


Information Technology Auditing IT Controls

James D. Boyd, MBA, CPA, CIA, CISA, CIG
Inspector General
Florida Dept. of Health

Class Overview


- ▶ Understanding IT Controls
 - ▶ Importance of IT Controls
 - ▶ Effective IT Controls
 - ▶ IT Roles and Responsibilities
 - ▶ Analyzing Risk
- 

Control Classifications

▶ General

- Information security policies
- Administration
- Access/Authentication
- Separation of key IT functions
- Management of systems acquisition and implementation
- Change management
- Backup/Recovery
- Business continuity

▶ Application

- Data edits
 - Balancing of processing totals
 - Transaction logging
 - Error reporting
- 

Governance, Management, Technical Controls

▶ Governance Controls


- ▶ Effective information management, security principles, policies, and processes.
- ▶ Performance and compliance.
- ▶ Mandated and controlled by board, in conjunction with management.
- ▶ Linked with organizational goals and strategies and outside bodies e.g. regulators.

▶ Management Controls


- ▶ Management responsible for internal controls;
 - All areas of the organization
 - Collaboration among board members and management is essential.
- ▶ Management must ensure IT controls are deployed to recognize risks to organization, processes and assets.
- ▶ Mechanisms and processes to mitigate and manage risks (protect, monitor, and measure results).

Governance, Management, Technical Controls

▶ Technical Controls

- Ensure the reliability of virtually every other control.
 - Protect against unauthorized access and intrusion.
 - Basis for reliance on the integrity of information.
 - Should include evidence of all changes and their authenticity.
 - Specific to technologies in use.
 - Implement and demonstrate compliance with policies
- 

General Controls

- ▶ Policies Should Include
 - General Policy Statement
 - Classification Statement
 - Definitions of Concepts
 - Personnel Policies
 - Business Continuity Requirements
- 

General Controls (cont.)

- ▶ Standards
 - Systems Development Process
 - Systems Software Configuration
 - Application Controls
 - Data Structures
 - Documentation
- 

General Controls (cont.)

- ▶ Organization and Management
 - Separation of Duties
 - Financial Controls
 - Change Management
 - Other Management Controls

General Controls (cont.)

- ▶ Physical and Environmental Controls
 - Physical Locks, Limiting Access to Servers
 - Restricting Physical Access to Specific Individuals
 - Fire Detection and Suppression Equipment
 - Storing Equipment Away from Environmental Hazards

General Controls (cont.)

▶ Systems Software Controls

- Access rights allocated and controlled according to the organization's stated policy.
- Division of duties enforced through systems software and other configuration controls.
- Intrusion and vulnerability assessment, prevention, and detection in place and continuously monitored.
- Intrusion testing performed on a regular basis.
- Encryption services applied where confidentiality is a stated requirement.
- Change management processes — including patch management — in place to ensure a tightly controlled process for applying all changes and patches to software, systems, network components, and data.

General Controls (cont.)

▶ Systems Development and Acquisition Controls

- User requirements should be documented, and their achievement measured.
- Systems design should follow a formal process to ensure user requirements and controls are designed into the system.
- Systems development should be conducted in a structured manner to ensure requirements and design features are incorporated into the finished product.
- Testing should ensure that individual system elements work as required, system interfaces operate as expected, users are involved in the testing process, and the intended functionality has been provided.
- Application maintenance processes should ensure that changes in application systems follow a consistent pattern of control and are subject to validation.
- Where systems development is outsourced, the outsourcer or provider contracts should require similar controls.

Application Controls

- ▶ Application Based Controls
 - Data is accurate, complete, authorized and correct
 - Data is processed as intended
 - Output is accurate and complete
 - Record tracking data from input to processing to output

Application Controls (cont.)

▶ Input Controls

- Checks integrity of data entered into a business application.
- Input is checked to ensure that it remains within specified parameters.

▶ Processing Controls

- Provide automated means to ensure processing is complete, accurate, and authorized.

▶ Output Controls

- Address what is done with the data. Should compare actual result with intended result and check them against the input.


Application Controls (cont.)

- ▶ Integrity Controls
 - Can monitor data in process and/or in storage to ensure data remains consistent and correct.
- ▶ Management Audit Trail
 - Enable tracking of transactions from the source to the ultimate result and to trace backward to identify transactions and events. These controls should monitor the effectiveness of overall controls and identify the source of errors.


Information Security

- ▶ Elements of Information Security
 - Confidentiality
 - Integrity
 - Availability


IT Controls Framework

- ▶ Key Components
 - Regulatory and Statutory Compliance
 - Consistency with organization goals and objectives
 - Assurance activities comply with policies and an organizations risk appetite
- 

Key Indicators of Effective IT Controls

- ▶ Ability to execute new upgrades, products and services
 - ▶ Projects delivered on time, and within budget
 - ▶ Predictable resource allocation
 - ▶ Consistency in availability and reliability of information and services
- 

Key Indicators of Effective IT Controls (cont.)

- Clear communication to management of effective controls
 - Ability to protect against new threats and recover from any disruptions
 - Efficient use of customer support center or help desk
 - Security consciousness throughout organization
- 

IT Roles in the Organization

- ▶ Overall Objectives of IT:
 - Delivery of reliable information securely and efficiently
 - Protect stakeholders interests
 - Enable mutually beneficial relationships that accomplish business objectives
 - Identify and respond to threats and potential violations appropriately

IT Roles in the Organization


(cont.)

- ▶ Board of Directors / Governing Body
 - Awareness of key IT topics
 - Understanding of IT infrastructure and components
 - Approval of data classifications and related access rights

IT Roles in the Organization

(cont.)

▶ Audit Committee

- Understanding of financial management and organizations reliance on IT for financial processing and reporting
 - Ensuring IT is covered in committee meetings
 - Overseeing assessment of IT controls
 - Reviewing business and control issues related to new system development and acquisition
- 

IT Roles in the Organization

(cont.)

▶ Audit Committee (cont.)

- Examining internal and external audit plans and ensuring IT is adequately covered.
- Reviewing audit results and monitoring resolution of issues.

IT Roles in the Organization

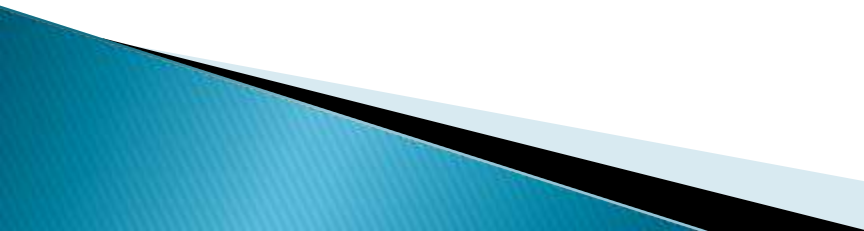
(cont.)

- ▶ **Governance Committee**
 - Ensure potential and current board members have suitable IT knowledge
 - Assess board committee performance in IT oversight
 - Review external regulatory governance assessments as related to IT
 - Ensure board review IT policies periodically

IT Roles in the Organization

(cont.)

▶ Chief Executive Officer

- Define IT related objectives and performance measures.
 - Custodian over organizations IT related critical success factors
 - Understand and approve short and long-range IT strategy.
 - Approve IT resources, including structure and oversight/monitoring.
 - Identify IT issues for periodic management, board, and staff discussion.
 - Ultimate level of responsibility.
- 

IT Roles in the Organization

(cont.)

▶ Chief Information Officer

- Understand business requirements that drive the need to implement IT.
- Develop IT partnerships with business management to:
 - Ensure IT strategy is aligned with the business strategy.
 - Ensure compliance.
 - Benefit from improvements to process-efficiency.
 - Mitigate assessed risks
- Design, implement, and maintain an IT internal control framework.
- Plan, hire/contract, and control IT resources.
- Explore, assess, select, and implement technology advances (e.g. wireless communications).

IT Roles in the Organization

(cont.)

- ▶ **Chief Information Officer** (cont.)
 - Provide training for IT personnel to ensure that levels of knowledge and skills remain current.
 - Operate as the highest-level data/system custodian and IT control owner.
 - Measure the operational performance of IT in support of business objectives by:
 - Setting expectations.
 - Evaluating results.
 - Develop means to verify that IT is providing services and support as expected.

IT Roles in the Organization

(cont.)

▶ Chief Information Security Officer


- Develops and implements the information security policy.
- Controls and coordinates information security resources, ensuring they are allocated adequately to meet the organization's security objectives.
- Ensures alignment of information security and business objectives.
- Manages operational information risks throughout the organization.
- Oversees IT security within the organization.
- Provides education and awareness on information security issues and new best practices.

IT Roles in the Organization

(cont.)

- ▶ Chief Information Security Officer (cont.)
 - Develops end-user policies for the usage of IT information, in conjunction with the human resources function.
 - Coordinates information security work with the CIO.
 - Advises the CEO, CIO, and Board on IT risk issues.
 - Acts as a key link for the CAE when internal auditing performs IT control-related audits

Risk Considerations in Determining Adequacy of IT Controls

- ▶ Risk Appetite and Tolerance
 - ▶ Performing Risk Analysis
 - ▶ Value of Information
 - ▶ Appropriate IT Controls
 - ▶ Risk Mitigation Strategies
 - Accept the risk
 - Eliminate the risk
 - Share the risk
 - Control/mitigate the risk
- 

Analyzing Risk

- ▶ Control Characteristics to Consider
 - Is the control effective?
 - Does it achieve the desired result?
 - Is the mix of preventive, detective, and corrective controls effective?
 - Do controls provide evidence when parameters are exceeded or controls fail?
 - How is management alerted to failures, and which steps are expected to be taken?
 - Is evidence retained (audit or management trail)?

Analyzing Risk

- ▶ **Control Characteristics to Consider** (cont.)
 - Do IT policies — including for IT controls — exist?
 - Have responsibilities for IT and IT controls been defined, assigned, and accepted?
 - Are IT infrastructure equipment and tools logically and physically secured?
 - Are access and authentication control mechanisms used?
 - Is antivirus software used and updated?
 - Are security patches up-to-date?

Analyzing Risk

- ▶ **Control Characteristics to Consider** (cont.)
 - Is firewall technology implemented in accordance with policy?
 - Are external and internal vulnerability assessments completed and risks identified and appropriately resolved?
 - Are change and configuration management and quality assurance processes in place?
 - Are structured monitoring and service measurement processes in place?
 - Are specialist IT audit skills available (either internally or outsourced)?

Analyzing Risk

- ▶ **Control Characteristics to Consider** (cont.)
 - Is stored data adequately protected?
 - Is sensitive data, sent across public networks, encrypted?
 - Are security systems, and processes, regularly tested?
 - Have the default security settings and passwords been changed?

IT Roles in the Organization

▶ Audit

Internal Auditing – CAE and Audit Staff

- Advising the audit committee and senior management on IT internal control issues.
- Ensuring IT is included in the audit universe and annual plan (selecting topics).
- Ensuring IT risks are considered when assigning resources and priorities to audit activities.
- Ensuring that audit planning considers IT issues for each audit.
- Performing IT risk assessments.
- Performing IT enterprise-level controls audits.
- Performing IT general controls audits.
- Performing IT applications controls audits.
- During systems development or analysis activities, operating as experts who understand how controls can be implemented and circumvented.

IT Roles in the Organization

(cont.)

▶ Audit (cont.)

◦ External Auditor

- The extent of the external auditor's responsibilities for understanding and evaluating the IT system and related IT controls during financial audits.
- The scope of the external auditor's responsibilities for examining the IT system and controls during any formal attestation that may be required by statute or regulation, such as internal controls over financial reporting and other regulatory requirements.

Questions?

James D. Boyd, MBA, CPA, CIA, CISA, CIG
Inspector General
Florida Dept. of Health
4052 Bald Cypress Way
Bin #A03
Tallahassee, FL 32399-1704
(850)245-4141

