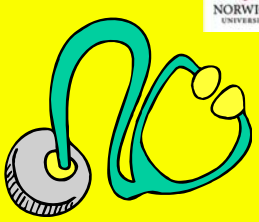
Security Audits, Standards, & Inspections

CSH6 Chapter 54

"Security Audits, Standards and Inspections"

Donald Glass, Chris Davis, John Mason, David Gursky, James Thomas, Wendy Carr, and Diane Levine

Topics



- Introduction
- Auditing Standards
- SAS 70 Audits
- Sarbanes-Oxley
- Addressing Multiple Regulations
- Technical Frameworks for IT Audits

Introduction (1)

- Non-IT auditors
  - Financial: accuracy/integrity accounting
  - External: material, macro-level issues (e.g., governance, reporting, legal compliance)
  - Internal: transaction-level controls, protecting assets, validating systems
- Recent legal/regulatory changes affect auditing
  - Especially *regulatory* compliance
  - Validating protection of mission-critical systems
  - Ensuring that weaknesses in IT infrastructure/security do not affect other parties (who can sue for damages)

Introduction (2)

- Management attitudes range from
  - We have to do this – part of cost of doing business
  - Nice to have (but don't spend much)
- These attitudes ignore added value from audits
  - QUESTION FOR CLASS: WHAT ARE SOME BENEFITS OF AUDITS BEYOND ASSURANCE OF COMPLIANCE?
  - Auditing increasingly included in IA training programs & certifications

Auditing Standards

- Introduction to ISO
- ISO/IEC 27001
- Gramm-Leach Bliley Act
- Auditing Standards Conclusions

Introduction to ISO

- International Organization for Standardization
  - Nongovernmental cooperative
  - Create, identify, publish industry standards
  - Business & technology (not just IT)
- Member committees work on specific standards
  - Represent best practices
  - E.g., ISO 9000 standards have become world-recognized for quality
  - ISO 27000 increasingly accepted as international standard for information security management
- See also CSH6 Chapters
  - 44 "Security Policy Guidelines"
  - 65 "Role of the CISO"

History of ISO Standards (1)

- British Standard (BS) 7799 published Feb 1995
  - Part 1: *Best Practices for Information Security Management*
  - Part 2: *Specifications for Information Security Management Systems*
  - Part 3: *Guidelines for Information Security Risk Management*

History of ISO Standards (2)

- BS 7799 Part 1 became ISO 17799 (Dec 2000) with 10 domains:

1. Business continuity planning
2. Systems access control
3. System development & maintenance
4. Physical & environmental security
5. Compliance
6. Personnel security
7. Security organization
8. Computer & operations management
9. Asset classification & control
10. Security policy

History of ISO Standards (3)

- Later converted ISO 17799 to ISO/IEC 17799:2005
  - IEC = International Electrochemical Commission (Geneva)
  - Information Technology – Security Techniques – Code of Practice for Information Security Management
- Added objectives, controls
- Updated previous editions to include new technology
  - E.g., wireless networks
- ISO/IEC 27000 goes beyond ISO/IEC 17799 (see next slides)

ISO/IEC 27001 (1)

- ISO/IEC 27000: Fundamentals & Vocabulary
- ISO/IEC 27001:2005. ISMS – Requirements
- ISO/IEC 27002:2005. Code of Practice for Information Security Management
- ISO/IEC 27003:2010. ISMS Implementation Guidance
- ISO/IEC 27004*. Information Security Management Measurement
- ISO/IEC 27005*. Information Security Risk Management
- ISO/IEC 27006:2007. Requirements for Bodies Providing Audit and Certification of Information Security Management Systems

Notes:
ISMS = *information security management system*
* Under development as of March 2010

ISO/IEC 27001 (2)

- ISO/IEC 27001
  - Similar to OECD guidance on security of IS & NW
  - Includes PDCA cycle
    - ✓Plan-Do-Check-Act
    - ✓Invented by W. Edwards Denning (1950s)
- Certification
  - Indicates formal compliance with standards
  - Business benefits (public visibility to stakeholders)
  - Operational benefits (fewer errors, better response, greater resilience)

Gramm-Leach Bliley Act

*Financial Services Modernization Act of 1999 = GLBA**

- Main proposers were Phil Gramm, Jim Leach, and Thomas Bliley, Jr
- Regulates security of consumers'
  - Personal financial information
  - Nonpublic personal information (NPI)
- Also governs
  - Privacy requirements for information
  - Disclosures to third parties
  - Prevention of pretexts for information-gathering

***See also CSH6 Chapter 64: US Legal & Regulatory Issues**

Auditing Standards Conclusions

- May combine compliance, auditing, risk management into cooperative function
- Growing managerial acceptance of need for risk management
- Benefits of regular audits include
  - Threat identification
  - Reduced costs through optimization of resource allocation & operations
  - Support for internal information assurance
  - Protection against lawsuits through certification & compliance with industry standards
  - Supporting due diligence claims

SAS* 70 Audits

- Introduction to SAS 70
- Costs and Benefits of SAS 70 Audits
- SAS 70 Audits Conclusion

*Statement of Auditing Standards

Introduction to SAS 70 (1)

- SAS 70 = Statement on Auditing Standards 70
  - American Institute of Certified Public Accountants (AICPA)
  - *Reports on the Processing of Transactions Used by Service Organizations*
  - Full text available online http://umiss.lib.olemiss.edu:82/record=b1038093
- Terminology
  - *Service organization* (provides outsourcing)
  - *Service auditor* (works for outsourcer)
  - *User organization* (client)
  - *Users' auditors* (works for client)

Introduction to SAS 70 (2)

- SAS 70 audits primary method of evaluating possible outsourcing supplier
- Outsourcing growing
  - Reduce costs
  - Focus on mission-critical function internally
  - Outsourced functions include
    - ✓Customer service, help desk
    - ✓Back-office data processing
    - ✓Human resources management, benefits
    - ✓Web site hosting
    - ✓Claims processing
    - ✓Finance & accounting

Introduction to SAS 70 (3)

EXHIBIT 54.1 Types of SAS 70 Audits

SAS 70 Report Content	Type I	Type II
Independent service audits report	Included	Included
Service organizations description of controls	Included	Included
Information provided by the independent service auditor; includes a description of the service auditor's tests of operating effectiveness and the results of those tests	Optional	Included
Other service relevant information	Optional	Included

- Type II audits include mandatory tests
- Type I may not test controls
- Therefore Type II more expensive but preferable for organizations desiring continuous process improvement

Introduction to SAS 70 (4)

- Process
  - Initial assessment
  - Evaluation of processing / transaction systems & controls
  - Develop statement of work (SOW)
  - Present SOW with estimated
    - ✓Completion date
    - ✓Details
    - ✓Costs
  - Interviews with management, technical administrators

Introduction to SAS 70 (5)

- Management of audit team
  - ❑Usually CPA in charge of team
  - ❑Technical audit lead
    - ✓Evaluation / testing systems & networks
  - ❑Application lead
    - ✓Evaluation / testing application software
    - ✓E.g., databases, administrative software
- Auditors evaluate compliance with internal & external standards
- Report on deviations from expectation

Costs and Benefits of SAS 70 Audits

- Initial SAS 70 audit costs between $25K - $1M
- Small organization may not find it cost-effective
- Larger organizations use SAS 70 to comply with GLBA and SOX (Sarbanes-Oxley Act)
- SAS 70 uses COSO** standard
  - ❑Process for reviewing internal controls
  - ❑SOX §404 uses COSO – see next section of these slides & §54.4 of text
- See pro/cons of SAS 70 (Exhibit 54.2 in CSH6)
  - ❑Reformulated on following page

** Committee of Sponsoring Organizations of the Treadway Commission

Costs & Benefits of SAS 70 Audits (reformulated)

Feature	For User Org	For Service Org
Independent assessment of controls	+	+
Lower cost for evaluation of controls	+	-
No additional review of controls required	+	-
SAS 70 audits are forward looking (can refer to predictions)	-	-
SAS 70 audits must be continuously reviewed & updated	+	-
SAS 70 audits increase value of services	+	+
Disruption to service organization reduced by eliminating need for user organization auditors to audit service organization	+	+
SAS 70 audit can be used to build strong working relationship between service & user organizations	+	+
Audit results can provide opportunities for improvements	+	+

SAS 70 Audits Conclusion

- SAS 70 audit is *not* 100% guarantee of perfect security
- But viewed as high-level assurance for confidence
- Particularly useful in ensuring compliance with SOX §404 reporting
  - ❑*See next section of slides*

Sarbanes-Oxley (SOX)

- Introduction to SOX
- Section 404
- Achieving Compliance
- Audit and Certification
- SOX Conclusion

Introduction to SOX (1)

- Financial reporting act enacted July 2002
  - ❑Guided by Paul S. Sarbanes & Michael G. Oxley
- Response to scandals (Enron, WorldCom)
  - ❑Enron
    - ✓Oct 2001 – executives hid $B in debt
    - ✓Share prices crashed from $90 to $1
    - ✓$11B losses by shareholders
    - ✓Execs went to prison for fraud
    - ✓Auditors went bankrupt
  - ❑WorldCom
    - ✓Fraudulent accounting started 1999
    - ✓2002: auditors proved $3.8B fraud (ultimately found $11B fraud)

Introduction to SOX (2)

- Executive officers must
  - Certify effective internal controls
  - Accept personal responsibility/liability for failures
- SOX provides for severe penalties
  - Civil, criminal
  - May include imprisonment of officials
- Organizations must plan for repeatable demonstrations of compliance

SOX §404

- Directly addresses IT in financial reporting
- Requires attention to internal controls
  - Adequacy
  - Effectiveness
- Widespread industry acceptance of need for constant, honest compliance

Achieving Compliance

- Intro to SOX Compliance
- Control Framework
- COSO
- CobiT
- Testing

Intro to SOX Compliance

- Identify key processes in organization
- Determine how processes implemented & controlled
- Determine methods for reporting success / failure
- Provide coverage across entire system life cycle
- Include projects, design, architecture, development, delivery, operations
- Auditor will examine core processes, adequacy of controls, execution of controls

Control Framework

- Securities & Exchange Commission (SEC) mandates COSO framework
- Public Company Accounting & Oversight Board (PCAOB)
  - Also supports COSO
  - In Auditing Standard No. 2,
    - ✓ *An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements*

COSO* Framework

- See http://www.coso.org
- Core elements of internal control:
  - Control environment
  - Risk assessment
  - Control activities
  - Information & communication
  - Monitoring

* Committee of Sponsoring Organizations of the Treadway Commission

COBIT (1)

- ISACA* defined *Control Objectives in Information Technology* framework
- 4 domains, 34 IT processes, 215 control objectives
- Recommends 12 specific processes for SOX compliance (see CSH6 §54.4.3.3). Areas are:
  1. Application software
  2. Technology infrastructure
  3. Operations
  4. Solutions & changes

(cont'd next slide)

*Originally the *Information Systems Audit and Control Association*

COBIT (2)

- Areas in COBIT for attention in SOX compliance (cont'd)
  5. Changes
  6. Service levels
  7. 3rd party services
  8. System security
  9. Configuration
  10. Problems & incidents
  11. Data
  12. Physical environment & operations

Testing

- Issues
  - ❑Planning and scheduling tests
  - ❑Determining sample sizes
- Must balance resources & need for compliance
  - ❑Smaller samples cost less
  - ❑But reliability decreases
- SOX compliance includes more than technical infrastructure
  - ❑Also include processes in meetings

Audit and Certification

- Internal audit
  - ❑Culmination of SOX testing
  - ❑Final quality assurance checkpoint
  - ❑Verifies compliance
  - ❑Mandates correction of errors before external audit begins
- External Audit
  - ❑Usually end of financial year
  - ❑Should have *no* gaps or failings – all will be reported as noncompliance in final report
- Scheduling
  - ❑Some organizations certify quarterly or monthly

SOX Conclusion

- SOX compliance integrated into wider risk-management program
- Move to integration in control culture
  - ❑Embedded
  - ❑Proactive
  - ❑Risk-aware
  - ❑Genuine
    - ✓Don't allow attitude that mere compliance acceptable
    - ✓Must aim at exceeding current regulations
    - ✓Adapt to changes (internal & regulatory)

Addressing Multiple Regulations

- History of US Govt Security Standards
- Comprehensive Frameworks
- Legislative Requirements in USA
- NIST SP 800-53
- Federal Information Systems Management Act (FISMA)
- Risk Framework
- Multiple Regulations and IS Audits Conclusion

History of US Government Security Standards

- DoD Computer Security Center Rainbow Series
  - Began 1980s
  - Covers different colors
- Best practices developed
  - Standards
  - Experiences
  - Lessons learned
- Many sources today
  - ISACA,
  - DISA-STIG*
  - NSA,
  - NIST

*Defense Information Systems Agency *Security Technical Implementation Guides*

Comprehensive Frameworks

- **COBIT** – *Control Objectives for Information and related Technology*
  - http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx or http://tinyurl.com/46ul39f
- ITIL – Information Technology Infrastructure Library
  - http://www.itil-officialsite.com/
- National Institute of Standards & Technology
  - NIST SP 800-60: *Guide for Mapping Types of Information and Information Systems to Security Categories.*
  - http://csrc.nist.gov/publications/PubsSPs.html

Legislative Requirements in USA

- FISMA: Federal Information Security Management Act of 2002
- SOX: Sarbanes Oxley Act of 2002
- HIPAA: Health Insurance Portability & Accountability Act of 1996

NIST SP 800-53 Rev 4

- *Recommended Security Controls for Federal Information Systems*
  - Guidelines for selecting & specifying controls
  - Revised 2012-02-28
  - http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf
- Benefits
  - Consistent, comparable, repeatable approach to selecting security controls for IT systems
  - Minimum security controls consistent with FIPS* 199, *Standards for Security Categorization of Federal Information and Information Systems*
  - Stable/flexible catalog of controls
  - Foundation for assessment methods

*Federal Information Processing Standard

NIST SP 800-53 Rev 1 (cont'd)

- Applicable to all US federal information systems except designated national security systems
- Guidance for implementation of FIPS* 200, *Minimum Security Requirements for Federal Information and Information Systems*
  - Also used by state, local, tribal governments
  - Private-sector organizations in critical infrastructure
- Extensive framework consistent with wide range of requirements (see p 54.16)

*Federal Information Processing Standard

Federal Information Systems Management Act (FISMA)

- Passed into law as part of E-Government Act of 2002
- Requires every federal agency to
  - Develop
  - Document
  - Implement

  } Agency-wide IA program to control information & systems
- Includes framework of minimum requirements
  - See p 54.17

OMB Circular A-130, Appendix III

- Security of Federal Automated Information Resources
- Supports FISMA requirements
- Mandates
  - Planning for security
  - Ensuring appropriate officials assigned security responsibility
  - Periodic reviews of security controls
  - Authorizing system processing before operations begin
  - Periodic review of operations security

Risk Framework*

1. Categorize systems & needs
2. Initial security controls
3. Supplement for local conditions
4. Document plan
5. Implement controls
6. Assess controls
7. Authorize operations
8. Monitor & assess continuously

* §54.5.3

Multiple Regulations and IS Audits Conclusion

- NIST Computer Security Resources Center (CSRC) excellent start for resources
  - http://csrc.nist.gov/publications/PubsSPs.html
- FISMA consistent with COSO
- Excellent basis for adapting to local needs
  - Even if more stringent than legal requirements for specific organization
  - May forestall radical overhaul if regulations change

Technical Frameworks for IT Audits

- Framework 1: People, Processes, Tools & Measures
- Framework 2: STRIDE
- Framework 3: PDIO
- General Best Practices
- Technical Frameworks Conclusion

Framework 1: People, Processes, Tools & Measures

- PPTM good starting point for analysis

1. People central to security
2. Processes must be validated
3. Tools (including physical controls)
4. Measures – metrics (how do we know we are OK?)

Framework 2: STRIDE

1. Spoofing
2. Tampering
3. Repudiation
4. Information disclosure
5. Denial of service
6. Elevation of privilege

Framework 3: PDIO

1. Plan
2. Design
3. Implement
4. Operations

General Best Practices

1. Defense in depth
2. Positive security model (deny by default)
3. Fail safely
4. Run with least privilege
5. Avoid security by obscurity
6. Keep security simple
7. Detect intrusion & keep logs
8. Never trust infrastructure & services without checking
9. Establish secure defaults
10. Use open standards, not proprietary methods

Optional Homework

- Research any of the laws and frameworks discussed in chapter using Kreitzberg Library and Web searches
- Upload URL of interesting article(s) to NUoodle
  - Discuss interesting aspects relevant to audits and standards
  - Support for points made in chapter
  - Different perspectives on or contradiction of specific points
  - Additional insights of interest to class

Now go and study