IT Auditing for the Non-IT Auditor:
How to Prepare for an IT Audit
What to Expected During the Audit
How to Respond to Findings

Greg Matayoshi
IntelliBridge Partners LLC
Greg Matayoshi

Director in IntelliBridge Partners, Consulting Division of Macias Gini & O’Connell, LLP

- Certified Information Systems Auditor.
- IT General Control and Application Audits
- IT Performance Audits
- IT Strategic Planning

www.intellibridgepartners.com
Today’s Objectives

• Provide a basic understanding of IT Audits
  • How to prepare
  • What to expect
  • How to respond

• Describe Top 10 IT Controls Audit Findings
Provide a Basic Understanding of IT Audits
Information Technology Controls

IT controls purpose:

- Minimize the risk of fraud, waste, and abuse
- Provide assurance on the accuracy and integrity of financial data
- Enable an organization to focus on creating value for customers and stakeholders
Information Technology Controls

Auditor’s Premises:
1. Management is responsible for establishing and maintaining effective internal control over financial reporting.
2. Management is responsible for designing and implementing programs and controls to prevent and detect fraud.

As auditors, we look for reasonable assurance that these controls and programs are in place.
Information System Reviews

Information system reviews provide an understanding of information systems, control issues, and areas of risk.

These reviews are an important part of financial audits, and follow similar principles.

The standards for information system reviews, however, are IT-focused rather than financial-focused.
Information System Reviews

- Identifies control issues and areas of risk for the audit team to consider.
- Standards based upon ISACA and COBIT.
- Can encompass general controls as well as application controls.
- Required understanding as part of SAS 104-111.
Information Technology Controls

Information technology controls consist of both general (organization-level) and application-specific controls.
General and Application Controls

General Control Areas:
- Governance
- Systems development
- Change management
- Security
- Computer operations

Application Control Areas:
- Completeness
- Accuracy
- Validity
- Authorization
- Segregation of duties
General and Application Controls

Plan and Organise

Acquire and Implement

Deliver and Support

Monitor and Evaluate

Business's Responsibility

IT's Responsibility

Business's Responsibility

Functional Requirements

Control Requirements

Application Controls

Automated Services

COBIT
How to Prepare
How to Prepare for the IT Audit

• Ensure IT policies and procedures are available and up-to-date.
  - IT Administrative Policies and Procedures -- Communications to Functional Users
    - Password Standards
    - Appropriate Use
    - Expectation of Privacy
    - Ownership of Data
    - Physical Security of Assets
    - Software Licensing and Piracy

www.intellibridgepartners.com
How to Prepare for the IT Audit (cont.)

- Policies and procedures for acquisition of software and systems.
  - Should require or ensure:
    - Definition of business and technical requirements
    - Analysis and comparison of multiple products
    - Cost-benefit analysis
    - Security and control implications
    - Technical support needs
    - Testing procedures
    - Implementation procedures
    - Conversion and training procedures.
How to Prepare for the IT Audit (cont.)

- Policies and procedures for program change management.
  - Testing and sign-off process
  - Security and control requirements
  - Migration procedures.
How to Prepare for the IT Audit (cont.)

- Batch Processing Procedures
- Technical Support Policies
- IT Position Job Descriptions
- Backup Procedures
- Account Provisioning – Network and Applications
- IT Organizational Chart
  - Where does IT fit in the organization? Does it report to a functional user department?
  - Do any persons with administrative IT authority report outside of the IT department?
- IT Topology Diagram
  - Primary servers, data linkages, internet connectivity
How to Prepare for the IT Audit (cont.)

- Inventory of Hardware and Operating Software
  - Type of Computers: Mini, Server, Desktop/Client
  - Make
  - Model
  - Quantity
  - Purpose
  - Operating Software
  - Vendor
  - Current Version of Operating System Installed
How to Prepare for the IT Audit (cont.)

- Inventory of Accounting and Information Systems
  - Application Name
    - Purchased/Modified/Developed?
    - Vendor
    - Current Version
    - Operating System
    - Use of Software
    - Related Transaction Cycles

- Antivirus
- Firewalls
- Backup Systems
- Help Desk Systems
How to Prepare for the IT Audit (cont.)

- Review current practices to ensure they comply with formal policies and procedures.

- Other Areas:
  - Disaster Recovery and Business Continuity
  - Risk Assessments
  - PCI Compliance
  - Network Penetration Testing
What to Expect
What to Expect

Depending on the type of audit, the auditor will first request documentation and then follow up with on-site interviews and testing.

The auditor should define the scope of the audit being conducted and the timeframe.

The following are the control areas most likely to be covered during a general controls review:
What to Expect (cont.)

IT Governance Controls

- Controls should ensure that senior management takes responsibility for IT and are kept informed of any significant issues.

- IT Steering Committee
- IT Strategic Plan
What to Expect (cont.)

System Acquisition, Development and Change Management

• Controls should ensure that an appropriate methodology to implement new systems and to support program and system changes are followed.
  □ Testing to determine impact of new programs and systems on security, data integrity, availability, and performance.
  □ Program testing in separate environment.
  □ Programmers do NOT have access to production system.
  □ Emergency changes are controlled and viable roll back procedures are available.
What to Expect (cont.)

Computer Operations
• Controls should ensure that systems and data are backed up on a timely basis and stored separately.
  ❑ When is system and application data backed up?
  ❑ How often are backup tapes/disks rotated off site?
  ❑ Where are backup tapes/disks stored?
  ❑ Is storage secure and environmentally controlled?
  ❑ Are backup tapes/disks periodically tested to ensure data can be recovered?
Computer Operations

• Controls should ensure that systems and data can be recovered in a timely manner in the event of a disaster.
  ❑ Has a disaster recovery and business continuity plan been developed?
  ❑ When was it last tested?

• Adequate technical support should be available to resolve user and processing problems in a timely manner.
  ❑ Have service level agreements been established?
  ❑ Have performance metrics been established?
Computer Operations

- IT assets should be protected from physical and environmental hazards.
  - All server rooms should provide adequate security and protection for IT assets
    - Locked entry, limited access
    - Dry fire suppression system
    - Independent A.C. system
    - Battery backup, generators
    - Raised floors and general cleanliness
    - Auto notification of temperature extremes
What to Expect (cont.)

Access to Programs and Data

• Has an IT Risk Assessment been performed?
  ❑ Identification of risks
  ❑ Measures of Likelihood and Impact
  ❑ Assessment of mitigating controls
  ❑ Identification of data and sensitivity of data.
What to Expect (cont.)

• Authentication and Authorization Controls – Procedures review and testing.
  ❑ Access controls to all three layers will be assessed and tested
    o Database
    o Application
    o Client
  ❑ Account provisioning and authorization
  ❑ Password configuration standards (MS AD GPO)
    o Length: 7-14 characters
    o Expiration: not more than 90 days.
    o Strong passwords enforced
    o Password history enforced
    o Auto account lockout: 3-5 attempts
### Default Domain Policy

#### Default Domain Policy
- Data collected on 3/4/2013 5:50:29 PM
- Computer Configuration (Remote)

#### Policies
- **Windows Settings**
- **Security Settings**
  - **Account Policies/Password Policy**
    - **Policy**: Enforce password history
      - **Setting**: 3 passwords remembered
    - **Policy**: Minimum password age
      - **Setting**: 150 days
    - **Policy**: Minimum password length
      - **Setting**: 0 days
    - **Policy**: Minimum password expiration
      - **Setting**: 6 characters
    - **Policy**: Password must meet complexity requirements
      - **Setting**: Enabled
    - **Policy**: Change password using reversible encryption
      - **Setting**: Disabled
  - **Account Policies/Account Locked Policy**
    - **Policy**: Account lockout duration
      - **Setting**: 59 minutes
    - **Policy**: Account lockout threshold
      - **Setting**: 12 invalid logon attempts
    - **Policy**: Account lockout session time
      - **Setting**: 59 minutes
  - **Account Policies/Prevent Policy**
    - **Policy**: Enforce user login restrictions
      - **Setting**: Disabled
    - **Policy**: Minimum lifetime for service ticket
      - **Setting**: 30 minutes
    - **Policy**: Maximum lifetime for user ticket
      - **Setting**: 180 minutes
    - **Policy**: Maximum lifetime for client ticket, removed
      - **Setting**: 2 days
    - **Policy**: Maximum lifetime for computers, clock synchronization
      - **Setting**: 5 minutes
  - **Local Policies/Audit Policy**
    - **Policy**: Audit account logon events
      - **Setting**: Success, Failure
    - **Policy**: Audit account management
      - **Setting**: Success, Failure
    - **Policy**: Audit process service access
      - **Setting**: Success, Failure
    - **Policy**: Audit log file
      - **Setting**: Success, Failure
    - **Policy**: Audit policy change
      - **Setting**: Success, Failure
    - **Policy**: Audit privilege use
      - **Setting**: Success, Failure
  - **Local Policies/User Rights Assignment**
    - **Policy**: Add user to domain group
      - **Setting**: WOODLANDS\Admin, WOODLANDS\Domain Admins
  - **Local Policies/Security Options**
    - **Policy**: Account Policies
      - **Setting**: Remove guest account
        - **Setting**: "Guest\Cow"
    - **Policy**: Interactive Logon
      - **Setting**: Prompt user to change password before expiration
        - **Setting**: 19 days
  - **Network Security**
What to Expect (cont.)

• Authentication and Authorization Controls – Procedures review and testing.
  ❑ Database Administrator Access: Schema Owner access – monitoring
  ❑ Application Authorization Roles and Profiles:
    o Periodic reviews and testing
    o Account provisioning sign-offs
  ❑ Remote Access Authorization
  ❑ Network Security Device (IDS, IPS) Access:
    o Authorizations
    o Monitoring
    o Log Review
How to Respond

• Clearly understand the criteria and condition.
• Auditor should present the materiality or impact of the finding.
• Obtain consensus on condition.
• To address the finding, clearly state the following:
  ❑ Agreement (or disagreement) with the finding.
  ❑ Responsible party for addressing the finding.
  ❑ Clearly defined actions that will be taken to address the finding.
  ❑ Timeline the finding will be addressed.
Top 10 IT Control Findings
IT Control Audit Issues

Over the last four years, MGO has performed IT control reviews for 50 governmental organizations.

- Cities
- Counties
- Transit Agencies
- State Agencies
- Medical Centers
- Retirement Systems
- Colleges and Universities
- Housing and Redevelopment Agencies.

Our finding areas were consistent across these organizations.
#10: Absence of an IT Risk Assessment

Control Objective: Mechanisms have been established to identify and react to risks, both internal and external.

An appropriate IT Risk Assessment program should:
- Be part of ongoing risk management program
- Independently conducted
- Identify IT risks and their likelihood, impact and mitigating controls
- Determine data security classes
- Determine assignment of data and application owners
#9: Insufficient Network and Database Monitoring

Control Objective: Network security controls have been implemented to safeguard company IT resources and data. Network security devices are appropriately managed.

Program controls should consider:

- Firewall management
  - Who has access?
  - How are changes to configuration managed?
  - Review of logs
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Database monitoring
#8: Insufficient Server Room Controls

Control Objective: IT assets are adequately protected.

Controls should ensure that:

- Access is limited to authorized personnel
- Environmental and monitoring systems include:
  - Uninterruptable power supplies (UPS) and backup generator
  - Independent air conditioning
  - Fire suppression
  - Monitoring
#7: Lack of a Defined SDLC

**Control Objective:** An appropriate development/acquisition methodology has been implemented for new systems.

An SDLC methodology should consider:
- Development/acquisitions of new systems
- Changes to existing systems
- Major and small projects, including:
  - Emergency changes
  - Operating software changes
  - Configuration changes

![SDLC Model Diagram](image-url)
#6: Need for Formal Change Control Management

Control Objective: An appropriate program change methodology has been implemented.

Procedures should account for:
- Impact of changes
- Program testing
- Managed program updates
- Logging emergency fixes
- Authorization of program changes
- Migration into production
- Version control
- Documentation of program changes
#5: Lack of IT Administrative Policies, Procedures and Password Configuration Standards

Control Objective: IT Responsibilities have been appropriately defined and communicated to users.

Policies and procedures are key to effective internal controls. An effective set of IT-related policies and procedures should address:

- Physical security of IT assets
- Ownership of information, data, software
- Agency access to computer information and hardware
- Installation and use of software
- Personal use of computer hardware and software
- Email usage
- Internet usage
- Telecommuting
- Password configuration.
#4: Outdated or Missing IT Strategic Plan

**Control Objective:** IT strategic plans are developed that are closely aligned with the business objectives.

Proper IT strategic plans incorporate the following:

- IT Steering Committee function
- Definition of IT Goals and Objectives – long term and short term
- Process for review, updates, and progress status reporting
- Aligned to the goals and objectives of the agency as a whole.
#3: Missing Controls for New User Setup and Account Termination

**Control Objective:** User account access privileges are authorized.

Formal processes for both user account setup and terminations should include:

- **Account setup**
  - Defined process
  - Should start with Human Resources
  - Audit trail
  - Authorization from data or application owner before access given

- **Account termination**
  - Defined process
  - Should start with Human Resources
  - Audit trail
  - Addresses both planned and unplanned departures.
#2: Insufficient Disaster Recovery Plan

Control Objective: Contingencies for unforeseeable events have been developed and implemented.

A disaster recovery plan should include the following, at a minimum:

- Disaster definition and declaration
- Personnel and contact information
- Vendor contacts
- Identification of systems and information to be addressed
- Step-by-step procedures with assigned responsibilities
- Date last reviewed, date last tested.
#1: Undefined Authorization Roles and Administrator Access

**Control Objective:** Authentication and authorization controls exist for access to the operating and significant application systems.

User privileges within the Network, Application and Database layers should be reviewed and validated.

- Electronic enforcement of segregation of duties
- Documentation of roles and profiles
- Periodic review of the active accounts
- Periodic testing of the roles

**Network Administrator Access:**
- Enterprise, Domain, and Schema Administrator Groups
- Assignment to groups

**Database access:**
- Database monitoring tools
- Schema Owner access monitoring
Questions & Contact Info

Greg Matayoshi
gmatayoshi@intellibridgepartners.com
916.642.7060