



OHIO

DIGITAL GOVERNMENT SUMMIT

A GOVERNMENT TECHNOLOGY EXECUTIVE LEADERSHIP FORUM

Surviving an IT Audit: Five Lessons Learned

Merritt Maxim
CA Inc.

IT Audit Background

- An IT audit should focus on determining risks that are relevant to information assets, and assess controls in order to reduce or mitigate these risks
- IT Audit generally covers:
 - Hardware, operating systems, network, security
- In addition, there are specialized audits for applications:
 - Application audits review controls in 3rd party, custom and home-grown software

IT Audits are Crucial

Survey of SOX filers who reported “material weaknesses,”
IT controls was the lead culprit

- IT controls (27%)
 - Revenue (18%)
 - Taxes (11%)
 - Financial reporting and close (10%)
-
- Of respondents who reported a material weaknesses, what was source of material weakness?

Lesson #1: Implement a Fixed Audit Schedule and Stick to it

- McAfee IT Audit Survey (spring 2008)
 - Approx. 25% of respondents ran audits on an ad-hoc basis
- Why?
 - Relying on informal ad-hoc IT audits almost guarantees that audits will always receive lower priority against other projects
 - Fixed schedule instill discipline in organization
 - Alignment of IT audits with financial audits can identify and remediate items of mutual interest
 - Fixed audit schedule enables better project and budget planning
 - No missed audits because of budget overruns

Lesson #2: Automate Wherever Possible

- Data collection
 - McAfee IT Audit Survey-spring 2008
 - 50%+ of respondents still using spreadsheets for collection
- Control Testing
- Why?
 - Increase operational inefficiency
 - Reduce time and effort for testing
 - High effort and unplanned work around audits indicated a poorly-controlled environment
 - Increase accuracy
 - Builds repeatable and more sustainable processes
 - Reduces the impact of future IT audits
 - Automation is one area where technology can yield big benefits

Lesson #3: Utilize Existing Frameworks

- Aim to map IT controls against multiple regulations to a foundational standard
 - ISO 27001 is a good example
- Seek single and comprehensive policies that can apply across regulations
- Why?
 - Consolidates the number of required separate audits
 - Test controls once, but have test apply against multiple regulations
 - Generates substantial compliance savings

Lesson #4: Adopt Risk-Based Approach

- Utilize risk assessments to:
 - To identify the level of uncontrolled risk
 - To appraise an organization's internal controls
- Leveraging risk and control objectives
 - Group similar controls together
- Why?
 - Prioritize which areas should be reviewed 1st
 - Even if single control fails, you can prove that:
 - "I'm still adequately managing this risk" or
 - "I'm achieving the overall objective of this control."

Lesson #5: Track Regulatory Environment

- External environment is dynamic
- Regulations are updated/modified
- Tracking changes (*and the impact on your organization*) takes time & \$\$
- Why?
- Want agility to adjust to changes
- Do not want to get caught off guard

Thank You

Merritt.maxim@ca.com

508-628-8597



Mary Taylor, CPA Ohio Auditor of State



Ohio Auditor of State
Mary Taylor, CPA

How to Survive an IT Audit

Presented by: Jim Swonger,
Senior Audit Manager

www.auditor.state.oh.us

OBJECTIVES:

- Identify what might be involved when you have your IT audit.
- Provide a checklist for your survival kit for how to best make it through your IT audit.



What Could You See in an IT Audit?

1. Test of **GENERAL CONTROLS**
 - Overall IT Environment
 - Development and Implementation of New Applications and Systems
 - Changes to Existing Applications and Hardware Systems
 - IT Security
 - IT Operations

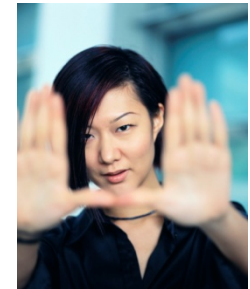
13



General Controls

Overall IT Environment

- IT Planning
- IT Training
- Evaluations



General Controls

Development and Implementation of Applications and Systems

- Project Management (SDLC, Project Methodology)
- Design/Selection of Software
- Testing of Applications/Systems
- Migration into Production
- Conversion of Data
- Training and Documentation

15

General Controls

Changes to Existing Applications and Hardware Systems

- Change Requests (Change Life Cycle)
- Testing of Program Changes/System Upgrades
- Migration to Production
- Training and Documentation



16

General Controls

IT Security



- Security Management (Computer Security Policy, Termination Procedures, Periodic Access, Access Authorization, Computer Violations)
- System-level Access (Operating System Level)
- Application-level Access (Menu/transaction Level)
- System Software and Utilities
- Physical and Environmental Controls

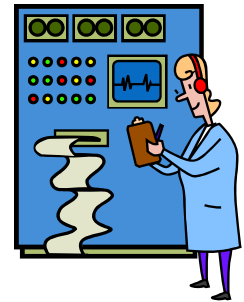


17

General Controls

IT Operations

- System Admin and Maintenance
(Operational failures, DB management, batch schedules)
- Backups
- Business Resumption/Disaster Recovery



What Could You See in an IT Audit?

2. Test of **APPLICATION CONTROLS**

- Trace and document a transaction through the application from input to output.
- Identify key automated controls along this path.
- Test the key automated controls.

19

Application Control Objectives:

Transaction-level control objectives:

1. Authorization
2. Completeness of Input
3. Accuracy of Input
4. Cutoff of Transactions
5. Transaction Classification
6. Transaction Occurrence

20



Application Control Objectives:

Cycle-level control objectives:

1. Existence
2. Integrity of Standing Data
3. Completeness/Accuracy of the Update
4. Completeness/Accuracy of Transaction Data
5. Restricted Access to Assets and Records

21

What Could You See in an IT Audit?

3. AUDIT SOFTWARE

- The auditor obtains a year-end detail transaction data file of the audit-significant application.
- Use audit software to perform data analysis.
- Refoot, stratify, detect gaps/dupes/bad data, identify populations, pull samples, produce aging reports, recalculate rates/fees, etc.

22

What Can I do to Survive?

Some suggestions on how to expedite the audit process for both you and those pesky IS auditors ...



What Can I do to Survive ?

- Know what applications/systems the auditors are testing; this should be made clear at the entrance conference (or sooner).
- Know ASAP when they are coming and how long they plan to stay.
- Understand what type of audit work will be conducted (G/C, application controls, substantive testing ?).

24



What Can I do to Survive ?

- Try to have the auditors provide an initial request of supporting documentation ASAP.... Before the audit starts, if possible.
- Have an audit liaison assigned to the audit team management (can act as helpful interface/hammer if problems arise).



25

What Can I do to Survive ?

- Conduct brief periodic status meetings to hear recommendations/audit issues as they occur.
- Make sure you know the various levels of comments you may receive (verbal, CD, SD, MW, etc). Understand the possible implications of these comments to your entity.

26



What Can I do to Survive ?

- Budget for staffing to assist the auditors (more doable after a few audit cycles).



- Make sure you invite key players to the exit conference to minimize second-hand dissemination of audit findings and discussions.



27

What Can I do to Survive ?

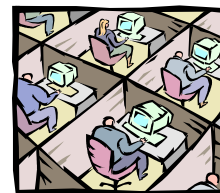
- Provide any requested audit items ASAP.
We know you're very busy but...
- Ask what will be expected at the next audit?
Provide a status of prior year
recommendations? Other audit issues?

28



What Can I do to Survive ?

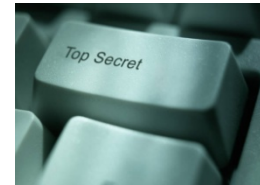
- Plan to provide space and connectivity to your auditors.



- Be familiar with the best practices that guide the data processing control and processing environment. (DAS and CoBiT are used by the AoS for state agency audits.)

What Can I do to Survive ?

- Be sure you discuss how sensitive audit data (e.g. security parameters, data files w/ personal identifiable information) will be handled when requested.



- A contact list w/ key contact names, numbers, email addresses is valuable to the audit team.

What Can I do to Survive ?

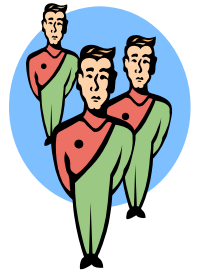
- Establish ASAP how you want the auditors and your staff to request/receive information. (Through a liaison, managers, contact personnel, whoever provides the data?)
- Make sure any request you receive from the auditor is prioritized so lengthy requests can be completed most effectively.

31



What Can I do to Survive ?

- Emphasize communication between the auditors and the different participating departments to eliminate any redundant requests for the same information.
- Consider key performance indicators (KPI) to monitor your internal goals for providing documentation to the audit team.



32

What Can I do to Survive ?

- Have policies, procedures, and standards for all key processes in your IT shop..... AND FOLLOW THEM.
- Have policies that cover computer usage, terminations, access authorization, periodic access reconciliations, computer violation reporting, IDS, firewall admin, application development/acquisition, program change, batch processing, data security and privacy, backup and retention, DRP, DB admin.



33

And Finally...



- If you have ANY questions for your auditors, NEVER hesitate to ask them.
- Remember: We're your friends and we're there to help !



Auditor of State Office

Information Systems Audit (ISA)

88 East Broad Street, 10th Floor
Columbus, Ohio 43215

Jim Swonger, CISA

Presenter Phone: (614) 728-7214

Office Fax: (614) 728-7199

E-mail: jmswonger@auditor.state.oh.us

35





Mary Taylor, CPA
Auditor of State

88 East Broad Street
Columbus Ohio, 43215

Phone: (800) 282-0370 Fax: (614) 466-4490

E-mail: contactus@auditor.state.oh.us

www.auditor.state.oh.us



Ohio Office of Budget and Management

Business Process and IT Audit

About the Office of Internal Audit

- Created under HB 166
- Includes 20 state agencies
- Reports to Office of Budget & Management and the State Audit Committee

Definition: Internal Audit

- Internal auditing is an **independent, objective assurance and consulting** activity designed to **add value and improve an organization's operations**. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to **evaluate and improve the effectiveness of risk management, control, and governance processes**.

Goals

- Ensure Agencies are governed efficiently
- Ensure projects and systems are successful
- Ensure processes are optimized
- Ensure transparency and accountability
- Ensure risks are understood and managed

Key Focus Areas



Financial



Business Process



Information Technology



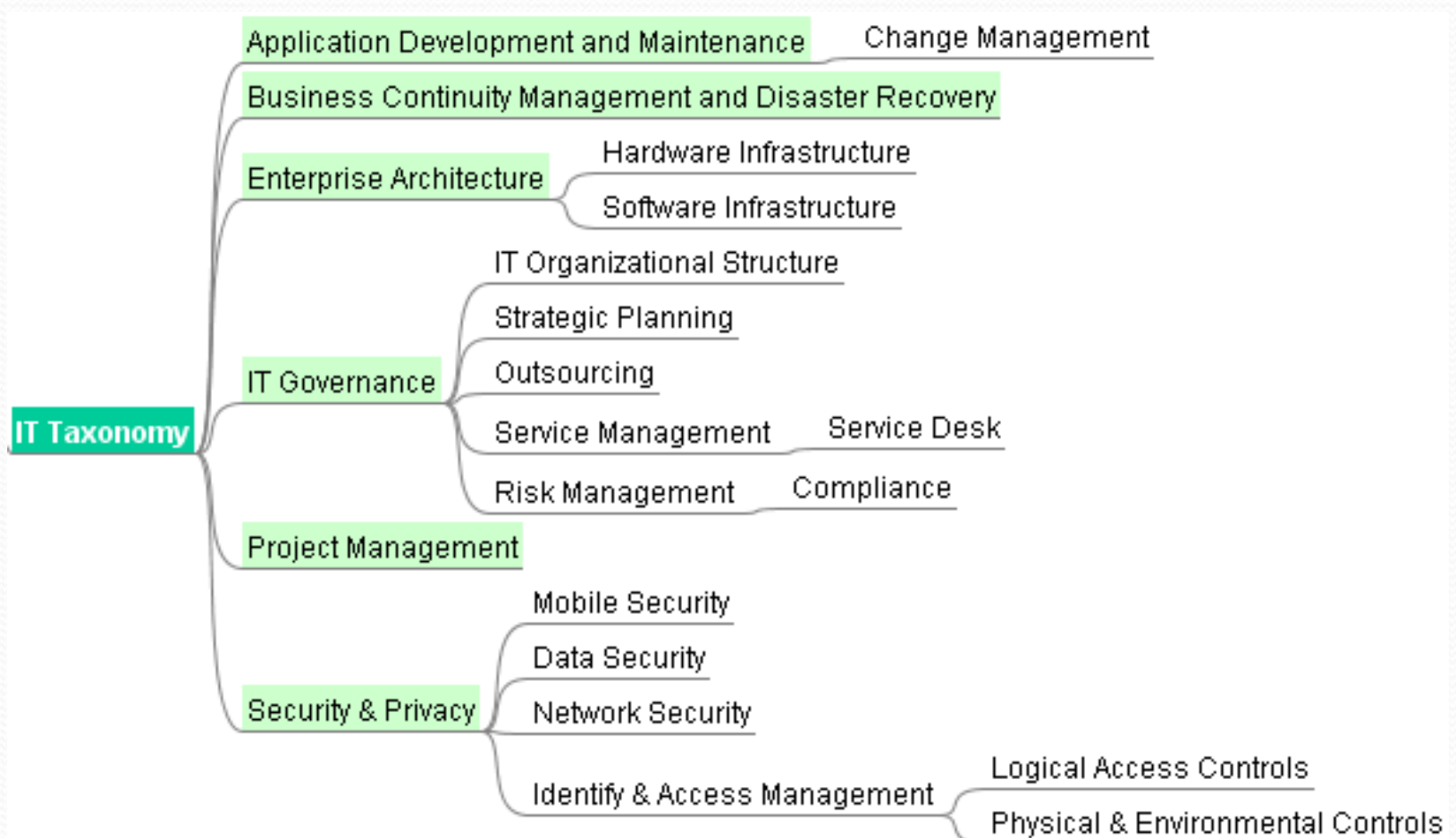
Outputs

- Agency Audit Reports
- Enterprise Audit Reports
- Top 10 Business Process concerns
- Top 10 IT concerns

Frameworks / Standards

- Department of Administrative Services
 - Office of Information Technology
- Agency-specific policies / standards / guidelines / procedure
- Committee of Sponsoring Organizations of the Treadway Commission (**COSO**)
- Control Objectives for Information and Related Technology (**COBIT**)
- IT Governance Institute's **Val IT** Framework
- Information Technology Infrastructure Library (**ITIL**)
- Sarbanes-Oxley Act (**SOX**)

IT Taxonomy



Upcoming Business Process Assurance Activities

- **Enterprise Maturity**
 - Evaluate enterprise maturity with process-based transformation
- **Process Maturity**
 - Audit "Payroll" process
 - Audit "Procurement & Vendor Review" process
 - Audit "Expenditures & Accounts Payable" process
 - Audit "Financial Reporting" process

Upcoming IT Assurance Activities

- **IT Governance**
 - Gather information about organization's IT environment
- **IT Governance – Strategic Planning**
 - Evaluate Business-IT Priority Alignment
- **IT Governance – Service Management**
 - Evaluate IT Service Desk process
- **Security & Privacy – Data Security**
 - Evaluate Database Activity Monitoring
- **Security & privacy – Mobile Security**
 - Evaluate Laptop & Portable Devices Security
- **Business Continuity Management and Disaster Recovery**
 - Audit DR testing on revenue generating sites (Taxes & Licenses, Fees & Permits)



Ohio Office of Budget and Management

Raj Subramanian

Chief of Business Process & IT Audit

Office of Internal Audit

Phone: 614-466-1976 (W)

Email: Raj.Subramanian@obm.state.oh.us



Ohio Office of Budget and Management

Office of Internal Audit

30 E. Broad Street, 35th Floor
Columbus, OH 43215

Joe Bell

Chief Audit Executive

mail: Joe.Bell@obm.state.oh.us

OHIO

DIGITAL GOVERNMENT SUMMIT

GOVERNMENT TECHNOLOGY
EXECUTIVE EVENTS



A GOVERNMENT TECHNOLOGY EXECUTIVE LEADERSHIP FORUM