Using COSO Principle 11 for IT Audits

Colin Shogren: IT Audit Manager

Bruce Flinn: Associate Principal IT Auditor
Agenda

- A little about ourselves
- IT auditing at the WI Legislative Audit Bureau (LAB)
- What is Principle 11
- Steps taken
- Gathering entity information
- Changes to methodology
- Defining key controls
- Next steps
About LAB
About Bruce

- University of Wisconsin – Eau Claire
- LAB beginnings
- CISA
- LAB current
About Colin

- Graduated from DePaul University
- CPA, CISA, PMP
- 25 years of private industry experience
  - Started career as an “EDP” auditor
  - Time in finance, IT, and internal audit
- Hired by LAB 2 years ago
  - IT Audit Manager
  - Bring some different ideas to the IT audit process
Observations

- Moving from internal audit to external audit
- Workpapers, workpapers, workpapers
- How much testing is enough?
- Control design
- Part of the control
Purpose of LAB Audits

- Financial statement
- Federal compliance
- Performance
Purpose of LAB IT Audits

- Support of financial, compliance, and performance audits
LAB IT Audit Strategy

Data Center Controls

Agency-Wide Controls

Application Controls
LAB IT Audit Strategy

- Determine audits being completed (financial/compliance)
- Identify critical financial/compliance systems
- Identify supporting controls systems for financial/compliance systems
- Conduct review at data center level and communicate to agency auditors
- Conduct review of remaining items at the agency and potentially application levels
IT Audit Strategy (continued)

Ensure coverage of 6 key audit areas

1. Physical security
2. Back-ups
3. Data control and operations
4. Change management
5. Patch management
6. Disaster recovery/continuity of operations
IT Audit Work

- Gain an understanding of the processes and controls in place
- Determine if control is properly designed and placed in operation, and
- Test for effectiveness/compliance
Limitations of IT Audit Work

1. Scope of audits
2. Materiality
3. Post-auditing
4. Resources
What is COSO Principle 11?

COSO Principle 11 states that the organization selects and develops general control activities over technology to support the achievement of objectives. Points of focus supporting Principle 11 state that the organization:

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

*Source: COSO Framework*
Principle 11 High-Level Steps

- Gain an understanding of the environment
  - The IT infrastructure and components
  - The end-computing areas such as laptops, hand-held devices, and spreadsheets
  - IT applications outsourced to the cloud and other off-site service providers
  - How the technology function is managed throughout the entity.

- Analysis of application controls and the assessment of information-processing risks they are addressing

- Analysis of the general controls over technology that protect the application controls

- Use a system with procedures to assign a value to the probability that the controls will (or will not) prevent or detect and correct the error
Understanding Controls Over Technology (Journal of Accountancy, May 2014)
COSO Principle 11 Flow

1. Gain an Understanding of the Entity

2. Identify and assess the risk of IT general controls not achieving objectives

3. Identify and assess the risk of IT application controls not achieving objectives

4. Using an assessment process, determine the effectiveness of Principle 11
Steps Taken

- Reviewed the CIS 20 as a possible starting point
- Reviewed the NIST cybersecurity framework
- Developed an initial matrix
- Gathered entity information for the first year
- Streamlined the information gathering process
- Made changes to IT audit methodology
- Identified key application and general controls
Gathering Entity Information

- Surveys/data requests
- Agency self assessments
- Inquiries with management
- Agency audits
Changes to Methodology

- Focus of testing
- Evaluation of IT control objectives
- IT risk-based audits
- Resources
Defining Key Controls

- General controls
  - Access to programs and data
  - Program change and development
  - Computer operations

- Application controls
  - Access to programs and data
  - Program changes and development
  - Operations and scheduling
  - Interfaces and data movement
  - Application specific controls
Next Steps

- Agency Audits
  - Updating key controls
  - Consistent binder organization
- Determine how to risk score controls
- Risk-based audits
- Reporting for risk-based audits
- Methodology reassessment
Benefits of Risk-Based Audits

1. No financial/compliance scope limitations
2. Different materiality considerations
3. No post-audit considerations
Key Takeaways

Utilizing Principle 11 as a framework can help to guide or “right size” your IT audit work that supports your financial audits

The COSO principles may be something to pay more attention to in the future (appeared as part of the compliance supplement this year, part VI)
Questions?

- Colin Shogren: 
  Colin.Shogren@legis.Wisconsin.gov

- Bruce Flinn: 
  Bruce.Flinn@legis.Wisconsin.gov