Surviving an IT Audit

Michael Hammond, CISA, CRISC, CISSP, C|EH
Director, IT Audit Services
O’Connor & Drew P.C.
mhammond@ocd.com
www.ocd.com
Who am I?

Michael Hammond

- USAF veteran (IT and paralegal)
- 15 years global financial services company
  - System admin (Win/Linux/VMware,AIX,Solaris)
  - IT manager
  - IT service delivery manager
  - Internal IT Audit
- October 2012, moved to Public Accounting ~ Started IT Audit practice
Agenda

- What is an IT Audit?
- What can trigger an “Audit”?
- Inside the IT Audit process
- Resources
What is an IT Audit?

- An independent examination of IT controls
- A check and balance in the system of controls
- An objective party evaluates control design and efficacy using test samples against the control objectives
- Not the enemy; a control function, like Risk or Legal
Types of Audits

- IT General Controls (ITGC)
  - Network, Server, Storage, Datacenter control settings
  - System level administrator or privileged access
  - Backups
  - Password controls
- Application Control Review
  - Business rules applied via technical controls; SAP, PeopleSoft, Line of Business App
  - Separation of Duty (SoD)
- Integrated Audits
  - Business Auditor & IT Auditor work as one team to assess an end to end business process inclusive of management and technical controls
What Can Trigger an IT Audit
Internal and External Triggers

- Internal
  - Board of Directors (Audit and Examining Committee)
  - Continuous Monitoring control testing
  - Enterprise Risk review
- External
  - Privacy Laws (201 CMR 17)
  - Credit Card Payments (PCI-DSS)
  - HIPPA
  - Software Audits (BSA)
Massachusetts 201 CMR 17
Standards for the protection of personal information for residents of the commonwealth. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records.

Management
- Written Information Security Policy (WISP)
- Employee training

Identification
- Risk assessment and classification
- Systems and processes that collect & store PII

Protection
- Detecting and preventing system failures; patches, virus, etc
- Access Controls; restrict access to records and files containing PII to those who need such information to perform their job duties
- Encryption; in storage and transmission across public networks
Inside the IT Audit Process
IT Audit process

1. Understand the Control Environment
2. Identify Key Controls
3. Evaluate Design
4. Test Effectiveness
5. Report Findings
Guiding Principles

- Never, ever lie or misrepresent the facts
- Don’t cover up the truth
- Identify risk
- Rate risk
- Identify controls which mitigate the risk
- Perform self testing using standard frameworks
- Self identify control weakness
- Identify best practices, map internal controls
IT Audit Preparation Tips

• Ask yourself these questions:
  • Who are the stakeholders?
  • What does the InfoSec policy require (password complexity)?
  • What do the lawyers require (retention/compliance)?
  • What happens if the control breaks and what could go wrong?
  • What happens if the risk materializes?
  • What are Best Practices for your industry?
  • Is this a compliance review (check the box) or risk based?

• Document these questions and answers

• Repeat! Repeat! Repeat!
IT Audit Preparation Tips

• Align yourselves with other technical verticals. Auditors like to see you are thinking of the big picture, and not just silos of execution. The process can fall down between groups.

• Use common frameworks (NIST, ISO, COBIT) as guidelines for leading practices.

• Collaborate with the Auditors outside of the actual audit.
IT Audit Execution Tips

• Auditors, especially new auditors, often do not know your process and controls as well as you do. They may not be subject matter experts in the technology.

• The auditors role is to ask questions, document control points, and observe evidence which satisfies the control objective. Questions such as:
  • Where is documentation to manage the platform/application kept?
  • How is a new employee added/removed to/from an application?
  • How is a new administrator added/removed to/from a platform?
  • How is the application or operating system kept up to date?
IT Audit Support

Providing evidence to support controls

• Screenshots are great to show **existence** (but they may not show evidence of yesterday or last month)
IT Audit Support

Providing evidence to support controls

- Dump of a log file to evidence **effectiveness** of a control

- Records (pdf/csv/word) retained in a secured read only location are ideal for evidencing **effectiveness** over time. Create checksums.
IT Audit Support

Creating MD5sums - http://www.md5summer.org/
IT Audit Support

Providing evidence to support controls
• Capture date/time and host name in screenshots
IT Audit Support

Providing evidence to support controls

Make the auditor do the heavy lifting

• Let the auditor watch you dump the log file or configuration and then provide it to them for analysis
• Let the auditor watch you export the running configuration to a development appliance. Give the auditor credentials for review
• Grant the auditor access to the synchronized disaster recovery node to review

These not only share the workload, but foster a trusting relationship between IT and IT Audit.
Software Audits

• You negotiated (hopefully) for software licenses, negotiate the software audit as well

• Perform your own software audit to identify discrepancies in licensing
SANS 20 Critical Controls (1-4)

<table>
<thead>
<tr>
<th>Critical Security Control</th>
<th>Critical Security Control Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Inventory of Authorized and Unauthorized Devices</td>
<td>Reduce the ability of attackers to find and exploit unauthorized and unprotected systems: Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops, and remote devices.</td>
</tr>
<tr>
<td>2 Inventory of Authorized and Unauthorized Software</td>
<td>Identify vulnerable or malicious software to mitigate or root out attacks: Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.</td>
</tr>
<tr>
<td>3 Secure Configurations for Hardware &amp; Software on Laptops, Workstations, and Servers</td>
<td>Prevent attackers from exploiting services and settings that allow easy access through networks and browsers: Build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system.</td>
</tr>
<tr>
<td>4 Continuous Vulnerability Assessment and Remediation</td>
<td>Proactively identify and repair software vulnerabilities reported by security researchers or vendors: Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.</td>
</tr>
</tbody>
</table>
Resources

- ISACA – CoBIT - www.isaca.org
- COSO – www.coso.org
- Michael Hammond – mhammond@ocd.com