SNIA

STORAGE NETWORKING INDUSTRY ASSOCIATION

EDUCATION

Preparing for a

Storage Security Audit

LeRoy Budnik, Knowledge Transfer

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA and is subject to other copyrights[1].
- Member companies and individuals may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced without modification
  - The SNIA must be acknowledged as source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee and the Storage Security Industry Forum.

[1] © 2000-2006 Knowledge Transfer

Abstract

Storage Security Audit

The thought of “being audited” often evokes fear. Actions taken on stored information, storage infrastructure security and the practices of storage professionals are all subject to internal and external audit. Recently, the specialized nature of IS auditing has extended to include the storage infrastructure, however, auditors with specialized storage skills and knowledge are a limited resource. Auditors are required to be technically competent in the storage area while being aware of the many standards and legal requirements, in addition to security guidelines. That makes them a great asset to our work! As a result, a storage security auditor can provide great benefit to the storage professional and their organization.

Storage professionals maintain information security policies within and around the storage infrastructure; some establish policies and practices, independently, or in concert with others. When we set a security or storage policy, we do so based on our understanding of the requirements, our personal experience and budget constraints. However, is our due diligence enough? This is where the auditor can provide external validation and recommendations (authentication, control, encryption, etc.) in midst of their role as professional skeptic and risk manager.

Objectives

In this session, we present a client case scenario, review the Storage Security Audit Process and then follow the process in a micro case study. Our goal is to prepare you for a storage security audit. In addition, we believe that your perspective will change from implementing storage security to designing for secure storage.

After completing this tutorial, you should be able to:

- Describe the Storage Security Audit Process
- Secure Information Assets in the Storage Systems
- Integrate security and governance practices into storage systems and storage infrastructure life cycle and management, including business continuity and disaster recovery

Storage Security Audit

The Storage Security Audit is a systematic, professional examination and verification of security and information management controls as applied in the storage infrastructure. It is performed by an independent party or internal audit function.

As a systematic test, the audit is performed against defined criteria, including, but not limited to ISO, ISACA[2], ITIL[3] and SNIA Storage Security Best Practices to determine adequacy and effectiveness of data security and data integrity procedures and whether activities and implementations conform to planned arrangements and whether these arrangements are implemented effectively to achieve the organizations security policy and objectives.

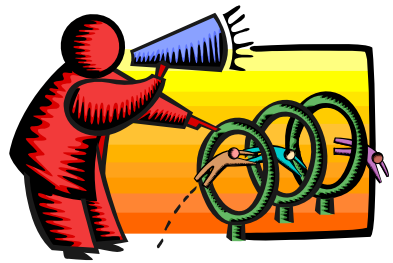
Upon completion, the auditor renders an opinion as to the effectiveness, consistency and conformity, based on evidence, and recommends necessary changes to storage activities and infrastructure.

[2] © Information Systems Audit and Control Association
[3] © IT Infrastructure Library

Storage Security Audit

Why audit storage security?

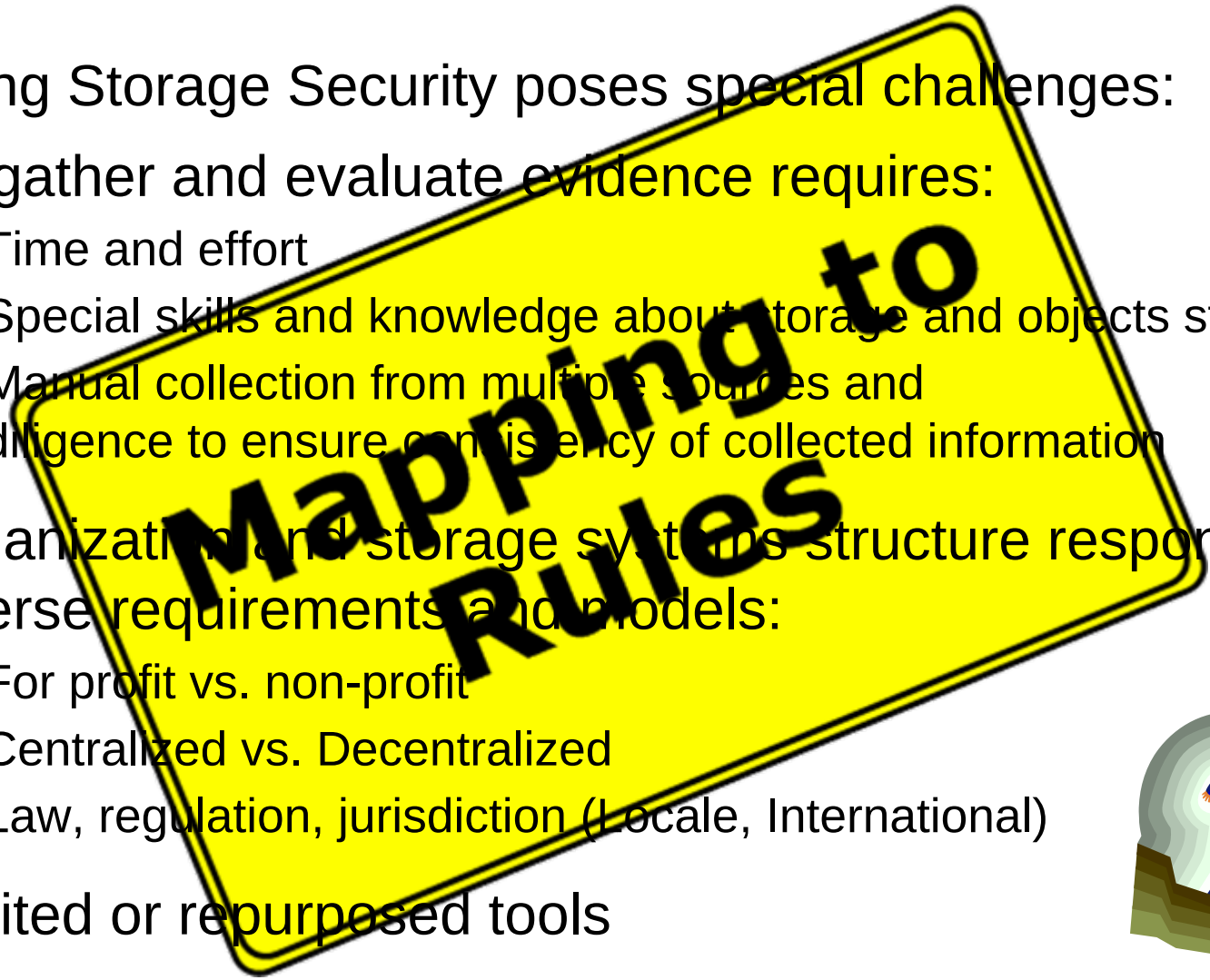
- To analyze storage configuration and controls to:
  - Identify security risks
  - Determine compliance with organization policy
  - Measure consistency with industry best practices
- To ensure configuration within IT security practices which:
  - Decrease costs
  - Improve efficiency
  - Reduce unscheduled business interruption
- To protect internal controls and reporting procedures
  - Sarbanes-Oxley, Section 404
  - European Union Data Protection Directive
  - Australia Communications Security Instructions



Special Challenges

Auditing Storage Security poses special challenges:

- To gather and evaluate evidence requires:
  - Time and effort
  - Special skills and knowledge about storage and objects stored
  - Manual collection from multiple sources and diligence to ensure consistency of collected information
- Organizational and storage systems structure respond to diverse requirements and models:
  - For profit vs. non-profit
  - Centralized vs. Decentralized
  - Law, regulation, jurisdiction (Locale, International)
- Limited or repurposed tools



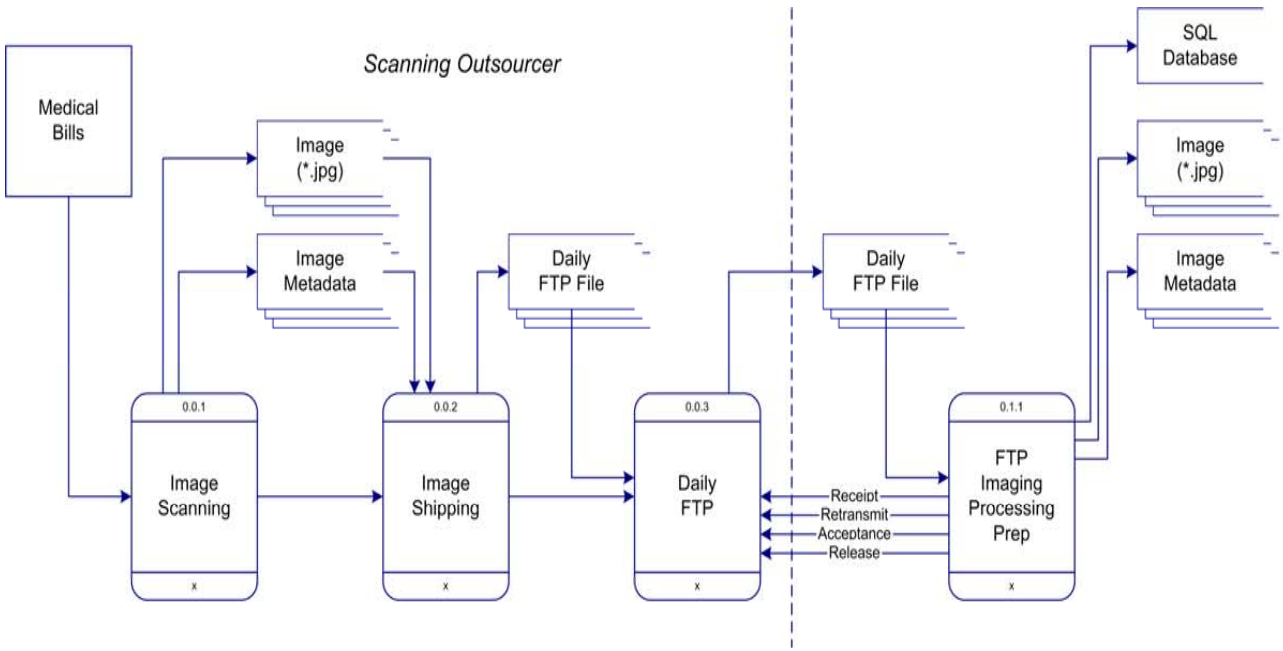
Introducing “the Client”

Insurance Company

- Actuarial
- Underwriting
  - Commercial
  - Personal
  - Property and Casualty
- Customer Service
  - A/R
  - Agency
  - Claims
  - Commercial Audit
  - Imaging
  - Policy Assembly
- Legal
- Loss Control
- Marketing
- Corporate Accounting
  - Commercial Services A/R
  - Agency Services A/R
  - Claims Services
  - Payroll
  - Taxes
- Portfolio (Investment)
- H/R
  - Training
  - Facilities
  - Pension
- Office Services
  - Email
  - Shared Services (file, print, network)

Claims Processing

Given an application workflow:



Data Parameters

- Medical Billing
- Image File Size 7-18k
- Image Metadata 512 or less
- 5 TB of images = 3 years
- Total Usable = 6 TB
- Growth rate = 5%/mo.
- Backup = 22 hours

SLA Parameters

- Avail = M-F 7:00 - 19:00
- RTO = 72 hours to hot site

Storage Security Audit Process

Process Overview

- Initiate the Audit Process
  - Charter
  - Staffing
- Storage Audit Planning
  - Select the type of Storage Audit
  - Detailed scoping
  - Set priorities by audit area
- Gather, test and review data by
  - Subject area
  - Audit area
- Communicate/Report

Initiate the Process

- Create an Audit Charter
  - Define Scope (including the storage subject area)
  - Set Objectives
  - Assign Responsibility
  - Delegate Authority to perform the audit
  - Reporting
- Select auditors who have:
  - Independence and adhere to professional ethics and standards
  - Knowledge about general audit techniques and storage specific audit techniques, demonstrating competence in:
    - Storing technologies and applications
    - Business continuance and disaster recovery
    - Legal and regulatory requirements
  - Skill with highly specialized tools
    - Scanners, Intrusion tests, Penetration tests

Storage Audit Planning[10%]

SNIA
Storage Networking Industry Association
EDUCATION

Business Environment

- Mission, Objectives, Purpose, and Processes

Business/IT Requirements

- Availability, Integrity, Security, and Technology

Contents to Review

- Policy, Standards, Guidelines and Procedures

Organization

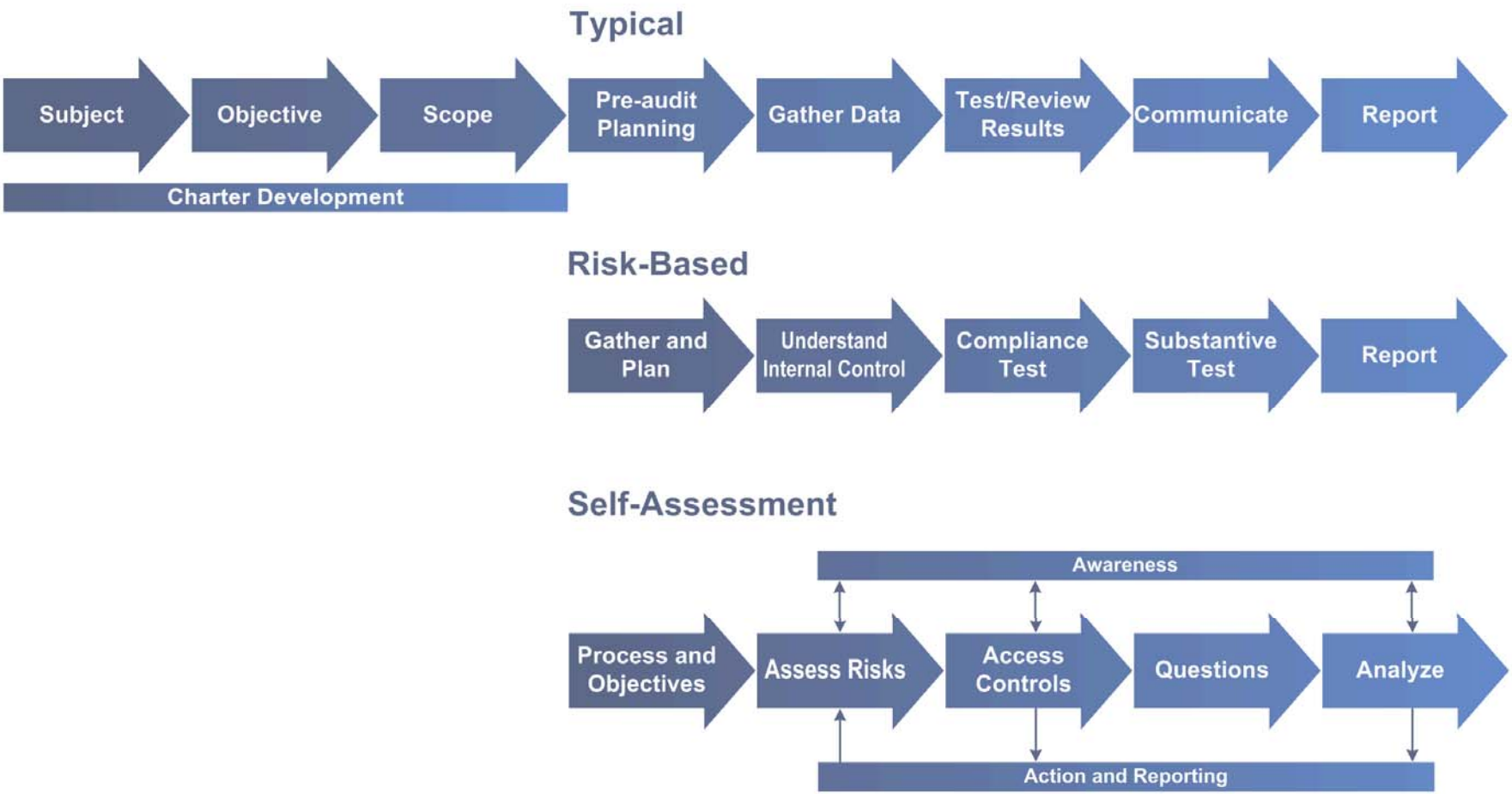
- Risk assessment
- Review internal controls
- Set audit scope

Select Audit Templates

- Operational
- Storage Components
  - By vendor
  - By infrastructure component/type
- Specialized
  - FFIEC (Federal Financial Institutions Examination)
  - ISO 17799/27001
  - PCI (Payment Card Industry)
  - SAS 70 (Statement of Auditing Standards)
    - Service organization description and test of control objectives and activities (outsource)
  - SAS 94 (Computer Assisted Auditing Techniques)
  - SEC17
- Forensic

10% reflects relative importance in audit process

Audit Type and Phases[2]

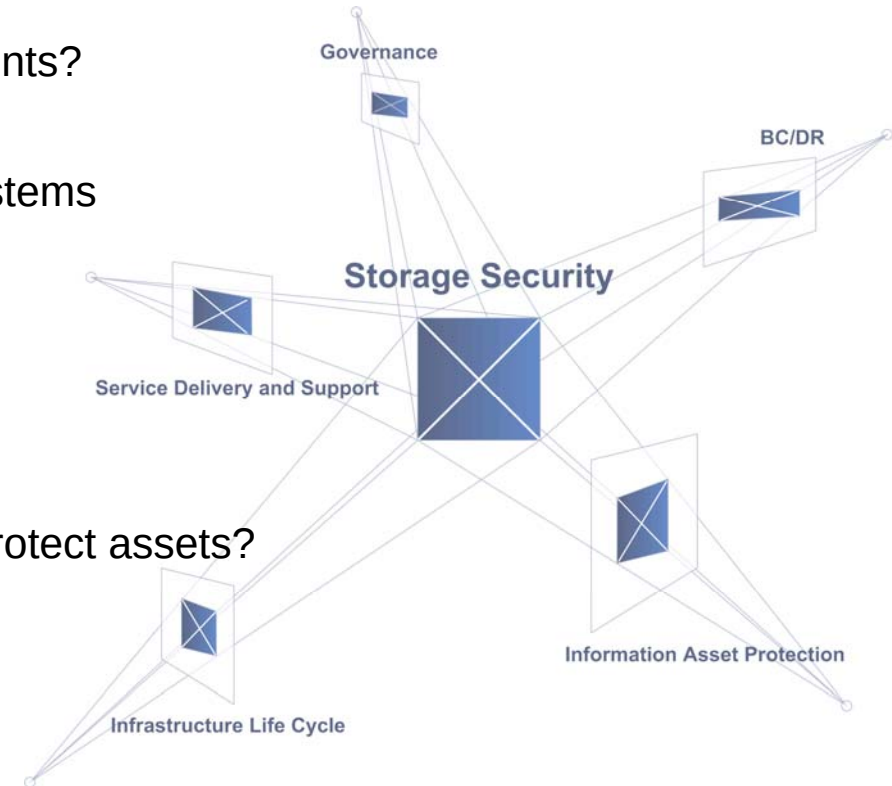


[2] General Sources: ISACA and ITIL

Audit Areas

The audit captures requirements, expected behavior and implementation as a series of perspectives.

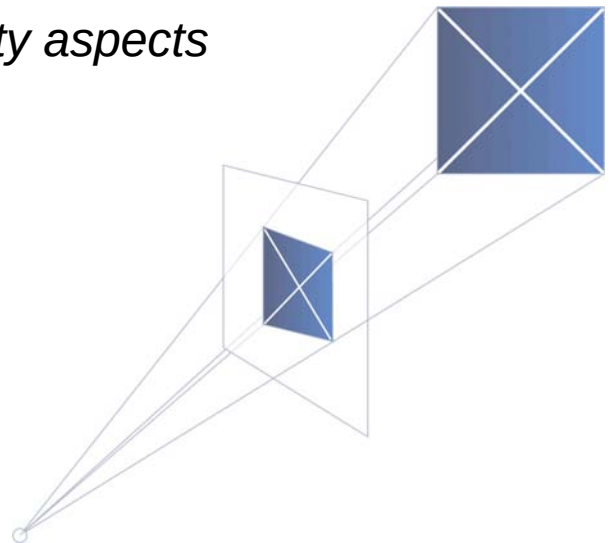
- Governance (15%)
  - What are the limits, laws and requirements?
- Infrastructure Lifecycle (16%)
  - Is storage security embedded in the systems development process?
- Service Delivery and Support (14%)
  - Is storage security part of the way people do their work?
- Information Asset Protection (31%)
  - Does current storage design properly protect assets?
- BC/DR (14%)
  - Is storage security built into BC/DR?



% reflects relative importance in audit process

Areas

focusing on their storage security aspects



Governance[15%]

Governance is both internal and external. Directors or others charged with the creation of wealth for all stakeholders must behave ethically in accordance with corporate governance. IT governance encompasses all stakeholders and seeks alignment of IT and enterprise objectives. An audit seeks evidence of IT alignment and governance in the internal control systems that monitor risk. For the storage subject area: it seeks the evidence in policies, procedures, risk management and control.

Strategic Alignment

- Information Security Policy
  - Balance Control / Productivity
  - Administration / Management
- Procedures include:
  - Segregation of duties
  - Storage security controls
- Risk Management

Embedding Accountability

- Access control, rights
  - Content
  - Configuration
  - Classification (sensitivity)
- Compensating Controls
  - Audit trail
  - Logging

15% reflects relative importance in audit process

Infrastructure Life Cycle[16%]

Infrastructure Life Cycle provides assurance that the management practices for development through disposal of systems and infrastructure will meet the organization's objectives. Within the portfolio, the storage class of components has become a stable, shared service with separate ownership and life cycle. The storage class has higher strategic importance than other classes. However, it has unique complexity and cost that is more visible. Poor storage security weakens the overall system. For the storage subject area: it seeks evidence that the storage components, policies and procedures will meet security requirements through their life cycle.

Is security designed in?

- Are controls in place?
- Is level of protection sufficient?
- What are the test plans?
- Re-evaluation of exposures during operational life? At change points?

Interesting areas…

- CIA, authentication, non-repudiation
- Certificate/registration authorities
- Encryption, key management
- Email security

16% reflects relative importance in audit process

Service Delivery and Support 14%

Service delivery and support provide assurance that the services will meet the organizations' objectives. Practices enable services. People perform the practices, which include storage security tasks. If the tasks are performed, the storage should be secure. Secure storage ensures stability of the information assets. Stable assets enhance value. For the storage subject area: an audit seeks evidence that the storage professional(s) follows the security policies and procedures in the course of their daily work.

- Segregation of duties
- Passwords
- Access accounting, Logging
- No evidence that data was altered in an unauthorized manner
- Vulnerabilities identified and resolved in a timely manner
- Detection of intrusion
- Regular security assessments
- Encryption
- Key management
- Media management
- Trans-border data flow
- Minimize data loss due to theft or maintenance
- Secure storage testing

14% reflects relative importance in audit process

Information Asset Protection[31%]

Information Asset Protection provides assurance that the security architecture (policies, standards, procedures and controls) ensures the confidentiality, integrity and availability of information assets. Evaluation of the current infrastructure design against models of control adequacy provides assurance. The model includes controls, processes used to store, retrieve, transport and dispose of information. For the storage subject area, the audit seeks to ensure that proper policies, procedures, controls (e.g. authentication, encryption, logging) have been engineered into the infrastructure.

Applicable Standards

- ISO17799/27001
- CobiT 4.0
- Legislation
- PCI DSS

A few areas…

- Implementation
- Data Classification, Value
- Access, Controls, Risk
- Penetration testing

31% reflects relative importance in audit process

BC/DR[14%]

Business Continuity and Disaster provides assurance that in the event of a business disruption, the business continuity and disaster recovery processes will ensure the timely resumption of IT services, minimizing the business impact. Using an ISO 27001/24762 approach, risk to availability is also a security risk. The process identifies risk scenarios, crisis levels and action plans. It also includes responses to non-storage threats that require storage services. For the storage subject area, the auditor will seek evidence that the storage infrastructure is able to provide an appropriate response to a variety of risk scenarios.

- Data protection (RAID)
- B/R (RTO/RPO)
- Depth of Retention
- Storage Maintenance
- Business Impact Analysis
- Security in Contractual agreements
- Channel extension
- Classification of systems
- Recovery strategies/alternatives
- Salvage

14% reflects relative importance in audit process

A word from our Sponsor

Storage Security Practices

SNIA Storage Security Industry Forum
SSIF

To help organizations address storage networking risks and compliance issues, the SNIA storage security activities (Security TWG and SSIG) have developed the Storage Security Best Current Practices found at: www.snia.org/ssif/documents

1. Secure storage management
2. Identify and assess all storage interfaces
3. Create risk domains
4. Monitor and control physical access
5. Avoid failures due to common mistakes
6. Address data security compliance
7. Protect externalized data
8. Understand the exposures
9. Implement appropriate service continuity
10. Utilize event logging

Summary

Conclusion

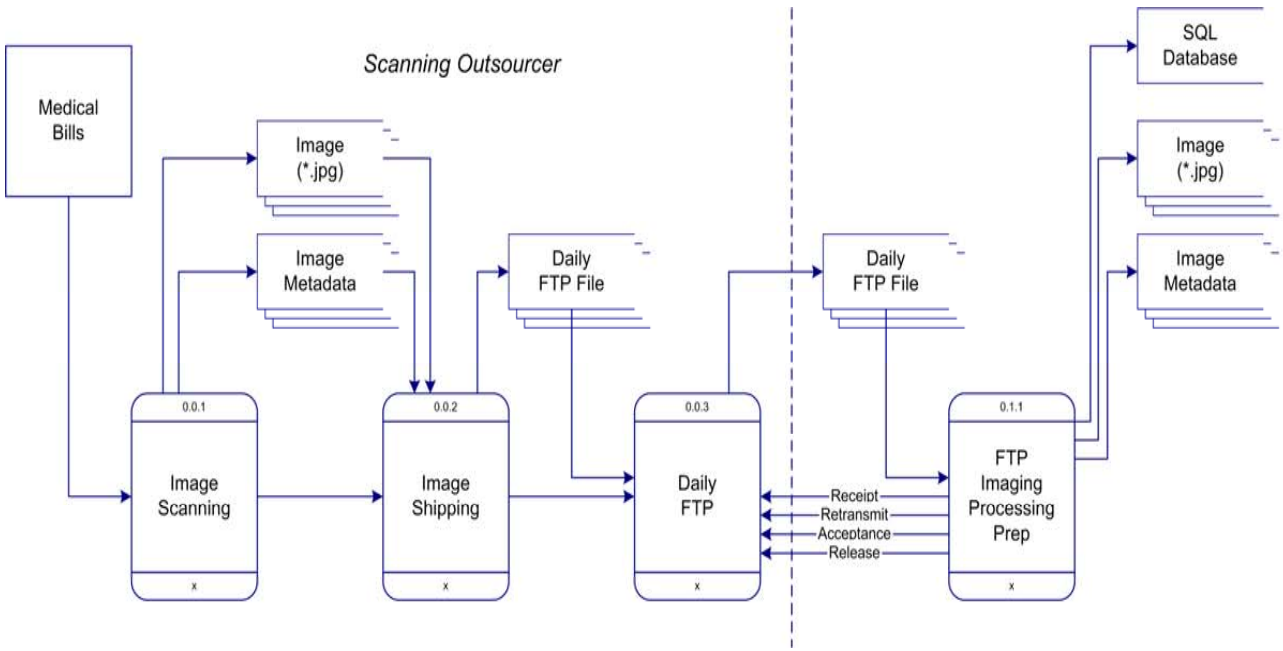
The process of moving to an operational approach that accepts security audits as an inevitable part of daily storage management will enable actions that mirror continuous self assessment of current security levels. It will also provide justification for new and validation of existing storage management practices.

Admittedly, in the absence of automated tools to address the needs of storage security auditors, at first, this will be difficult. However, it is yet another opportunity to improve storage security as we progress toward a model of secure storage.

Case Study

Claims Processing

Given an application workflow:



Data Parameters

- Medical Billing
- Image File Size 7-18k
- Image Metadata 512 or less
- 5 TB of images = 3 years
- Total Usable = 6 TB
- Growth rate = 5%/mo.
- Backup = 22 hours

SLA Parameters

- Avail = M-F 7:00 - 19:00
- RTO = 72 hours to hot site

Subject

Areas to be audited:

- Databases
- Network
- Servers
- Storage

Applications to be audited:

- All

Objectives

- Develop an storage security audit plan, reviewed annually, using risk assessment techniques, which identifies audits to be conducted each year; such audit plan shall be approved by BOD
- Conduct audits in the annual audit plan each year with documented deviations.
- Ascertain the adequacy of controls for safeguarding information assets at rest and in transit and, when appropriate, verifying the existence of information assets.
- Reduce cost
- Detect potential for fraud
- Reduce risks to availability
- …

Scope

Specific systems, function or unit of organization included in the review:

- Disk arrays
- Fabrics
  - Fibre Channel, IP
  - File (NAS)
- IP networks carrying storage traffic
- Backup, Archive and D/R
  - Tape
- Workflows
- Management infrastructure
- Servers associated with storage infrastructure

Pre-audit Planning

SNIA
Storage Networking Industry Association
EDUCATION

Technical Resources:

- O/S (Windows, Unix)
- Database (DB2, Oracle, SQL Server)
- Network (LAN, WAN)
- Storage (Array, Fabric, Backup, D/R)
- Application specific

Locations:

- Home office
- Scanning site (if not covered by SAS 70)
- D/R site

Sources:

- Input/Decision Matrix
  - People
  - Decision Style
- Documents
  - Design
  - Policy
  - Operations
- Applicable
  - Law
  - Regulation
- Systems, general and specific infrastructure

Gather Data - Policy

General documents

- Applicable law
- Workflow
  - Scan/Input
  - Modification/Revision
  - Retention
    - At scan site
    - At production site
- Access Controls
  - Process for gaining access
  - Audit logging
- Infrastructure tasks
  - Volume Management
  - File system management
  - LUN
  - Fabric

Storage infrastructure

- Process for gaining access
  - Current access documents
  - Current rights assignment
- Change control
- Compensating controls
- Replacement
  - Disk
  - Tape
  - Fabric components
  - Server
  - HBA
- B/R, D/R

Gather Data - Technical

- Location of hosts relative to firewall and fabric
- Configuration data
  - Hosts
  - Fabrics
  - Arrays
  - Libraries
  - Networks
  - Firewalls
  - ACLs

Gather Data
Secure Storage Management[3-1]

SNIA
Storage Networking Industry Association
EDUCATION

Misc.

- Is SSL/SSH in place at all management interfaces?
  - Telnet bypass? Off?
- Status of Telnet access?
- In-band storage management command?
  - Inhibition in-band commands?
- Method of authentication?
- Timeout?

Management Station

- Admin/password
- Hidden passwords for management application
  - Vendor
  - Underpinning database
- If tied to RADIUS?
  - Roles
  - Users assigned
  - Degree of administrative rights
- Administrative chain-of custody for original media
- Access to commands

Communicate

Exit interview:

- Use FC-SP switch authentication to reduce risks to availability caused by inappropriate fabric merge
- Use content level encryption when transmitting medical records from scan to production site
- Use link level encryption between production and D/R site
- Inhibit access for USB devices
- Activate and centralize logging
- Place active data destruction policy at scan side
- Modify backup and remote replication procedures

Report

- Follow-up review procedures:
  - Verify change of encryption pattern
- Test of controls:
  - Verify capture of log events, including security events
- Soundness of documents, policies and procedures:
  - Document if this criteria is met or areas for improvement

Q&A / Feedback

- Please send any questions or comments on this presentation to SNIA: tracksecurity@snia.org

Many thanks to the following individuals for their contributions to this tutorial.

SNIA Education Committee

Richard Austin
Eric Hibbard
Larry Hofer
Phil Huml