



Streamlining Security Audits

2004 ISACA Conference – San Francisco

Douglas W. Barbin, CISSP, CPA, CFE, GCFE
Director – Global Security Consulting



Let's Kickoff with a Discussion...

Why do security audits take so long?

At the end of the audit, what are some of the key disappointments or failures that can occur?

Why do you think these occurred?



Why Do Security Audits Take So Long?

Missed expectations require the auditor to redo some portion of the audit or assessment.

- + The scope of the audit was not correctly identified and bound
- + The level of detail was either too much but more often not enough

The “right” requirements and standards were not used so retests had to be performed.

- + Holes in the assessment methodology
- + Confusion or misunderstanding of the standards

The person or persons performing the audit did not have the right qualifications and had to “fumble” about the audit.

The tools did quite gather all of the necessary information so retests had to be performed.



And the Let Downs...

“Didn’t cover everything I wanted or needed.”

“Not detailed (or deep) enough.”

“Too detailed, in the wrong areas.”

“Didn’t address (or fully address) X regulation or Y standard”

“Reports didn’t contain the right types of lingo that help me with my compliance challenges.”

“Auditors didn’t know what they were doing.”

“Tools did not hit the right areas.”

“Tools interrupted my company’s network.”



Common Themes or Drivers

Terminology

Expectations Management

Requirements and Standards

Scope

- + What to audit

- + How “deep” to audit

Deliverables

Auditor Qualifications

Tools



Intro and Objectives

Introduction

- + I started as a Forensic Accountant and segued to Computer Forensics and Security Auditing
- + I currently run VeriSign's Consulting Practice on the West Coast
- + I have managed hundreds of information security audits
- + I current manage VeriSign's West Coast Security Practice

Objectives/Outline

- + Discuss how to make audits more efficient and effective manner
- + Discuss how to better use processes, frameworks, and standards
- + Discuss the types of skills and training needed
- + Discuss security audit tools and when most appropriate to use them



Frameworks and Standards

The Audit Framework includes:

- + Source: Standards and Requirements
- + Criteria
 - How the Standards and Requirements are Assessed?
 - Criteria for success/failure

Sources

- + Regulations (HIPAA, GLBA, 21 CFR Part 11, etc.)
- + Industry Standards (ISO17799, Visa CISP, MasterCard SDP, etc.)
- + Audit Frameworks (FFIEC, COSO, COBIT, etc.)

What is Needed

- + Understanding of ALL sources
- + Mapping of High Level Regulations/Standards and Criteria
- + Mapping to a common criteria or set of audit sources standards



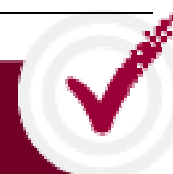
High-Level Standards Mapping Example

Security Practice	HIPAA Standards	GLBA (FTC Regulations)	21 C.F.R. Part 11	California Law on Notice of Security Breach (Guidelines)
Access Control (e.g., unique user identification, emergency access procedure automatic logoff, encryption and decryption)	✓	✓	✓	✓
Audit Controls	✓	✓	✓	✓
Integrity Controls (e.g., mechanism to authenticate data)	✓	✓	✓	✓
Person or Entity Authentication	✓	✓	✓	✓
Transmission Security (e.g., integrity controls or encryption)	✓	✓	✓	✓



Specific Requirements

Platform/Application Logon			Describe controls in place or planned. Use additional comments.	Planned Controls Target Date
Control	Y/N?	RA Sheet reference		
PASSWORD CONSTRUCTION Are password lengths a minimum of 6 characters?		P, OSS, VI, A		
PASSWORD CONSTRUCTION Must passwords contain at least one alpha, one numeric, and one special character?		P, OSS, VI, A		
PASSWORD CONSTRUCTION If tools are available to validate the password construction, have they been deployed and verified to ensure they do not in themselves compromise the passwords?		P, OSS, VI, A		
PASSWORD EXPIRATION Where available, does the system warn the user of the pending expiration of his or her password according to Company policy?		P, OSS, VI, A		
INITIAL PASSWORDS When an account is created, is it assigned a random and secure password that is preset to expire upon logon?		P, OSS, VI, A		
INITIAL PASSWORDS Are the passwords assigned by security administrators unique to each user?		P, OSS, VI, A		
DEFAULT PASSWORDS Have all default passwords and user IDs/accounts for all hardware and software products been changed?		P, OSS, VI, A		
PASSWORD CHANGES Must a valid password be entered before it can be changed?		P, OSS, VI, A		
PASSWORD CHANGES Are password changes logged as part of the Session Activity Log?		P, OSS, VI, A		



Other Example (Source: ISF)

ISO Ref	ISO/IEC 17799 Sub-heading level	SH Ref	Security Healthcheck Question(s)
3.1.1	Information security policy document	4	Is there a comprehensive, documented information security policy?
3.1.1	Information security policy document	5	Is the information security policy communicated to all individuals with access to the enterprise's information and systems?
3.1.2	Review and evaluation	4	Is there a comprehensive, documented information security policy?
4.1.1	Management information security forum	1	Has top management's direction on information security been established?
4.1.1	Management information security forum	2	Is top management's (eg board-level director) commitment to information security demonstrated?
4.1.1	Management information security forum	3	Is control over information security provided by a high-level working group, committee or equivalent body?
4.1.1	Management information security forum	9	Is there a specialist information security function?
4.1.2	Information security co-ordination	11	Are individuals appointed to co-ordinate information security arrangements locally?
4.1.2	Information security co-ordination	12	Are local security co-ordinators competent to carry out their security responsibilities?
4.1.3	Allocation of information security responsibilities	21	Is 'ownership' of critical information and systems assigned to capable individuals?

	Security Healthcheck Question(s)	Response	Extended Information
1	Has top management's direction on information security been established?	Question not selected	Direction on information security can be set by: developing a high-level information security policy that applies enterprise-wide; assigning overall responsibility of information security to a top-level director or equivalent; chairing key information security working groups; monitoring the security condition of the enterprise; and allocating sufficient resources to information security.
2	Is top management's (eg board-level director) commitment to information security demonstrated?	Question not selected	Top management should demonstrate their commitment to information security by: 'signing-off' key documents (eg an information security policy); assigning overall responsibility for information security to a top-level director (or equivalent); chairing key information security working groups; monitoring the security condition of the enterprise; and allocating sufficient resources to information security.
3	Is control over information security provided by a high-level working group, committee or equivalent body?	Question not selected	A high-level working group, committee or equivalent body would typically consist of: top management; one or more business 'owners'; the head of information security (or equivalent); representatives of other security-related functions; or the head of IT (or equivalent).



Requirements . . . Interpretation . . . Scope

Terminology is Key

- + Audit terms
- + Standards terms
- + Technology terms

Interpretation/Guidance

- + Provided in the standards
- + Putting the honours on the auditor's judgment

Scope

- + Expectations of testing
- + Level of detail
- + Sample size
- + Specific tests

Lessons

- + Need to be on the same page in terms of terminology
- + Understand (AND AGREE UPON) the standards
- + Understand (AND AGREE UPON) what constitutes success/failure
- + Understand (AND AGREE UPON) test procedures and sampling approach



Skills and Training

- Standards are often incomplete and lack specific clarity
- Traditional audit standards have always relied more on the experience of the auditor than the details of the requirements
- Challenge is that auditors and even some IT auditors do not always have the skills and training necessary to perform Information Security Auditors
- Some Examples of Skills/Training that would be most applicable to auditors:
 - + Policies, Standards, and Regulations
 - + Network and Security Architecture
 - Network Segmentation Concepts
 - External Points of Presence
 - Wireless Access Points
 - + Firewall Technology
 - + Common Threats and Vulnerabilities
 - + Assessment Toolsets



Tools

- Enterprise Tools
 - + NetIQ
 - + Symantec ESM
- Patch/Configuration Management Tools
 - + Pedestal Security Expressions
 - + Patchlink
- Vulnerability Assessment Tools
 - + Nessus/NeWT
 - + GFI LanGuard
 - + CyberCop
 - + ISS Internet Scanner
 - + ISS System Scanner
- Technology Enabled Services
 - + VeriSign MVPS (shameless plug)
 - + Qualys
 - + Foundstone FoundScan
 - + Securescan Perimeter



Tools

- Web and Application Assessment Tools

- + Nikto
- + Paros
- + SPI Dynamics WebInspect
- + Kavado ScanDo
- + Watchfire (formerly Sanctum) AppScan
- + OWASP WebScarab (Open Source)

- DataBase

- + AppDetective for Web Applications (AppSecInc)
- + ISS Database Scanner

- Platform Specific Tools

- + CIS Tools
 - Windows
 - Unix
 - Cisco
- + Somersoft Tools (e.g. DumpSec)



Tools

- War-Dialing
 - + THC-Scan
 - + PhoneSweep
- Password Auditing
 - + L0pht Crack 5
 - + John the Ripper
- Wireless
 - + NetStubler
 - + Kismet
 - + GPS Unit & MapPoint
- AS/400 and Mainframes
 - + ESM Modules
 - + AS/400 Manual Questionnaires
- Others? What have Your Experiences Been?



Summary

What we've talked about:

- + We've talked about the challenge of implementing information security audits
- + We've discussed key of successful security audit planning and the pitfalls therein
- + We've talked about training and need for the auditors to have and maintain certain skills
- + We've talked about the tools need and how to evaluate them to make sure they meet the specific needs of the audit

In short . . . The security audit process is far for standard and very complex. Prior proper planning cannot be understated.

I thank all of you for your time, your input, and your and interaction today.





Thank You!

dbarbin@verisign.com

916.928.7230

