Integrating COBIT 5 With COSO 2013

Stephen Head
Senior Manager, IT Risk Advisory Services
Our Time This Evening

• Importance of Governance
• COBIT 5 Overview
• COSO Overview
• Mapping These Frameworks
• Stakeholder Expectations
• Implementation Considerations
• Other Frameworks/Guidance
• Questions
Why Is Governance Important?

**BUSINESS OUTCOMES OF GOVERNANCE OF ENTERPRISE IT (GEIT)**

- **42%** Improved management of IT-related risk
- **40%** Improved communication and relationships between business and IT
- **38%** Lower IT costs
- **37%** Improved IT delivery of business objectives
- **28%** Improved business competitiveness

*Source: ITGI Global Status Report on the Governance of Enterprise IT (GEIT) 2011.*
Use of Frameworks

IT Security and Risk Management Frameworks
Percentage of Respondents Using

- COBIT: 57.9%
- Internally Developed Framework: 11.6%
- COSO: 11.6%
- ISO 27000: 9.1%
- NIST: 5.0%
- ITIL: 2.5%
- Other: 2.5%

n = 121.
Source: CEB 2014 IT Audit Benchmarking Survey.
Allocation of IT Audit Hours by Framework

Allocations of IT Audit Hours by Type of Information Security Framework Used

Average Allocation

- **COBIT (n = 63)**
  - Change Controls: 14.9%
  - Software Development, Acquisition, Implementation, and Maintenance: 10.5%
  - Cyber Security: 8.4%
  - Data Privacy and Protection: 7.6%
  - Information Risk Governance: 6.5%
  - Third-Party Security: 4.7%

- **Internally Developed Framework (n = 12)**
  - Other IT Audit Work: 22.0%
  - Change Controls: 8.3%
  - Software Development, Acquisition, Implementation, and Maintenance: 16.3%
  - Cyber Security: 7.7%
  - Data Privacy and Protection: 5.2%
  - Information Risk Governance: 4.4%
  - Third-Party Security: 5.2%

- **COSO (n = 12)**
  - Other IT Audit Work: 18.8%
  - Change Controls: 11.9%
  - Software Development, Acquisition, Implementation, and Maintenance: 10.3%
  - Cyber Security: 12.5%
  - Data Privacy and Protection: 4.5%
  - Information Risk Governance: 4.3%
  - Third-Party Security: 3.7%

- **ISO 27000 (n = 9)**
  - Other IT Audit Work: 13.9%
  - Change Controls: 10.4%
  - Software Development, Acquisition, Implementation, and Maintenance: 7.8%
  - Cyber Security: 8.4%
  - Data Privacy and Protection: 13.7%
  - Information Risk Governance: 3.8%
  - Third-Party Security: 10.1%

Source: CEB 2014 IT Audit Benchmarking Survey

Note: Allocation does not add to 100%. Categories not included in the above chart are Software Quality and Effectiveness, Data Classification, Cloud Platforms, Management Planning and Organization of IT and/or IS, External Network Security, System Development Life Cycle, and Business Continuity and Disaster Recovery.
COBIT Overview
What Is COBIT?

- A Business Framework for the Governance and Management of Enterprise IT
- Accepted globally as a set of tools that ensures IT is working effectively
- Provides common language to communicate goals, objectives and expected results to all stakeholders
- Based on, and integrates, industry standards and good practices in:
  - Strategic alignment of IT with business goals
  - Value delivery of services and new projects
  - Risk management
  - Resource management
  - Performance measurement
COBIT 5 Key Areas

Source: COBIT 5 Framework, page 32, © 2012 ISACA. All rights reserved.
Processes for Governance of Enterprise IT

Source: COBIT 5 Framework, figure 16, page 33. © 2012 ISACA. All rights reserved.
### DSS04 Manage Continuity

**Area:** Management  
**Domain:** Deliver, Service and Support

#### Process Description
Establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the enterprise.

#### Process Purpose Statement
Continue critical business operations and maintain availability of information at a level acceptable to the enterprise in the event of a significant disruption.

The process supports the achievement of a set of primary IT-related goals:

<table>
<thead>
<tr>
<th>IT-related Goal</th>
<th>Related Metrics</th>
</tr>
</thead>
</table>
| 04 Managed IT-related business risk | • Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment  
• Number of significant IT-related incidents that were not identified in risk assessment  
• Frequency of update of risk profile |
| 07 Delivery of IT services in line with business requirements | • Number of business disruptions due to IT service incidents  
• Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels  
• Percent of users satisfied with the quality of IT service delivery |
| 14 Availability of reliable and useful information for decision making | • Level of business user satisfaction with quality and timeliness (or availability) of management information  
• Number of business process incidents caused by non-availability of information  
• Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor |

Source: *COBIT 5 Enabling Processes*, page 185.  
© 2012 ISACA. All rights reserved.
### DSS04 Process Practices, Inputs/Outputs and Activities (cont.)

<table>
<thead>
<tr>
<th>Management Practice</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSS04.02 Maintain a continuity strategy.</td>
<td>From AP012.06</td>
<td>Description</td>
</tr>
<tr>
<td>Evaluate business continuity management options and choose a cost-effective and viable continuity strategy that will ensure enterprise recovery and continuity in the face of a disaster or other major incident or disruption.</td>
<td>Risk-related root causes</td>
<td>Business impact analyses</td>
</tr>
<tr>
<td></td>
<td>Risk impact communications</td>
<td>Continuity requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Approved strategic options</td>
</tr>
</tbody>
</table>

**Activities**

1. Identify potential scenarios likely to give rise to events that could cause significant disruptive incidents.
2. Conduct a business impact analysis to evaluate the impact over time of a disruption to critical business functions and the effect that a disruption would have on them.
3. Establish the minimum time required to recover a business process and supporting IT based on an acceptable length of business interruption and maximum tolerable outage.
4. Assess the likelihood of threats that could cause loss of business continuity and identify measures that will reduce the likelihood and impact through improved prevention and increased resilience.
5. Analyse continuity requirements to identify the possible strategic business and technical options.
6. Determine the conditions and owners of key decisions that will cause the continuity plans to be invoked.
7. Identify resource requirements and costs for each strategic technical option and make strategic recommendations.
8. Obtain executive business approval for selected strategic options.

Source: *COBIT 5 Enabling Processes*, page 187. © 2012 ISACA. All rights reserved.
COSO Overview
What is COSO?

Definition: COSO is a leading framework for designing, implementing, and conducting internal control and assessing the effectiveness of internal control.

COSO Internal Control Framework

22 years ago.....

- Most of the developments in business and technology that we take for granted today had not been realized
- Companies were just starting to connect through EDI
- Smartphones, Google, and Facebook did not exist
- Internet was still ramping up
- Most everyone used dial-up modems
- Internal Control evaluation was relatively unsophisticated
- Internal Auditors struggled to address evolving client-server networks
- Many of today’s financial reporting regulations had yet to be written

Source: Internal Auditor August 2013
Why COSO 2013?

- Business and operating environments have changed dramatically, becoming increasingly complex, technology driven, and global
- Large scale governance and internal control breakdowns have occurred in the last 20+ years
- Stakeholders are more engaged, seeking transparency and accountability
- Increased expectations for risk assessments at all levels of the organization (financial, operations, regulatory, IT)
### Summary of Changes

*The Update increases ease of use and broadens application*

<table>
<thead>
<tr>
<th>What did <em>not</em> change...</th>
<th>What did change...</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Core definition of internal control</td>
<td>• 17 Principles codified</td>
</tr>
<tr>
<td>• Three categories of objectives and five components of internal control</td>
<td>• Role of objective setting clarified</td>
</tr>
<tr>
<td>• Each of the five components of internal control are required for effective internal control</td>
<td>• Reflects increased role and relevance of technology</td>
</tr>
<tr>
<td>• Important role of judgment in designing, implementing and conducting internal control, and in assessing its effectiveness</td>
<td>• Incorporates enhanced discussion of governance</td>
</tr>
<tr>
<td></td>
<td>• Expands “Reporting” objective</td>
</tr>
<tr>
<td></td>
<td>• Enhances consideration of anti-fraud expectations</td>
</tr>
<tr>
<td></td>
<td>• Increases focus on non-financial reporting objectives</td>
</tr>
</tbody>
</table>
## COSO 2013

<table>
<thead>
<tr>
<th>5 Components</th>
<th>17 Principles</th>
<th>77 Points of Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Environment</td>
<td>Commitment to integrity and ethical values</td>
<td>4</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Independent board of directors oversight</td>
<td>4</td>
</tr>
<tr>
<td>Control Activities</td>
<td>Structures, reporting lines, authorities, responsibilities</td>
<td>3</td>
</tr>
<tr>
<td>Information &amp; Communication</td>
<td>Attract, develop and retain competent people</td>
<td>4</td>
</tr>
<tr>
<td>Monitoring Activities</td>
<td>People held accountable for internal control</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>6. Clear objectives specified</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>7. Risks identified to achievement of objectives</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>8. Potential for fraud considered</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>9. Significant changes identified and assessed</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>10. Control activities selected and developed</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>11. General IT controls selected and developed</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>12. Controls deployed through policies and procedures</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>13. Quality information obtained, generated and used</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>14. Internal control information internally communicated</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>15. Internal control information externally communicated</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>16. Ongoing and/or separate evaluations conducted</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>17. Internal control deficiencies evaluated and communicated</td>
<td>3</td>
</tr>
</tbody>
</table>

Source: COSO.org
COSO Mapping Coverage by Principle

Source: CEB analysis.
Mapping COBIT 5 to COSO 2013
## COSO 2013

<table>
<thead>
<tr>
<th>5 Components</th>
<th>17 Principles</th>
<th>77 Points of Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control Environment</strong></td>
<td>1. Commitment to integrity and ethical values</td>
<td>4</td>
</tr>
<tr>
<td><strong>Risk Assessment</strong></td>
<td>2. Independent board of directors oversight</td>
<td>4</td>
</tr>
<tr>
<td><strong>Control Activities</strong></td>
<td>3. Structures, reporting lines, authorities, responsibilities</td>
<td>3</td>
</tr>
<tr>
<td><strong>Information &amp; Communication</strong></td>
<td>4. Attract, develop and retain competent people</td>
<td>4</td>
</tr>
<tr>
<td><strong>Monitoring Activities</strong></td>
<td>5. People held accountable for internal control</td>
<td>5</td>
</tr>
<tr>
<td><strong>Clear objectives specified</strong></td>
<td>6. Clear objectives specified</td>
<td>5</td>
</tr>
<tr>
<td><strong>Risks identified to achievement of objectives</strong></td>
<td>7. Risks identified to achievement of objectives</td>
<td>5</td>
</tr>
<tr>
<td><strong>Potential for fraud considered</strong></td>
<td>8. Potential for fraud considered</td>
<td>4</td>
</tr>
<tr>
<td><strong>Significant changes identified and assessed</strong></td>
<td>9. Significant changes identified and assessed</td>
<td>3</td>
</tr>
<tr>
<td><strong>Control activities selected and developed</strong></td>
<td>10. Control activities selected and developed</td>
<td>6</td>
</tr>
<tr>
<td><strong>General IT controls selected and developed</strong></td>
<td>11. General IT controls selected and developed</td>
<td>4</td>
</tr>
<tr>
<td><strong>Controls deployed through policies and procedures</strong></td>
<td>12. Controls deployed through policies and procedures</td>
<td>6</td>
</tr>
<tr>
<td><strong>Quality information obtained, generated and used</strong></td>
<td>13. Quality information obtained, generated and used</td>
<td>5</td>
</tr>
<tr>
<td><strong>Internal control information internally communicated</strong></td>
<td>14. Internal control information internally communicated</td>
<td>4</td>
</tr>
<tr>
<td><strong>Internal control information externally communicated</strong></td>
<td>15. Internal control information externally communicated</td>
<td>5</td>
</tr>
<tr>
<td><strong>Ongoing and/or separate evaluations conducted</strong></td>
<td>16. Ongoing and/or separate evaluations conducted</td>
<td>7</td>
</tr>
<tr>
<td><strong>Internal control deficiencies evaluated and communicated</strong></td>
<td>17. Internal control deficiencies evaluated and communicated</td>
<td>3</td>
</tr>
</tbody>
</table>

Source: COSO.org
Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM03 Ensure Risk Optimisation
- EDM04 Ensure Resource Optimisation
- EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

- AP001 Manage the IT Management Framework
- AP002 Manage Strategy
- AP003 Manage Enterprise Architecture
- AP004 Manage Innovation
- AP005 Manage Portfolio
- AP006 Manage Budget and Costs
- AP007 Manage Human Resources
- AP008 Manage Relationships
- AP009 Manage Service Agreements
- AP010 Manage Suppliers
- AP011 Manage Quality
- AP012 Manage Risk
- AP013 Manage Security

Build, Acquire and Implement

- BAI01 Manage Programmes and Projects
- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build
- BAI04 Manage Availability and Capacity
- BAI05 Manage Organisational Change Enablement
- BAI06 Manage Changes
- BAI07 Manage Change Acceptance and Transitioning
- BAI08 Manage Knowledge
- BAI09 Manage Assets
- BAI10 Manage Configuration

Deliver, Service and Support

- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls

Processes for Management of Enterprise IT

Source: COBIT 5 Framework, figure 16, page 33. © 2012 ISACA. All rights reserved.
Mapping COBIT 5 to COSO 2013

Source: Relating The COSO Internal Control-Integrated Framework and COBIT. © 2014 ISACA. All rights reserved.
COSO Principle 1

The organization demonstrates a commitment to integrity and ethical values.

COBIT 5 Coverage:

• EDM01 Ensure Governance Framework Setting and Maintenance
• APO01 Manage the IT Management Framework
• APO07 Manage Human Resources
COSO Principle 2

The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

COBIT 5 Coverage:

- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM03 Ensure Risk Optimization
- EDM04 Ensure Resource Optimization
- EDM05 Ensure Stakeholder Transparency
COSO Principle 3

Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

COBIT 5 Coverage:

• EDM01 Ensure Governance Framework Setting and Maintenance
• APO01 Manage the IT Management Framework
COSO Principle 4

The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

COBIT 5 Coverage:

• APO01 Manage the IT Management Framework
• APO07 Manage Human Resources
COSO Principle 5

The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

COBIT 5 Coverage:

• All COBIT 5 Processes
COSO Principle 6

The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

COBIT 5 Coverage:

• All COBIT 5 Processes
COSO Principle 7

The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

COBIT 5 Coverage:

- EDM03 Ensure Risk Optimization
- APO12 Manage Risk
COSO Principle 8

The organization considers the potential for fraud in assessing risks to the achievement of objectives.

- COBIT 5 Coverage:
  - EDM01 Ensure Governance Framework Setting and Maintenance
  - APO01 Manage the IT Management Framework
  - APO07 Manage Human Resources
  - MEA03 Monitor, Evaluate and Assess Compliance With External Requirements
COSO Principle 9

The organization identifies and assesses changes that could significantly impact the system of internal control.

COBIT 5 Coverage:

- APO01 Manage the IT Management Framework
- BAI02 Manage Requirements Definition
- BAI05 Manage Organizational Change Enablement
- BAI06 Manage Changes
- BAI07 Manage Change Acceptance and Transitioning
COSO Principle 10

The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

COBIT 5 Coverage:

• All COBIT 5 Processes
COSO Principle 11

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

COBIT 5 Coverage:

• DSS06 Manage Business Process Controls
COSO Principle 12

The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

COBIT 5 Coverage:

• APO01 Manage the IT Management Framework
COSO Principle 13

The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

COBIT 5 Coverage:

• APO11 Manage Quality
• MEA01 Monitor, Evaluate and Assess Performance and Conformance
• MEA02 Monitor, Evaluate and Assess the System of Internal Control
COSO Principle 14

The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

COBIT 5 Coverage:

• APO01 Manage the IT Management Framework
COSO Principle 15

The organization communicates with external parties regarding matters affecting the functioning of internal control.

COBIT 5 Coverage:

• EDM05 Ensure Stakeholder Transparency
COSO Principle 16

The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

COBIT 5 Coverage:

- MEA02 Monitor, Evaluate and Assess the System of Internal Control
COSO Principle 17

The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

COBIT 5 Coverage:

- EDM05 Ensure Stakeholder Transparency
- MEA02 Monitor, Evaluate and Assess the System of Internal Control
Expectations
Regulatory Expectations

- What methodology does your organization use for IT governance?
- Regulatory Expectations (tomorrow’s expectations, not today’s expectations)
- Remember, you are aiming at a moving target
- How do you want to be viewed (A market leader, middle of the pack, or late adopter)
- Domestic vs. International Regulators
External Audit and Professional Expectations

- Can External Auditors rely on the work of Internal Audit?
- IIA Standard 1210 – Are you proficient if you are using outdated standards?
- IIA Standard 2110 – Are you making appropriate recommendations for improving the governance process?
Audit Committee Expectations

• In the opening keynote address at the 2014 Governance, Risk, and Control Conference, IIA Global Chairman Anton van Wyk made the point that 60% of board members want to spend more time on IT.

• Board members are growing increasingly concerned about IT governance and the organization’s ability to stand up to regulatory and public scrutiny.

• Don’t wait for an audit committee member to ask an embarrassing question (Have you implemented COBIT 5 and COSO 2013?)
Implementation Considerations
Implementation Considerations

• Getting from Point A to Point B
• Gap Assessment
• Management Support
• Project Plan/Manager/Sponsor
• Timing and Metrics
Implementation Considerations - Continued

- Lead time
- Metric weight factors and coverage
- Dashboard redesign
- Cutover point
Implementation Considerations - Continued

• Data Quality
• Upgrading/Creating SAPs
• Coordinating with Stakeholders
• Training
Integration COBIT 5 With COSO 2013

Transition Methodology

**Build Internal Awareness and Expertise**
- Build Awareness
  - Obtain Relevant Publications
- Revisit Concepts and Definitions
  - Internal Control Definition
  - Categories of Objectives
  - Control Components
  - Entity Structure
  - Management Judgment
- Understand the Principles
  - Principles (17)
  - Points of Focus
  - Approaches
  - Examples
- Understand Definition of Effective Internal Control
  - Present and Functioning
- Understand the Definition of Internal Control Deficiencies

**Perform Impact Assessment/ Prepare Project Plan**
- Revisit Existing Controls Documentation to Determine Adequacy
  - Financial Reporting Objectives
  - Risk Assessments
  - Significant Accounts / Disclosures
  - Assertions
  - Processes and Transactions
- Define the Project Plan and Methodology
  - Finalize Methodology and Approach
  - Define the Project Team
  - Develop the Project Plan

**Execute the Transition Plan**
- Documentation and Evaluation
  - Map the Principles and Components (Using Points of Focus, Approaches, and Examples) to the Existing Documentation
  - Confirm Existing Understanding with Control Owners
- Control Design Evaluation and Gap Remediation
  - Evaluate the Control Design
  - Define Gaps
  - Remediate Identified Gaps
- External Review
  - Coordinate with External Auditor

**Engage, Communicate and Train**
- Engage Broader Organization
- Communicate with Key Stakeholders
- Perform Training

**Overall Project Management**
Other Frameworks/Guidance
PCI-DSS 3.0

• Version 3.0 of PCI-DSS was released in November 2013

• Regulated by the PCI Security Standards Council and the major credit card brands

• Any entity that stores, processes, or transmits cardholder information MUST COMPLY with the PCI Data Security Standard (DSS)

• Entities include but are not limited to:
  – Acquirers
  – Merchants
  – Service providers
  – Trusted third parties

• Each card brand has their own compliance requirements based on this general requirement
PCI-DSS 3.0

| Build and Maintain a Secure Network and Systems | 1. Install and maintain a firewall configuration to protect cardholder data  
| 2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect Cardholder Data | 3. Protect stored cardholder data  
| 4. Encrypt transmission of cardholder data across open, public networks |
| Maintain a Vulnerability Management Program | 5. Protect all systems against malware and regularly update anti-virus software or programs  
| 6. Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures | 7. Restrict access to cardholder data by business need to know  
| 8. Identify and authenticate access to system components  
| 9. Restrict physical access to cardholder data |
| Regularly Monitor and Test Networks | 10. Track and monitor all access to network resources and cardholder data  
| 11. Regularly test security systems and processes |
| Maintain an Information Security Policy | 12. Maintain a policy that addresses information security for all personnel |

ITIL

- The Information Technology Infrastructure Library (ITIL), is a set of best-practices for IT service management (ITSM) that focuses on aligning IT services with the needs of the business.

- In its current form (known as ITILv3 and ITIL 2011 edition), ITIL is published in a series of five core publications, each of which covers an ITSM lifecycle stage.

- ITIL describes procedures, tasks and checklists that are not organization-specific, used by an organization for establishing a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.
ITIL

Service design

How service is utilized

How service is deployed

Possible service incidents

(Service transition)

Request for change

Guidelines, policies, and incentives to change utilization patterns

Usage guidelines, policies, and incentives to change utilization patterns

Service improvement

How service is utilized

How service is supported

How service is delivered

Requests for change

Objectives, policies, and guidelines

Requests for change

Service strategy

Compensating resources and requests for change

Design limitations
HIPAA

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Department of Health and Human Services (DHHS).

Privacy of health information
- Restricts the use and dissemination of identifiable health information
- Provides individuals with greater access and control of their medical information
- Regulates business partners and business partner agreements

Security of health information
- Ensures information integrity and confidentiality
- Protects against information tampering and unauthorized information uses and disclosures
HIPAA

Access Control, Audit Control
Integrity, Person or Entity Authentication
Transmission Security

Facility Access Controls, Workstation Use
Workstation Security, Device & Media Controls

Security Mgmt. Process, Sec. Officer, Workforce Security,
Proc., Contingency Plan, Evaluation, BACs

CIA

Technical Safeguards for EPHI

Physical Safeguards for EPHI

Administrative Safeguards for EPHI

Privacy Rule “reasonable” safeguards for all PHI
# HIPAA

<table>
<thead>
<tr>
<th>Domain</th>
<th>HIPAA Security Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Org</strong></td>
<td></td>
</tr>
<tr>
<td>Personnel</td>
<td>Sanction policy</td>
</tr>
<tr>
<td>Organization</td>
<td>Assigned security resp.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Risk management</td>
</tr>
<tr>
<td><strong>Apps</strong></td>
<td></td>
</tr>
<tr>
<td>Access</td>
<td>Information access management</td>
</tr>
<tr>
<td>Security</td>
<td>Automatic logoff</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td></td>
</tr>
<tr>
<td>Access</td>
<td>Access mgt: id, passwd, terminations</td>
</tr>
<tr>
<td>Security</td>
<td>Incident mgt</td>
</tr>
<tr>
<td><strong>Ops</strong></td>
<td></td>
</tr>
<tr>
<td>Physical</td>
<td>Facility access controls</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>DR plan</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HIPAA Security Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trng-Security reminders</td>
</tr>
<tr>
<td>Business associate contract</td>
</tr>
<tr>
<td>Evaluation</td>
</tr>
<tr>
<td>Password management</td>
</tr>
<tr>
<td>Audit controls &amp; activity review</td>
</tr>
<tr>
<td>Log-in monitoring</td>
</tr>
<tr>
<td>Mechanism to authenticate</td>
</tr>
<tr>
<td>Unique user ID</td>
</tr>
<tr>
<td>Trans. integrity controls</td>
</tr>
<tr>
<td>Encryption: email</td>
</tr>
<tr>
<td>Encryption: transactions</td>
</tr>
<tr>
<td>Castor controls</td>
</tr>
<tr>
<td>RM-vulnerabilities</td>
</tr>
<tr>
<td>Login monitoring</td>
</tr>
<tr>
<td>Media Accountability</td>
</tr>
<tr>
<td>Data backup and storage</td>
</tr>
<tr>
<td>Maintenance</td>
</tr>
<tr>
<td>Criticality of applications</td>
</tr>
</tbody>
</table>
Summary

The latest versions of COBIT and COSO are complimentary frameworks that can be mapped to one another.

Regulators, external auditors and audit committees will expect some form of governance framework to be in place and functioning.

Implementation requires sufficient planning and lead time.

Other frameworks and guidance exist that may be applicable to your organization.
Questions?

Stephen Head

stephen.head@experis.com

704-953-6688