The New COSO Framework, PII and Data Security

October 30, 2014
Planned Topics

• New COSO Framework
  • Why update the original framework?
  • What is changing?
  • New areas of emphasis
  • Timing and transition
  • Impact and opportunities

• PII and Data Security
  • What is PII?
  • Common Frameworks
  • Risk Based Approach
Transition Commentary – Tone has become more aggressive

“SEC staff plans to monitor the transition for issuers using the 1992 framework to evaluate whether and if any staff or Commission actions become necessary or appropriate at some point in the future.”
Paul Beswick, Chief Accountant, Office of the Chief Accountant
U.S. Securities and Exchange Commission
May 30, 2013

“I continue to question whether all material weaknesses are being properly identified. It is surprisingly rare to see management identify a material weakness in the absence of a material misstatement.”
Brian T. Croteau, Deputy Chief Accountant, Office of the Chief Accountant
U.S. Securities and Exchange Commission
December 9, 2013

“Unfortunately, over the decades, we’ve seen multiple cycles in which company management and internal and external auditors simply didn’t get it right in the area of internal control, resulting in failures to effectively define, understand, implement, and assess internal control.”
Jeanette M. Franzel, Board Member
PCAOB
March 26, 2014
Background

- COSO is a joint initiative of five supporting organizations
  - Institute of Management Accountants (IMA)
  - American Accounting Association (AAA)
  - American Institute of Certified Public Accountants (AICPA)
  - Institute of Internal Auditors
  - Financial Executives International (FEI)

- 1992 Original Framework
  - Established a common internal control model against which companies and organizations may assess their control systems

- Enhancing the Original Framework
  - Updates to reflect changes in the business world over the past 20 years
Why Update the Original Framework?

Original Framework


- Reflect changes in business & operating environments
- Expand focus on operations, compliance and non-financial reporting objectives
- Articulate principles to facilitate the development and assessment of internal control

Refresh Objectives

Updated Framework


- Updated, clarified and enhanced framework
- Broadens application: internal and non-financial reporting
- Clarifies requirements: Principles & Points of Focus

Enhancements

What is Remaining the Same?

- The definition of internal control:
  A process, effected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.

- The three categories of objectives
- The five components of internal control
- The requirement to consider each of the five components to assess effectiveness
- The use of judgment in designing, implementing and evaluating the effectiveness of systems of internal control
What are the Key Changes?

• Principles-based approach

• 5 components of internal control

• 17 principles that must be present and functioning in an effective system of internal control

• 81 points of focus are typically important characteristics of the 17 principles
What are the Key Changes?

• 17 principles are aligned with each of the five components

• Requirements of COSO principles
  • Must be present and functioning
  • Must operate in an integrated manner

• Added Points of Focus for each principle
  • Important characteristics of principles
  • Items management can consider to determine if the principles are present and functioning
COSO Components & Principles

Update articulates principles of effective internal control

- **Control Environment**
  1. Demonstrates commitment to integrity and ethical values
  2. Exercises oversight responsibility
  3. Establishes structure, authority and responsibility
  4. Demonstrates commitment to competence
  5. Enforces accountability

- **Risk Assessment**
  6. Specifies suitable objectives
  7. Identifies and analyzes risk
  8. Assesses fraud risk
  9. Identifies and analyzes significant change

- **Control Activities**
  10. Selects and develops control activities
  11. Selects and develops general controls over technology
  12. Deploys through policies and procedures

- **Information & Communication**
  13. Uses relevant information
  14. Communicates internally
  15. Communicates externally

- **Monitoring Activities**
  16. Conducts ongoing and/or separate evaluations
  17. Evaluates and communicates deficiencies
Points of Focus

Control Environment Component

**Principle 1:** The organization demonstrates a commitment to integrity and ethical values

**Points of focus:**

- Sets the tone at the top
- Establishes standards of conduct
- Evaluates adherence to standards of conduct
- Addresses deviations in a timely manner

- Some points of focus may not be relevant
- May facilitate designing, implementing, and conducting internal control
- Not required to separately assess whether points of focus are in place
New Areas of Emphasis

• Risk assessment
  • Increased focus on risk assessment process, and responding to assessed level of risk
  • Risk assessment related to fraud (Principle 8)

• Information technology
  • 14 of the 17 Principles include IT considerations
  • Includes IT general controls, and quality of data used to execute controls (Principle 13)

• Outsourced service providers (OSPs)
  • 12 of the 17 principles address monitoring of control activities performed by third-parties
  • Management retains responsibility for the controls
Assessing the System of Internal Control

• To conclude that your system of internal control is effective:

  • The five components of internal control and all relevant principles must be:
    • present and functioning
    • operating together in an integrated manner

• If a relevant principle is not present and functioning, a major deficiency exists in the system of internal control
Timing and Transition

- Transition period: May 14, 2013 to December 15, 2014

- 2013 framework will supersede original framework at the end of the transition period

- During the transition period, entities reporting externally (and their auditors) should disclose whether the original or updated version of the framework was used

SEC staff plans to monitor the transition for issuers using the 1992 framework to evaluate whether and if any staff or Commission actions become necessary or appropriate at some point in the future.”

Paul Beswick, Chief Accountant, Office of the Chief Accountant
U.S. Securities and Exchange Commission
May 30, 2013
Next Steps

COSO has developed a plan to help guide the transition:

The Five-Step Transition

**STEP 1**
DEVELOP AWARENESS, EXPERTISE, AND ALIGNMENT

**STEP 2**
CONDUCT PRELIMINARY IMPACT ASSESSMENT

**STEP 3**
FACILITATE BROAD AWARENESS, TRAINING, AND COMPREHENSIVE ASSESSMENT

**STEP 4**
DEVELOP AND EXECUTE COSO TRANSITION PLAN FOR SOX COMPLIANCE

**STEP 5**
DRIVE CONTINUOUS IMPROVEMENT

The 2013 COSO Framework & SOX Compliance
Impact will Vary by Organization

• Evaluate the 17 principles.

• Map the existing internal controls to the 17 principles.

• Evaluate whether each of the 17 principles and each of the five components are present and functioning, both individually and together, and document your findings.

• Are there gaps? Does your system of internal control need to be updated to address all principles? Consider areas of emphasis.

• Update internal control documentation.
Public Company Auditor Perspective

- Auditors must evaluate whether the 17 principles are present and functioning by:
  - Reviewing a map of a company’s existing internal controls over financial reporting to the 17 principles
  - Evaluating any identified gaps
  - Define testing approach: Most likely to select controls impacting multiple principles and higher risk controls

- Expect questions on focus areas: Risk Assessment, IT and OSPs

- Auditors must evaluate deficiencies by considering:
  - Whether the 17 principles are present and functioning
  - Whether deficiencies, in aggregate, indicate a material weakness exists
  - ELCs are generally indirectly related to financial statements and their evaluation is typically more qualitative than quantitative
Risk of Not Remediating Gaps

- SEC criteria for classifying internal control deficiencies
  - Material Weakness
  - Significant Deficiency
  - Control Deficiency

- If a Material Weakness is present, management must conclude:
  - Principle is **NOT** present and functioning
  - System of Internal Control is **NOT** effective
Deficiency Assessment Examples

• Competence of Personnel
• Compensation Structure
• Vendor Management Program
• Data Quality
Other Opportunities

• Opportunity to refresh the internal control system and update controls documentation to evidence mapping

• Enhance controls around third-parties, IT systems, data security (including PII), and the quality and reliability of data

• Focus on all areas of reporting – including internal and non-financial reporting

• Update risk assessment processes, including fraud, as needed
Personally Identifiable Information (PII) and Data Security
Our environment is changing, and our privacy policies and procedures need to keep pace. There is an increasing expectation from consumers, employees, stakeholders and courts that personal data be appropriately protected.
What is Personally Identifiable Information (PII)

Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

<table>
<thead>
<tr>
<th>Stand Alone</th>
<th>Linked or Linkable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Security Number</td>
<td>Medical, Education, and Employment Information</td>
</tr>
<tr>
<td>Drivers License or State ID #</td>
<td>Mother’s Maiden Name</td>
</tr>
<tr>
<td>Passport #</td>
<td>Citizenship or Immigration Status</td>
</tr>
<tr>
<td>Alien Registration Number</td>
<td>Account Passwords</td>
</tr>
<tr>
<td>Financial Account Number, Credit Card Number</td>
<td>Last 4 digits of SSN</td>
</tr>
<tr>
<td>Biometric Identifiers</td>
<td>Date of Birth</td>
</tr>
<tr>
<td></td>
<td>Criminal History</td>
</tr>
</tbody>
</table>
# Example Regulations

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Key Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gramm-Leach-Bliley Financial Modernization Act (GLBA)</td>
<td>Federal mandate to protect financial information. Required federal financial agencies and state insurance regulators to establish standards for consumer privacy protection by the institutions they oversee.</td>
</tr>
<tr>
<td>Health Insurance Portability and Accountability Act (HIPAA)</td>
<td>Sets out guidelines for handling data that contains medical information about individuals created by a covered entity.</td>
</tr>
<tr>
<td>The Health Information Technology for Economic and Clinical Health (HITECH) Act</td>
<td></td>
</tr>
<tr>
<td>Sarbanes-Oxley Act of 2002 (SOX)</td>
<td>Publicly traded companies must implement and maintain internal controls for the protection of corporate financial information.</td>
</tr>
</tbody>
</table>
# Resulting Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Key Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAIC/s Standards for Safeguarding Customer Information Model Regulation</td>
<td>Standards insurance entities must meet to comply with GLBA’s information security provisions.</td>
</tr>
<tr>
<td></td>
<td>Insurance licensees must establish a comprehensive, written information security program that includes administrative, technical, and physical safeguards for protection of confidential data appropriate to the size and complexity of the licensee and the nature and scope of its activities.</td>
</tr>
<tr>
<td>Payment Card Industry (PCI) Security Standards of 2005</td>
<td>Issued by MasterCard and Visa to protect credit card data.</td>
</tr>
</tbody>
</table>
Breach Examples

- Target, TJX, Sony, eBay, Michaels Stores, Home Depot, JP Morgan Chase, etc.
- AvMed Settlement
  - Class Action Lawsuit—result of data breach in 2009
    - Two laptops were stolen that held unencrypted personal and health data of more than 1 million AvMed members and their dependents.
  - $3 million settlement
  - Financial redress for people who didn’t actually experience identify theft.
  - Separate claims may be filed by people that were victims of identify theft as a result of the breach.
Cost of a Data Breach

2014 Cost of Data Breach Study: United States Ponemon Institute, May 2014

Cost of a data breach have increased:
- Cost per lost or stolen record = $201
- Total average cost paid by organizations = $5.9 million
- Average rate of customer churn increase by 15%
- Cause of breaches:
  - 44% caused by malicious or criminal attack
  - 31% caused by employee negligence
  - 25% caused by system glitches
- Strong data security posture to prevent incident reduced cost by as much as $21 per record.
“In the battle to keep your personal information private, it’s not just hackers you have to worry about but lax security and stupidity.”

Martyn Williams, IDG News Service
“The 5 biggest data breaches of 2014 (so far)”
June 11, 2014
Data Security Frameworks

- ISO/IEC 27001:2013
- COBIT
- ITIL
- NIST - Cybersecurity Framework
- HITRUST CSF
- SoGP
- COSO

Figure 15—COBIT 5 Governance and Management Key Areas

ISACA: A Business Framework for the Governance and Management of Enterprise IT
Creating Awareness

• Policies and procedures
  • Comprehensive policies and procedures for handling PII
  • Foundational privacy principles and objectives
  • Privacy rules of behavior
    • Proper handling of PII
    • Consequences for failure to comply

• Awareness, training and education
  • Designed to change behavior or reinforce desired PII practices
  • Focus attention on the protection of PII
    • Use of attention-grabbing techniques
    • New scams
    • Data breaches

• Self-remediation
Process Overview

Inventory Data

Monitor

Classify Data

Data Classification Guide

Remediate

Assess Security

Training & Education

User Awareness Programs
Data Classification Guide

• A risk-based approach to determine what data must be protected
  • Foundation for identification, classification and remediation of PII
  • Defines how data and systems will be addressed at each classification level

<table>
<thead>
<tr>
<th>Example Classification Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highly Sensitive</td>
</tr>
<tr>
<td>Sensitive</td>
</tr>
<tr>
<td>Internal</td>
</tr>
<tr>
<td>Public</td>
</tr>
</tbody>
</table>

• In addition to **data confidentiality**, the classification can include broader considerations - **data integrity** and **data availability**
Process Overview

Inventory Data

Data Classification Guide

Monitor
Classify Data
Assess Security
Remediate

Training & Education
User Awareness Programs
1) Business process walkthroughs
   • Understand types of data accessed, systems and tools used, and controls in place
   • Determine where data is coming from, where it is stored, and where it is processed

2) IT data flow diagrams
   • Identify supporting applications and infrastructure
   • Identify other data locations (e.g., interfaces, data warehouses, shared folders, email, cloud providers)

3) Data discovery tools
   • PII, PHI, PCI, Intellectual property (custom searches)
Process Overview

Inventory Data

Classify Data

Data Classification Guide

User Awareness Programs

Training & Education

Monitor

Remediate

Assess Security
Classify Data

- Risk-rate the data, systems and infrastructure in terms of confidentiality, integrity and availability needs
- Information system owners review the pre-defined data categories in the Data Classification Guide to locate matches for all information system data for which they are responsible
- Data category is officially recorded for each data type processed or stored by the information system
- When all data types constituting the information system have been classified, the security categorization of the information system will be determined based on the most sensitive information received by, processed in, stored in, and/or generated by the system under review
- Once objectively categorized, and appropriate security and control requirements can be applied based on the data categorization
Process Overview

Data Classification Guide

- Inventory Data
- Classify Data
- Monitor
- Remediate
- Assess Security

Training & Education

User Awareness Programs
Data Management

• Communicate data classification standards and security procedures
• User awareness campaign
• Define life cycle for confidential/highly sensitive data
  • Creation/collection
  • Use
  • Storage/Data Retention
  • Delivery
  • Destruction
• Define data owners and data stewards
  • Make and implement decisions about data
Access Controls

- Restrict access to sensitive or confidential information through IT systems, email copy, and paper distribution
- Periodic access reviews for sensitive/confidential data
- Remove system access from personnel that no longer work with the organization or who have changed job roles
- Restrict vendor access to confidential data
- Encryption for transmission and storage of sensitive data
- Limit the number of paper copies of confidential data
- Store paper copies in locked cabinets
- Develop and adhere to email destruction policy
User Administration

• Onboarding/Off-boarding process
  • Internal personnel
  • Vendors
  • Contractors
  • Documentation

• Education
  • Orientation - new hire
  • Basics - security, data sensitivity, transmission
  • Internal policies and procedures
Configuration Management

- Inventory IT assets
- Define minimum configuration standards
- Limit access to modify configurations
- Periodic reviews to ensure compliance
- Penetration testing
Vendor Management

- Identify data involved and the related vendors
- Assess vendor controls over sensitive data
  - Questionnaires
  - Right to audit
  - Availability of service organization control reports (SOC 1/2)
- Maintain contract requirements
  - Monitor regulations and update requirements
  - Communicate changes
Process Overview

Data Classification Guide

- Inventory Data
- Monitor
- Classify Data
- Assess Security
- Remediate

User Awareness Programs

Training & Education
Remediation

• Define a process to safely destroy PII that is no longer relevant and necessary

• De-identifying information
  • Masking/obscurity portions of the PII
  • De-identified information can be re-identified

• Anonymizing information
  • De-identified information where the code for re-identification no longer exists

• Minimize the use, collection, and retention of PII
  • Limit PII collections to the least amount necessary
Process Overview

Inventory Data

Data Classification Guide

Classify Data

Assess Security

Remediate

Monitor

Training & Education

User Awareness Programs
Monitor

• Evaluate remediation and ensure compliance with data security policies and procedures

  • Run data discovery or DLP tools
  • Test access to sensitive data
  • Test logical access processes (provisioning/de-provisioning)
Incident Response Plan for PII

• Preparation
  • Ability to respond quickly is critical (reporting 24/7)
  • Clearly define the information to be reported
  • Insurance

• Detection and analysis
  • Did the incident involve PII?

• Containment, eradication, and recovery
  Was PII accessed? How many records were affected?

• Post-incident activity
  • Lessons learned / continually update incident response plan
  • Providing individuals with remedial assistance (e.g., credit monitoring)
Resources – Data Security

- **NAIC Financial Condition Examiners Handbook**
  - Requires an IT review as part of regulators’ examination process and provides guidance to identify information security risks and evaluate the adequacy of controls and applicable risk management practices

- **NAIC Market Regulation Handbook**
  - Requires a review of computer security procedures to ensure insurance entities have appropriate controls, safeguards and procedures for protecting the integrity of customer information

- **NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)**
  - Provides guidelines for a risk-based approach to protecting the confidentiality of PII
Resources – New COSO Framework

• COSO
  • Internal Control – Integrated Framework Executive Summary
  • Internal Control – Integrated Framework and Appendices
  • Internal Control – Integrated Framework Internal Control over External Financial Reporting: A Compendium of Approaches and Examples
  • Internal Control – Integrated Framework Illustrative Tools for Assessing Effectiveness of a System of Internal Control

• AICPA
  • The Updated COSO Framework
Questions?