Technically Speaking: Control Activities Over Technology and the New COSO

Presenters:
Stephen W. Blann, Principal, Rehmann
Bert Nuehring, Partner, Crowe Horwath LLP
Scott M. Petree, Senior Manager, Plante & Moran, PLLC

Date: May 20, 2014, 2:00 – 3:40 pm
Agenda

- Review of COSO – Background and Framework
- Key Areas of IT Risk
- Information Security Framework by COSO
- Codification of Framework
- IT Controls
- Current and New Technology
- A Practical Approach to IC for Smaller Governments
- Published Documents about COSO
REVIEW OF COSO
BACKGROUND AND FRAMEWORK
COSO Project Background

- In November 2010, COSO announced a project to review and update the Internal Control – Integrated Framework (Framework) originally issued in 1992.
- The decision to revise the original Framework was driven by the following factors:
  - The COSO Board’s desire to make the Framework more relevant and useful
  - Business and operating environments have become more complex, technologically driven and global in scale since the original Framework was issued more than twenty years ago
  - Key stakeholders are more engaged and are seeking greater transparency and accountability for the integrity of “systems of internal control” that support business and governance
- The Board of Directors of COSO approved the updated Framework and issued it on Tuesday, May 14, 2013. It incorporates input from various organizations (e.g., AICPA, IIA, Public Accounting Firms, Regulators, etc.) and nearly 1,000 key stakeholders. The majority of respondents supported updating, but not overhauling the Framework.
- The revised Framework is expected to help organizations reduce risk, improve compliance, and strengthen internal controls.
Integrated Framework: Overview

- First published in 1992
- Gained wide acceptance following the financial control failures in the early 2000’s and initial SOX years
- Most widely used *Framework* for evaluating controls in the U.S
- Widely used around the world
- Most companies publicly disclose if they are following the Framework
Integrated Framework: Project Objectives

Original Framework


- Address Significant Changes to the Business Environment and Associated Risks
- Codify Criteria Used in the Development and Assessment of Internal Control
- Increase Focus on Operations, Compliance and Non-Financial Reporting Objectives

Enhancement Objectives

- Updated, Enhanced and Clarified Framework
- Seventeen Principles Aligned With the Five Components of Internal Control
- Expanded Internal and Non-Financial Reporting Guidance

Key Changes

Updated Framework

COSO, COBIT

- General internal control - COSO
- Information technology internal control – COBIT
- Control Objectives for Information & related Technology (COBIT)
- Developed by ISACA - Information Systems Audit & Control Association
Information Criteria

**EFFECTIVENESS**
Deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.

**EFFICIENCY**
Concerns the provision of the information through the optimal use of resources.

**CONFIDENTIALITY**
Concerns the protection of sensitive information from unauthorized disclosure.

**INTEGRITY**
Relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.

**AVAILABILITY**
Relates to the information being available when required by the business process now and in the future.

**COMPLIANCE**
Deals with complying with laws, regulations and contractual arrangements.

**RELIABILITY OF INFORMATION**
Relates to the provision of appropriate information for the workforce of the organization.
Control Objectives

2 Plan and Organize
- Define Strategic IT Plan
- Define Information Architecture
- Determine Technological Direction
- Manage IT Investment
- Manage IT Human Resources
- Assess & Manage IT Risks
- Manage Projects

3 Acquire and Implement
- Identify Automated Solutions
- Acquire & Maintain Application Software
- Acquire & Maintain Technology Infrastructure
- Enable Operation & Use
- Procure IT Resources
- Manage Changes
- Install & Accredit Solutions & Changes

4 Deliver and Support
- Define & Manage Service Level
- Manage Third-party Services
- Ensure Continuous Service
- Manage Performance & Capacity
- Identify & Allocate Costs
- Manage Service Desk & Incidents
- Manage Configuration
- Manage Problems
- Manage Data
- Manage Physical Environment
- Manage Operations

5 Monitor and Evaluate
- Monitor & Evaluate IT Performance
- Monitor & Evaluate Internal Control
- Ensure Regulatory Compliance
- Provide IT Governance
IT risk for governmental organizations – Starts with Risk Assessment
Where is my data?

- Type
- Storage
- Usage
- Sharing
Where is my data?

Exercise 1: Identify the types of data you manage

a) Public

b) Confidential / Sensitive

c) Private
Where is my data?

Type
Storage
Usage
Sharing

Exercise 2: Where is your data?

a) Portable disk drives
b) Employee desktops
c) Network folders
d) Network Folders / Servers
e) Online storage
   • Public
   • Private
f) Third-parties
g) Mobile devices (e.g. iPads)
h) Don’t know
Where is my data?

Type

Storage

Sharing

Exercise 3: Who & how are you sharing your data?

a) Who

- Family office employees
- Family members
- Employees of related family organizations
- Other third-parties

b) How are you sharing data

- E-mail
- Online portals
- Secure/encrypted media
What can go wrong?

Exercise 4: Identify threats to your data
a) Confidentiality
   a) Availability
b) Integrity
Use of mobile technology

Account Hijacking

Social Media

Cloud Computing
How can we fix it?
Information Security Framework
Risk-Based Information Security Process

- Perform an Information Security Risk Assessment
- Designate security program responsibility
- Develop an Information Security Program
- Implement information security controls
- Implement employee awareness and training
- Regularly test or monitor effectiveness of controls
- Prepare an effective Incident Response Procedure
- Manage vendor relationships
- Periodically evaluate and adjust the Information Security Program
IT Risk Assessment

- **Framework** - How to implement? NIST Standards 800-XX & Cybersecurity Framework Executive Order

- **IT Assets** - What should be protected?

- **Threats** - From what do the assets need protection and what is the likelihood that a threat will occur?

- **Impacts** - What are the immediate damages if the threat is realized (e.g. disclosure of information, modification of data)?

- **Consequences** - What are the long-term effects of the threat being realized (e.g. damage to reputation of organization, loss of business)?

- **Controls** - What are the effective security measures (security services and mechanisms) needed to protect the assets?

- **Residual Risk** - After implementation of the security controls, is the remaining risk acceptable?

<table>
<thead>
<tr>
<th>Phases</th>
<th>Identify Information Assets</th>
<th>Perform Criticality Analysis</th>
<th>Evaluate Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approach</td>
<td>Data</td>
<td>Private</td>
<td>Probability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Confidential</td>
<td>Impact</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sensitive</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Personal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Applications</td>
<td>Dependence</td>
<td>Inherent Risk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Functions</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Impact</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Infrastructure</td>
<td>Function</td>
<td>Controls in Place</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Complexity</td>
<td>Residual Risk</td>
</tr>
</tbody>
</table>
CODIFICATION OF FRAMEWORK
## COSO’s Codification of Framework Principles

<table>
<thead>
<tr>
<th>Control Environment</th>
<th>Risk Assessment</th>
<th>Control Activities</th>
<th>Information &amp; Communication</th>
<th>Monitoring Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Demonstrates commitment to competence</td>
<td>9. Identifies and analyzes significant changes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Enforces accountability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Companies will need to link their internal controls to the 17 principles.
Principles and Attributes Related to the Controls Activity Component

The organization selects and develops general control activities over technology to support the achievement of objectives:

- Determines dependency between the use of technology in business processes and technology general controls
- Establishes relevant technology infrastructure control activities
- Establishes relevant security management control activities
- Establishes relevant technology acquisition, development, and maintenance control activities
Information Technology Controls

- **Information Technology Controls** (or IT controls) are specific activities performed by persons or systems designed to ensure that business objectives are met.
- Subset of an enterprise's internal control.
- IT control objectives relate to the confidentiality, integrity, and availability of data and the overall management of the IT function of the business enterprise.
- IT controls are often described in two categories: IT general controls (ITGC) and IT application controls.
- ITGC include controls over the Information Technology (IT) environment, computer operations, access to programs and data, program development and program changes.
- IT application controls refer to transaction processing controls, sometimes called "input-processing-output" controls.
IT General Controls

Administrative Controls
- Policies
- Risk assessment
- Security responsibility
- User access process (new user, terminations, changes)
- Access authorization
- Security awareness & training
- Security incident response
- Contingency planning / data backup

Physical Controls
- Facility access controls
- Workstation controls
- Device and media controls

Technical Controls
- Authentication controls (password, etc.)
- Access controls (operating system, application)
- Audit controls (monitoring and testing)
- Encryption controls
- Architecture controls (firewalls, VPN, etc.)
- Configuration controls

Vendor Management Controls
- Contract language (confidentiality, ownership, regulatory and legal compliance)
- Security audit, SOC/SSAE 16
- Vendor access control
- Vendor copies of confidential information
IT General Controls

ITGC represent the foundation of the IT control structure. They help ensure the reliability of data generated by IT systems and support the assertion that systems operate as intended and that output is reliable. ITGC usually include the following types of controls:

• Control environment - controls designed to shape the corporate culture or "tone at the top"
• Change management procedures - controls designed to ensure changes meet business requirements and are authorized
• Source code/document version control procedures - controls designed to protect the integrity of program code
• Software development life cycle standards - controls designed to ensure IT projects are effectively managed
• Logical access policies, standards and processes - controls designed to manage access based on business need
IT General Controls

- ITGC controls (continued):
  - Incident management policies and procedures - controls designed to address operational processing errors.
  - Problem management policies and procedures - controls designed to identify and address the root cause of incidents.
  - Technical support policies and procedures - policies to help users perform more efficiently and report problems.
  - Hardware/software configuration, installation, testing, management standards, policies and procedures.
  - Disaster recovery/backup and recovery procedures, to enable continued processing despite adverse conditions.
  - Physical security - controls to ensure the physical security of information technology from individuals and from environmental risks.
IT Application Controls

- IT application or program controls are fully automated (i.e., performed automatically by the systems) designed to ensure the complete and accurate processing of data, from input through output.

- Categories of IT application controls may include:
  - Completeness checks - controls that ensure all records were processed from initiation to completion
  - Validity checks - controls that ensure only valid data is input or processed
  - Identification - controls that ensure all users are uniquely identified
  - Authentication - controls that provide an authentication mechanism in the application system
  - Authorization - controls that ensure only approved business users have access to the application system
  - Input controls - controls that ensure data integrity fed from upstream sources into the application system
  - Forensic controls - control that ensure data is scientifically correct and mathematically correct based on inputs and outputs
Assessing ITGC

- IT controls that typically are assessed may include:
  - Specific application (transaction processing) control procedures that directly mitigate identified financial reporting risks.
  - IT general controls that support the assertions that programs function as intended and that key financial reports are reliable.
  - IT operations controls, which ensure that problems with processing are identified and corrected

- Specific activities that may occur to support the assessment of the key controls above include:
  - Understanding the organization’s internal control program and its financial reporting processes
  - Identifying the IT systems involved in the initiation, authorization, processing, summarization and reporting of financial data
Assessing ITGC

- Specific activities that may occur to support the assessment of the key controls above include (continued):
  - Identifying the key controls that address specific financial risks
  - Designing and implementing controls designed to mitigate the identified risks and monitoring them for continued effectiveness
  - Documenting and testing IT controls
  - Ensuring that IT controls are updated and changed, as necessary, to correspond with changes in internal control or financial reporting processes
  - Monitoring IT controls for effective operation over time
ITGC and Financial Reporting

- Organizations must understand how the financial reporting process works and must be able to identify the areas where technology plays a critical part.
- In considering which controls to include in the program, organizations should recognize that IT controls can have a direct or indirect impact on the financial reporting process.
- Access controls exist within these applications or within their supporting systems, such as databases, networks and operating systems, are equally important, but do not directly align to a financial assertion.
- Application controls are generally aligned with a business process that gives rise to financial reports.
CURRENT AND NEW TECHNOLOGY
Spreadsheets or Databases

- Spreadsheets or databases are often used to provide critical data or calculations related to financial reporting.
- Financial spreadsheets are often categorized as end-user computing (EUC) tools that have historically been absent traditional IT controls:
  - They can support complex calculations and provide significant flexibility.
  - Flexibility and power come with the risk of errors,
  - an increased potential for fraud, and
  - misuse for critical spreadsheets not following the software development lifecycle.
- To remediate and control spreadsheets, public organizations may implement controls such as:
  - Inventory and risk-rank spreadsheets that are related to critical financial risks identified.
  - Identify key estimates and judgments of the enterprise, where sophisticated calculations and assumptions are involved.
  - Spreadsheets used merely to download and upload are less of a concern.
Spreadsheets or Databases

- Perform a risk based analysis to identify spreadsheet logic errors. Automated tools exist for this purpose.
- Ensure the spreadsheet calculations are functioning as intended (i.e., "baseline" them).
- Ensure changes to key calculations are properly approved.
- Responsibility for control over spreadsheets is a shared responsibility with the business users and IT.
  - The IT organization is typically concerned with providing a secure shared drive for storage of the spreadsheets and data backup.
  - The business personnel are responsible for the accuracy of the information.
Information security risks increase with the reliance on cloud computing;
Inter-organizational connectivity has expanded by leaps and bounds; computer hacking is commonplace; and
Data is often shared instantly without human review.
All of these factors led to COSO’s conclusion that IT controls must be explicitly considered for the Cloud.
Cloud Governance Components – Consumer
Cloud Governance Program

- **Corporate strategy** – Align your cloud strategy with your corporate and IT vision.
- **Business case creation** – Define requirements and criteria for moving business processes to the cloud.
- **Vendor selection** – Thoroughly assess vendors against defined criteria to verify that they meet business requirements.
- **Contract negotiation** – Set SLAs; review contracts to allow for SSAE 16 or the right to audit, and the right to access data in the event of termination.
- **Implementation** – Perform testing and migration with business process owners.
- **Operations** – Enforce SLAs with vendors, review independent auditor reports, monitor incident response, and perform periodic security assessments.
- **Termination and transition** – Establish predefined exit and transition strategy.
- **Vendor management** – Enforce SLAs with vendors, assess vendor continued financial viability, and confirm that vendor strategic direction continues to align with the organization’s strategy.
Sample Cloud Computing Control Areas

- Vendor and Contract Management
  - Vendor Reviews
  - Service Level Agreement Monitoring
  - SSAE 16 Report Reviews

- Logical Access
  - User Management Processes (new user access, changes to user access, terminations)
  - Segregation of Duties
  - Administrative Access

- Operations
  - Batches/Interfaces
  - Backup
  - Disaster Recovery/Business Continuity Planning

- Change Management
  - Application Change Management
  - System Development Life Cycle / System and Data Conversion

- Data Governance
  - Data Classification
Social Media Definitions

- **Wikipedia**: Social media includes web-based and mobile based technologies which are used to turn communication into interactive dialogue among organizations, communities, and individuals. Social media is ubiquitously accessible, and enabled by scalable communication techniques.

- **Merriam Webster**: Forms of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos).

- **About.com**: Social media is a type of online media that expedites conversation as opposed to traditional media, which delivers content but doesn’t allow readers/viewers/listeners to participate in the creation or development of the content.
# Social Media Risks

## Anticipated Risks

<table>
<thead>
<tr>
<th>Category</th>
<th>Risks</th>
</tr>
</thead>
</table>
| **Legal & Regulatory Compliance** | • Disclosure of confidential information  
• Violation of copyright laws  
• Protection of intellectual property rights  
• Legal and financial ramifications for non-compliance with industry regulations |
| **Security & Privacy**           | • Identity theft, social engineering  
• Ability to retain and log social media communication; data retention  
• Technical exploits: malware, viruses/worms, flash vulnerabilities, XML injection |
| **Brand and Reputation Damage**  | • Posting unfavorable or confidential information on a public site  
• Unclear behavioral expectation of end users to use social media  
• Defamation, copyright infringement |
| **Productivity Drop**            | Use of social media can be distracting |

40
Social Media

- Develop a comprehensive social media policy
- Limit employee use of personal social networking sites for business purposes
- Be cautious of employer use of social media during the hiring process
- Manage risks associated with third-party content
- Comply with substantive content requirements
- Review and monitor social media content
- Keep records of social media
A PRACTICAL APPROACH TO INTERNAL CONTROL FOR SMALLER GOVERNMENTS
COSO – One Size Fits All?

- In 2006, COSO issued a tailored version of its 1992 report, entitled *Guidance for Smaller Public Companies*
- Not specifically targeted at governments, but helpful nonetheless
- Emphasizes the cost vs. benefit principle of internal control
Cost vs. Benefit

- COSO defines internal control as:
  - A process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding:
    - Effectiveness and **efficiency** of operations
    - Reliability of financial reporting
    - Compliance with applicable laws and regulations
  - Cannot provide **absolute** assurance
“Small” vs. “Smaller”

- There is no “bright line” to define governments as small, medium-size or large
  - Fewer types of services provided
  - Fewer personnel, many having a wider range of duties
  - Fewer levels of management, with wider spans of control
  - Less complex transaction processing systems and protocols
Challenges for Smaller Governments

- Maintaining cost-effective internal control:
  - Managers that view internal control as a burden, rather than a benefit
  - Obtaining sufficient resources for adequate segregation of duties
  - Management’s ability to dominate activities and override internal control
  - Recruiting/retaining personnel with sufficient experience and skill in financial reporting and/or computer information systems
Challenges for Smaller Governments

- Potential solutions:
  - Wide and direct control from the top
  - Effective governing bodies
  - Compensating for limited segregation of duties
  - Information technology
  - Monitoring activities
Control from the Top

- Smaller governments may have one or more members of senior management that have an in-depth understanding of virtually all of the government’s operations
  - Can enhance effectiveness of internal control
  - Enables leaders to know what to expect and follow up on differences
  - Adds to risk of management override
Effective Governing Bodies

- Smaller governments have less complex structures, and may have more involved boards
  - Direct exposure to management
  - Careful review of monthly reporting, with follow-up questions
  - Extensive public transparency
Compensating for Limited SOD

- When it isn’t practical to fully segregate all duties, introduce supervision and review
  - Two sets of eyes are better than one
Information Technology

- Smaller governments tend to rely on “off-the-shelf” software
  - Not risk-free, but lower risk
  - Built-in features for limiting access
  - Be sure to use audit-trails, flags, and exception reports if available
Information Technology

- Securing important spreadsheets from accidental or unauthorized changes
Monitoring Activities

- Monitoring is an important part of the COSO Framework.
  - Management of smaller governments regularly perform such procedures, but have not always taken sufficient “credit” for their contribution to internal control effectiveness
  - Usually performed manually, but may rely on technology
Controls vs. Processes

- It is easy to confuse the processes used to create transactions with the controls designed to prevent or detect errors in those transactions.
- Smaller governments frequently use IT systems to process financial transactions, but design manual controls to review the output of those systems.
Automated vs. Manual Controls

- Generally Accepted Auditing Standards (GAAS) recognize the difference between automated and manual controls (AU-C 315.A53)
  - Manual controls may be independent of IT or may use information produced by IT
  - Smaller governments may need to rely more heavily on manual controls in the absence of a comprehensive set of IT controls
Achieving Further Efficiencies

- Controls should focus on financial reporting objectives directly applicable to the government’s activities and services:
  - Risk-based approach to internal control
  - Right-sizing documentation
  - Viewing internal control as an integrated process
Risk-based controls focus on quantitative and qualitative factors that potentially impact the reliability of financial reporting:

- Identify transactions or processes where something could go wrong
- Assess likelihood and significance
- Design controls specifically tailored to those risks
- Don’t rely on generic controls designed for “typical” governments without modification
Right-Sizing Documentation

red·tape *noun*

: excessive regulation or rigid conformity to formal rules that is considered redundant or bureaucratic and hinders or prevents action or decision-making
Right-Sizing Documentation

- Smaller governments should determine the nature and extent of their documentation needs
  - Promote consistency
  - Provide evidence of control effectiveness
  - While smaller governments may not require as formal documentation, certain elements (such as risk assessment) cannot be performed entirely in the CFO’s head
Viewing IC as an Integrated Process

- Remember the interrelationship of the 5 elements
  - Management has flexibility in choosing controls
  - Should adjust and improve controls over time
  - Effectiveness is measured overall, not by element
Final Thoughts

- Remember the objective of internal control
- Design IT controls that are consistent with the government’s risk assessment and resources
- Mitigate deficiencies in internal control with as much supervision and review as possible
  - Management
  - Governing body
  - Others within the organization
WHERE TO GET HELP?
Published Documents

The COSO Framework has been published in three volumes:

- **Executive Summary**: A high-level overview intended for the Board of Directors, Chief Executive Officer, other Senior Management, regulators, and standard setters
- **Framework and Appendices**: Sets out the Framework, including the definition of internal control and the components and principles supporting effective systems of internal control
- **Illustrative Tools for Assessing Effectiveness of a System of Internal Control**: Provides templates and scenarios that may be useful in applying the Framework

In addition, **Internal Control over External Financial Reporting: Compendium of Approaches and Examples** has been published to provide practical approaches and examples that illustrate how the components and principles set forth in the Framework can be applied in preparing external financial statements

The updated Framework and Compendium are available at [www.ic.coso.org](http://www.ic.coso.org)
QUESTIONS?