOX legislation in 2002, section 404 attestation requires an assessment of the effectiveness of an organizations’ internal control structure and procedures to ensure confidence in the Information Technology (IT) systems that house, transport, store, and transform data. SOX section 404 is principle-based, allowing wide latitude in implementation and execution.

COSO’s ERM framework has become a primary method for compliance with section 404 of SOX. James Lam defines ERM as “the integrated management of business risk, financial risk, operational risk and risk transfer to maximize a firm’s value to owners and customers⁹. With the widespread reliance on technology for financial and operational reporting, controls have long been recognized as a necessity. The controls and the control environment are particularly vital for corporate data and related information systems. “Effective internal control is predicated on risk... the controls themselves – exist for the purpose of minimizing the risk of financial reporting errors”¹⁰. Fiona Williams of Deloitte & Touche summarizes the use of risk assessments in COSO by stating: “COSO requires a formal risk assessment be performed to evaluate the internal and external factors that impact an organizations performance. The results of the risk assessment will determine the controls that need to be implemented”¹¹.

⁴ COSO, Enterprise Risk Management Integrated Framework, Executive Summary, Sept 2004

⁵ BASEL II, Basel is the Swiss city where the Basel II Capital Proposal was initiated, <http://www.federalreserve.gov/generalinfo/basel2/default.htm>

⁶ Sarbanes Oxley (SOX) : Sarbanes Oxley Act of 2002, Officially titled the Public Company Accounting Reform and Investor Protection Act of 2002. Created to protect investors by improving the accuracy and reliability of corporate disclosures

⁷ HIPAA: Health Insurance Portability and Accountability Act of 1996. Address the security and privacy of health data

⁸ Gramm-Leach-Bliley Act of 1999 also known as the Financial Modernization Act of 1999 controls the ways that financial institutions deal with the private information of individuals

⁹ James Lam, *Enterprise Risk Management: From Incentives to Controls*

¹⁰ <http://en.wikipedia.org/wiki/Sarbanes-Oxley> ACT

¹¹ Fiona Williams, Deloitte & Touche - Security Services Worldwide, <http://www.csoonline.com/read/080104/counsel.html>

Risk Assessment and Transparency

A risk assessment should be one of the first steps in creating a culture of transparency. Controls are designed to mitigate risks to critical assets identified during the risk assessment process. Any implementation of controls without identifying the critical assets may result in a loss of focus in satisfying the critical components within the governance process. Controls may be placed on non-critical assets using scarce organizational resources that could be utilized more effectively.

The Standards for the Professional Practice of Internal Auditing published by the Institute of Internal Auditors provide the following definitions on controls and the control environment¹²:

Control: Any action taken by management, the board and other parties to enhance risk management and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

Control Environment: The attitude and actions of the board and management regarding the significance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:

- Integrity and ethical values
- Management's philosophy and operating style
- Organizational structure
- Assignment of authority and responsibility
- Human resource policies and practices
- Competence of personnel

Regardless of the “tone at the top” in the corporate culture, management ultimately assumes the burden of risk associated with running the business and responsibility for implementing a risk management program.

IT GOVERNANCE

IT governance can be viewed as a component framework within an overall ERM program. IT governance aims to align culture, people, processes, performance and structure with the business strategy and objectives of the organization as a whole.

¹² Institute of Internal Auditors: <http://www.theiia.org/>

The criticality of IT and IT Governance arises from:

- increasing dependence on information and the systems and communications that deliver them
- dependence on entities beyond the direct control of the enterprise
- IT failures or breaches increasingly impacting reputation and enterprise value
- the potential for technologies to dramatically change organizations and business practices, create new opportunities and reduce costs
- the risks of doing business in an interconnected world
- the need to build and maintain knowledge essential to sustain and grow the business

IT Governance is designed to add transparency to corporate reporting. Putting together a culture and practice of transparency is an arduous and continuous process which does not happen overnight. Companies are being regulated into IT Governance by legislation like SOX. In order for IT Governance and SOX to become a business advantage instead of an on-going expense, corporations must gain tangible repeatable results from the process. The initial implementations of a SOX compliance program have been reported to be expensive. Audit fees for the Fortune 1000 increased by an average of \$2.3 million, or 66 percent, between 2003 and 2004, according to a study issued last month by professors at the University of Nebraska at Omaha¹³.

ISACA and IT Governance

The Information Systems Audit and Control Association (ISACA) adopted the following seven criteria¹⁴ that an information technology system must meet for an adequate IT governance program:

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

The criteria set out by ISACA are similar to those contained within the National Institute of Standards and Technology special publication 800-53 – Recommended Security Controls for Federal Information Systems, and the detailed information security standard ISO 17799. The methodologies and standard stress the importance of using a risk based approach to managing information security - specifically managing risks to the confidentiality, integrity, and availability of critical information. Conducting a risk

¹³ Johnson, Carrie, "Higher Audit Fees, More Accountability, Sarbanes-Oxley, Three Years Later", WashingtonPost.com, July 30, 2005, <http://www.washingtonpost.com/wp-dyn/content/article/2005/07/29/AR2005072901741.html> (8/02/05)

¹⁴ Information Systems Audit and Control Association, "IS Standards, Guidelines and Procedures for Auditing and Control Professionals, Section 3.1.3", March 2005.

assessment that takes input from all levels and facets of the organization is a good way to begin to build a corporate awareness of business risks and the consequences of risk.

OCTAVE and Risk Identification

Before risks can be managed, they must be identified. Risk is not objective; it is subjective and unique to the environment. A risk assessment may produce different results at different times in the business life cycle. However, the method used to conduct the risk assessment must be repeatable, standardized, and integral to the corporate culture. A methodology such as OCTAVE places the focus on the overall business risks and knowledge transfer gained from conducting self-directed assessments. OCTAVE is different from typical technology-only focused assessments and is centered on operational issues that balance risk, security policies, and technology with business objectives.

In 2001, U.S. Army Medical Research and Materiel Command (MRMC) established the Defense Healthcare Information Assurance Program (DHIAP) to develop a new self directed approach for evaluating and managing risk in their organizations. The OCTAVE methodology was the output of this program and provides a self-directed, tested, repeatable process. The OCTAVE processes document security requirements for an organization's critical information assets, determines threats and the risk of those threats being realized, and (with consideration of both the likelihood of the threat occurring and the cost of addressing it) develop plans and actions for mitigating the threats. The OCTAVE methodology was developed by Carnegie Mellon's Software Engineering Institute to be useful not only in the medical community but all organizations requiring risk assessment. To date, the methodology has been used successfully in the financial, insurance, medical, airline, automotive, and general manufacturing industries as well as agencies of the federal government.

The OCTAVE risk assessment methodology is a documented, tested, proven and repeatable process for assessing the organizational and technical risks to an information system. This risk assessment methodology is an ideal complement to instituting an enterprise risk management program in any organization.

Regulatory Mandates for Risk Management

SOX is unlike Y2K, a one-time event that will go away when completed. It is here to stay for the foreseeable future and the penalties for non-compliance are real. In November 2004, the US broadened the scope of its federal sentencing guidelines to include more emphasis on a more forward-looking and active involvement by management in the organization's compliance program as well as a more dynamic process to evaluate its effectiveness. The new standards require that an effective compliance program be proactive, that is, the program must take "reasonable steps to prevent illegal conduct in organizational activities."¹⁵ The other significant change to the

¹⁵ See United States Sentencing Commission, Guidelines Manual, §8B2.1 (a), Nov. 2002

sentencing guidelines is that programs have to be proactive, not reactive. The prior guidelines required an organization to re-evaluate its compliance program *after* an offense had been detected; the new guidelines require an organization periodically assess whether criminal conduct will occur.¹⁶

CONTROL FRAMEWORKS and RISK MANAGEMENT

ERM Frameworks

Numerous methodologies and/or frameworks have been proposed to define the components and processes involved in an effective ERM program.

Risk Management Frameworks ¹⁷		
Operational Risk	COSO, BASEL II	Audit/Maturity Models CMM, SAS70
IT Governance	CobiT, ITIL ¹⁸	
Information Security Management	ISO17799, FISMA ¹⁹ , GLBA ²⁰ , HIPAA, Systrust ²¹	
Detailed Policy Controls	NIST, FFIEC ²²	

Among the more popular with risk managers are COSO and CobiT. Both frameworks recommend the 1) Identification of risks from the perspective of different areas of the organization 2) Risk assessment, and 3) Risk Mitigation.

1) Common Methods to Identify Risks

- Objectives based- Any event that may endanger achieving an organizational objective partly or completely is identified as risk
- Scenario-based - Any event that triggers an undesired scenario alternative is identified as risk
- Taxonomy-based²³ - Based on the taxonomy and knowledge of best practices, a questionnaire is compiled. The answers to the questions reveal risks.
- Common-risk - Each risk in the pre-populated list can be checked for application to a particular situation

¹⁶ Guidelines Manual §8A1.2, (Commentary 3(k)(7))

¹⁷ Concept: Forrester Research

¹⁸ ITIL: documents used to aid the implementation of a framework for IT Service Management (ITSM)

¹⁹ FISMA: Federal Information Security Management Act of 2002

²⁰ GLBA: Gramm-Leach-Bliley Act

²¹ Systrust: principles to enable a CPA to evaluate the reliability of a system, American Institute of Certified Public Accountants, Inc.

²² FFIEC: Federal Financial Institutions Examination Council

²³ <http://www.sei.cmu.edu/publications/documents/93.reports/93.tr.006.html>

2) Risk Assessment - Once risks have been identified, they must then be assessed as to their potential severity of loss and to the probability of occurrence. The objective is to determine those risks to organization assets or objectives which have the highest likelihood of disrupting the organizations continued operations. If risks are improperly assessed and prioritized, time can be wasted in dealing with risk of losses that are not likely to occur or have negligible impact in the organization.

3) Risk Mitigation – techniques to manage risk. Usually involves trade-offs.

- Avoidance – usually cost prohibitive.
- Reduction (Mitigation) – reduce the severity of a potential loss.
- Transfer – another party to accepts the risk
- Retention (Acceptance) – all risk that are not avoided or transferred are retained by default.

COSO

Enterprise risk management consists of eight inter-related components derived from studies on how organizations are run. These components are integrated with management processes.²⁴ The Public Company Accounting Oversight Board has issued a guideline stating management should use an internal control framework such as COSO. The COSO framework describes how to assess the control environment and requires:

- determining control objectives,
- performing a risk assessments
- identification of adequate controls
- monitoring compliance.

Effective internal control is predicated on risk... the controls themselves – exist for the purpose of minimizing the risk of financial reporting errors.²⁵

The initial steps of COSO are:

- identifying the organizations' views and philosophy on risk.
- ensuring the organization has a process to align its' mission and objectives with its risk tolerance.
- identification of internal and external events affecting the achievement of an entities objectives
- distinguishing between risks and opportunities.

Following these activities, risks are analyzed (risk assessment) to consider the likelihood and impact and how the risks should be managed and implementing the

²⁴ COSO, Enterprise Risk Management Integrated Framework, Executive Summary, Sept 2004

²⁵ <http://en.wikipedia.org/wiki/Sarbanes-Oxley> ACT

controls necessary for adequate enterprise risk management. Figure 1 represents the relationships present in the COSO framework.

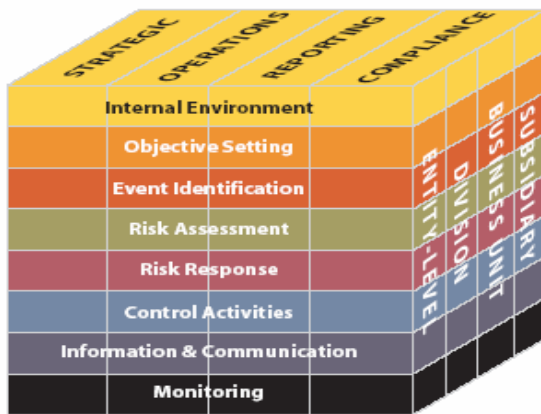


Figure 1: COSO Relationships

OCTAVE and COSO

The OCTAVE risk assessment methodology satisfies the COSO goals of

- establishing an organization view of risk and risk aversion
- determining and establishing the risk impact criteria
- focusing on critical areas that have a high impact to the organization
- comparing “best practices” to current organizational practices
- determining the risks in current technical IT controls and procedures
- establishing specific organizational best practices within a control framework
- providing an analysis framework for determining risk mitigation strategies
- establishing action plans to mitigate, avoid, transfer, or retain identified risks

Balancing Goals and Risk

Business value is maximized when strategy and objectives strike a balance between growth goals and related risks and deploys resources in pursuit of organizations objectives. The Institute of Internal Auditors defines risk as: "The uncertainty of an event occurring that could have an impact on the achievement of objectives. Risk is measured in terms of consequences and likelihood."

CobiT

ISACA states CobiT is 100 percent compliant with ISO17799, COSO I and COSO II, and maps onto many other related standards²⁶. Figure 2 reflects the importance of the risk assessment to the entire CobiT framework. Step two of the compliance process

²⁶ ISACA, IT Control Objectives for Sarbanes-Oxley, April 2004

calls for a risk assessment. CobiT does not specify or recommend a specific type of risk assessment methodology leaving the decision to each specific organization or auditor. The role of the internal auditor in implementing an enterprise risk management framework varies. Some would argue that the focus on SOX has created a culture focused on the minutia of financial reporting and procedures instead of creating a culture of “risk management” .²⁷

Transitioning from a documentation culture focused on internal controls (financial) to a culture aware of business risks and the management of those risks is necessary to gain lasting value from the compliance process. There is a real need to move away from a singular focus (financial controls) to a process improvement and strategic model of risk management that includes all the controls necessary for the whole organization. Auditors need to undergo additional focused training on risk management to understand the bigger business picture and to leverage the documented processes completed for SOX. A properly implemented ERM program provides a link between auditors and risk managers, and auditors and information security

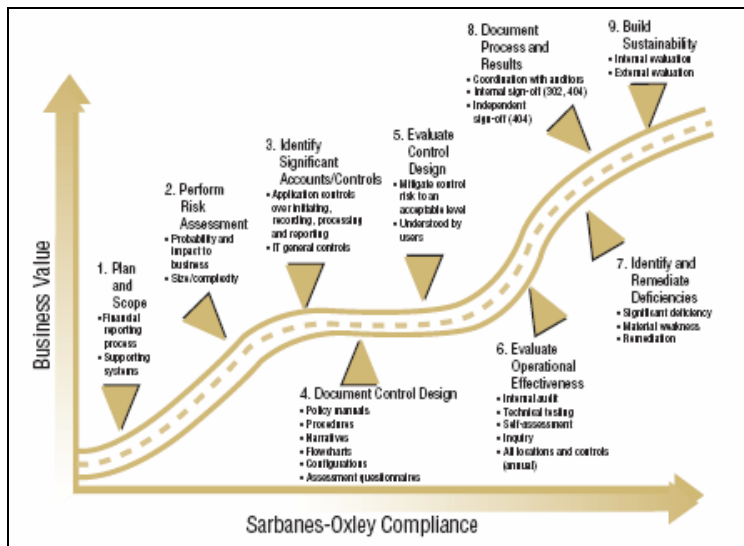


Figure 2: Risk Assessment in CobiT

COSO and CobiT Comparison

Both COSO and CobiT can be considered as member components of an overall enterprise risk management framework that also includes financial controls and other management controls. COSO and CobiT are directed toward different audiences. COSO’s target audience is management at large SEC-regulated companies whereas

²⁷ Sammer, J. Companies migrating from SOX “myopia” to ERM. *Compliance Week*, October 26, 2004

CobiT is intended for management, users, and auditors (mostly IT auditors). Both COSO and CobiT view control as an entity-wide process, with COSO focused on business and financial controls and CobiT focused on IT controls. This distinction defines and to a large degree determines the scope of each control framework²⁸.

Within COSO a risk assessment is a primary step (Step 2) within the framework, while CobiT considers the risk assessment to be one process within the planning and organization process (PO process 9.0). The Institute of Internal Auditors (IIA) recommends that COSO be the primary SOX reference with CobiT as the secondary source.

In particular, CobiT's Management Guidelines contain a framework responding to the need for control and measurability of IT by providing tools to assess and measure enterprise IT capability for the 34 CobiT IT processes. The tools include:

- Performance measurement elements (outcome measures and performance drivers for all IT processes).
- A list of critical success factors that provides succinct, non-technical best practices for each IT process.
- Guidance to enable an enterprise to implement effective governance over IT.
- Maturity models to assist in benchmarking and decision-making for capability improvements.

The CobiT framework was designed to address IT concerns.

CobiT has been developed by the IT Governance Institute as a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners.

OCTAVE Risk Assessment Methodology

The OCTAVE methodology can be utilized as the risk assessment methodology for sustainable SOX compliance. The OCTAVE methodology is currently being used to perform risk assessments within the health care domain (HIPAA), federal government information systems domain (FISMA) and the U.S. Department of Defense (DITSCAP) domain. The OCTAVE Methodology's combination of a Catalog of Practices with a tested, proven and repeatable process for assessing the organizational and technical risks has been shown to be well-suited to giving entities a solid start in risk assessment, assessment of threats, and risk management. The OCTAVE methodology is framework neutral and may be used for the risk assessment component/process for COSO and CobiT

In addition to COSO and CobiT, there is a need for a risk management methodology that allows the most critical assets of the enterprise to be protected.

²⁸ Institute of Internal Auditors: <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5553>

OCTAVE, The Operationally Critical Threat, Asset, and Vulnerability Evaluation is designed for an organization to gain understanding of their vulnerabilities from risks and tailor a plan to mitigate significant risks in their environment rather than applying scarce resources in an imprudent manner.

CONCLUSIONS

Most organizations are aware of the importance of protecting their critical business assets from the increasingly hostile environment of security threats, privacy concerns, legislation, and strict regulatory oversight. Managing the security and integrity of the corporate infrastructure, while at the same time allowing appropriate access to confidential information, has become a primary concern for organizational managers. Using COSO for business and financial processes, CobiT for IT processes and OCTAVE for overall enterprise risk assessment and mitigation planning can pay great dividends in streamlining operations and moving towards a proactive security posture. A company could time risk assessments to coincide with periodic internal control evaluations and disclosure requirements, thereby instilling the values of transparency, ethics and governance, and oversight in the company's culture.