Florida Inspectors General

Melinda M. Miguel
Chief Inspector General

IT Auditing

Sponsored by:

The Chief Inspector General and the Florida Chapter of the Association of Inspectors General

Enhancing Public Trust in Government

Melinda M. Miguel
Chief Inspector General

Discussion Topics

- IT Auditing Defined
- Audit Standards
- Role of the IT Auditor
- IT Controls
- References
- ISACA

IT Auditing Defined

"The evaluation of Information Systems, practices, and operations to assure the integrity of an entity's information."

Source: Information Technology Control and Audit, Auerbach Publications

Audit Standards

- Government Accountability Office (GAO)
- Institute of Internal Auditors (IIA)
- ISACA

Standards – GAO

The staff assigned to a GAGAS audit or attestation engagement should collectively possess:

d. skills appropriate for the work being performed. For example, skills in:

(2) information technology if the work involves review of information systems; (3.72)

Standards – GAO

When information systems controls are determined to be significant to the audit objectives or when the effectiveness of significant controls is dependent on the effectiveness of information systems controls, auditors *should* then evaluate the design and operating effectiveness of such controls. (6.24)

Standards – IIA

1210.A3 – Internal auditors *must have sufficient knowledge of key information technology* risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

Standards – IIA

2110.A2 – The internal audit activity *must* assess whether the information technology governance of the organization supports the organization's strategies and objectives

Standards – IIA

2130.A1 – The internal audit activity *must* evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and *information systems*….

Standards – ISACA

The IT Auditor is required to review and assess:

- Whether the IS function aligns with the mission, vision, values, objectives and strategies of the organization.
- Whether the IS function has a clear statement about the performance expected by the business and assess its achievement.
- The effectiveness of IS resource and performance management processes.

Standards – ISACA

The IT Auditor is required to review and assess:

- Compliance with legal, environmental and information quality, and fiduciary and security requirements.
- Control environment of the organization
- Risks that may adversely effect IT

Standards – ISACA

The IT Auditor is required to:

- Evaluate and monitor IT controls that are an integral part of the internal control environment of the organization.
- Assist management by providing advice regarding the design, implementation, operation and improvement of IT controls.

Role of the IT Auditor

- To assess the **efficiency** and **effectiveness** of IT
- To assess the **availability**, **integrity,** and **confidentiality** of IT Resources
- To assess the **protection\security** of IT Resources
- To report IT internal control issues

The Need For IT Controls

855 Incidents,174 million compromised records in 2011

- 98% of breaches stemmed from external agents
- 58% of all data theft was tied to activist groups
- 81% utilized some form of hacking
- 69% incorporated malware
- 97% of breaches were avoidable through simple or intermediate controls
- 96% of attacks were not highly difficult
- 96% of victims subject to PCI DSS had not achieve compliance
- 85% of breaches took weeks or more to discover
- 79% of victims were targets of opportunity

Source: Verizon's 2012 Data Breach Investigations Report

IT Resources

- Computer Hardware
- Operating Systems
- Application Systems
- Information Technology Operations
- Database Systems
- Networks

IT Controls

"The policies, procedures, practices and organizational structures, designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected."

Source: COBIT

IT Controls

General vs. Application Controls

- Both are needed/required to ensure the Reliability, Integrity and Availability of data
- They should consist of Preventive, Detective and Corrective control types
- Can be Manual, Physical or Logical

Melinda M. Miguel
Chief Inspector General

General IT Controls

General IT controls are pervasive throughout the IT environment and support numerous activities, but do not link directly to any specific business process or transaction.

General IT Controls

General IT control categories include:

- Security Management
- Access Controls
- Configuration Management
- Segregation of Duties
- Business Continuity/Disaster Recovery

Security Management

- Security Management Program
- Periodic Risk Assessments and Validation
- Security Control Policies and Procedures
- Security Awareness Training
- Periodic Testing and Evaluation
- Remediation of Security Weaknesses
- Security Over External Third Parties' Activities

Access Controls

- Protection of Information System Boundaries
- Identification & Authentication Mechanisms
- Authorization Controls
- Protection of Sensitive System Resources
- Audit & Monitoring Capability Including Incident Handling
- Physical Security Controls

Configuration Management

- CM Policies, Plans, & Procedures
- Current Configuration Identification Info
- Proper Authorization, Testing, Approval, and Tracking of all Configuration Changes
- Routine Monitoring of the Configuration
- Updating Software on a Timely Basis
- Documentation & Approval of Emergency Changes to the Configuration

Melinda M. Miguel
Chief Inspector General

Segregation of Duties

- Segregation of Incompatible Duties & Responsibilities and Related Policies
- Control of Personnel Activities Through Formal Operating Procedures, Supervision, and Review

Melinda M. Miguel
Chief Inspector General

Business Continuity / DR

- Assessment of the Criticality and Sensitivity of Computerized Operations & Identification of Supporting Resources
- Steps Taken to Prevent and Minimize Potential Damage and Interruption
- Comprehensive Contingency Plan
- Periodic Testing and Updating of the Contingency Plan

Application Controls

"Ensure the *completeness* and *accuracy* of the records and the *validity* of the entries made in the transactions and standing data resulting from both manual and automated processing."

Source: IT Governance Institute, www.itgi.org

Application Controls

"The manual or automated techniques used to *control input, processing*, and *output* of information in an application."

Source: Information Technology Control and Audit, Auerbach Publications

Application Controls

- Input Controls
  - Prevents invalid, missing, or erroneous data
  - Ensure errors are captured and effectively resolved
- Processing Controls
  - Ensures only authorized and accurate data is stored
- Output Controls
  - Ensures appropriate access and accuracy of data

Input Controls

- Input Authorization
  - Authorized source documents and input files are complete and accurate (e.g. batch totals, sequence checking, etc.)
  - Access Controls (e.g. Segregation of Duties)
  - Input data is approved
- Edit Checks (e.g. invalid field lengths or characters, missing data, incorrect data, or erroneous dates)
- Error Processing (e.g. error or warning messages, error reports, etc.)

Processing Controls

- Processing Errors are identified, logged, and resolved.
- Transactions are executed in accordance with the predetermined parameters and tolerances.
- Transactions are valid and unique (not duplicative).

Output Controls

- Reconciliation
- Distribution of Output is Clearly Defined
- Limited Physical and Logical Access Defined to Authorized Personnel
- Retention

IT Outsourcing

- Includes people, processes, hardware, software, and data.
- Service Level Agreements/Contracts
- Service Organization Control (SOC) Reports
- Service Provider's Internal Audit Group
- Performance of Independent Testing of the Outside Control Activities

Emerging Technology

- Increased Virtualization
- Cloud Computing
- Social Media
- Mobile Devices

References

- Federal Information System Controls Audit Manual (FISCAM)
- Issued by the Government Accountability Office (GAO)
- Primarily designed for evaluations of general and application controls over financial information systems that support agency business operations
- Used by auditors in reviewing internal controls as part of the annual financial statement audits required at all major federal agencies

Source: http://www.gao.gov/special.pubs/fiscam.html

References

- Global Technology Audit Guide (GTAG)
- Issued by the Institute of Internal Auditors (IIA)
- GTAG 2: Change and Patch Management Controls: Critical for Organizational Success, 2nd Edition
- GTAG8: Applications Control
- GTAG 9: Identity and Access Management
- GTAG 10: Business Continuity Management

Source: https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Practice-Guides.aspx

References

- NIST Special Publications
- COBIT 5
- ITIL

ISACA

- Started in 1967
- 100,000 constituents in 180 countries
- Certified Information Systems Auditor® (CISA®),
- Certified Information Security Manager® (CISM®),
- Certified in the Governance of Enterprise IT® (CGEIT®); and
- Certified in Risk and Information Systems Control™ (CRISC™) designations

ISACA Tallahassee

ISACA Tallahassee Chapter
PO Box 13473
Tallahassee, FL 32317
E-mail: isacatallahassee@gmail.com
Web site:
http://www.isaca.org/chapters4/Tallahassee

Questions?

Mike Blackburn
850-412-3977
Mike.Blackburn@ahca.myflorida.com

Sarah Beth Hall
850-410-5826
Sarah.Hall@dot.state.fl.us