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
✓ IT Audit Reporting
✓ 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 a controls 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, LOB
  - Separation of Duty (SoD)
- Integrated Audits
  - Business Auditor & IT Auditor work as one team to assess a business process inclusive of management and technical controls
What Can Trigger an IT Audit
Internal and External Triggers

- Internal Audits
  - Board of Directors (Audit and Examining Committee)
  - Continuous Monitoring control testing
  - Enterprise Risk review
- Federal Govt
  - FISMA
- External Audits
  - Public Companies (SOX)
  - Credit Card Payments (PCI-DSS)
  - HIPPA
  - Software Audits (BSA)
- Service Provider Audits
  - SSAE16 (SOC1, SOC2, SOC3, AT 101)
Service Provider Audits

**SOC1 (SSAE 16)**
- Restricted Report
- Report on Financial Controls
- Type 1 – Design
- Type 2 – Design & Effectiveness

**SOC2 (AT 101)**
- Restricted Report
- Review of Compliance & Operations

**SOC3 (AT 101)**
- Marketing Material
- Review of Compliance & Operations
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
• Identify best practices, map internal controls
IT Audit Preparation Tips

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

• Document these questions and answers

• Repeat! Repeat! Repeat!
IT Audit Preparation Tips

• Auditors like to see you are thinking of the big picture, and not just siloes of execution.

• Use of frameworks (NIST, ISO, COBIT) and why.

• Use the Auditors outside of the actual Audit.
IT Audit Execution Tips

- Auditors, especially new Auditors, often do not know your process and controls. They almost certainly do not know your technology. That is not their responsibility.

- Their job is to ask questions, document control points, observe evidence meets the control objective.

- Questions such as:
  - Where is documentation to manage the platform/application kept?
  - How is a new employee added/removed to the application?
  - How is a new administrator added/removed to the platform?
  - Who do you escalate issues to? Where do you get outside help?
IT Audit Support

Providing evidence to support controls

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

Providing evidence to support controls

• Dump of log files are great to evidence **effectiveness** of a control.

• Records (pdf/csv/word) retained in a secured read only location are ideal for evidencing **effectiveness** over time.
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 work.
  - 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 config and load it on a DEV appliance and then provide them the login credentials to the DEV appliance
  - Give the Auditor access to the synchronized DR node to review
IT Control Process Maturity

Continuous (Management) Monitoring

- Evaluate current state maturity and the highest level target of control maturity
  - This **does not** mean the operation center is “always on”.
  - This **does** mean control testing metrics are captured and reviewed by management and changes to existing controls are evaluated for risk mitigation and value towards the target maturity

For example:

- Backups are performed nightly. However, the restore metric over time shows critical files are not available for restore. Refine the backup control.
- Egress monitoring alerts on potentially sensitive files leaving the network. Monthly review of these reports “tweak” the filters. Management reviews the effectiveness of these tweaks to refine the control.
IT Audit Reporting
Impact of Audit Reports

Often heard “The Audit report got him/her fired”. In reality…..

• Audit reports are an opinion based on the examination results

• Audit reports can be used to drive enhancements of controls and their effectiveness; funding and focus (people/ process/ technology).
Combined with Financial Statements

- **Unqualified Opinion** – Based on the auditors reasonable assurances of testing controls, this is a clean report.

- **Qualified Opinion** – The Auditor found a situation which does not comply with generally accepted principles, but otherwise the testing found no other significant observations.

- **Adverse Opinion** – The Auditor found the auditee materially misstated a financial statement.
Software Audits

• You negotiated (hopefully) for software licensees, negotiate the software Audit as well

• Perform your own software Audit for findings
Observation Remediation

• Agree on management action to be taken to remediation observations before execution
• Retain remediation evidence long enough to show remediation was completed for the next Audit.
• Include date/time stamps in screenshots with server/node names identifying devices.
• Reevaluate Auditor observations periodically to identify if recommended control enhancement still mitigates the original risk. There is no value in executing unnecessary controls.
Resources

- ISACA – CoBIT-  [www.isaca.org](http://www.isaca.org)

- ISO – ISA 27001/27002-  


- GTAG – Global Technology Audit Guides -  [https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Practice-Guides.aspx](https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Practice-Guides.aspx)

- COSO –  [www.coso.org](http://www.coso.org)


- Me! –  [mhammond@ocd.com](mailto:mhammond@ocd.com)