S21 - Auditing IT System Configurations

Nick Ali and Samuel Laine

September 21, 2009 – September 23, 2009

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Auditing IT System Configurations

September 21, 2009 – September 23, 2009

ISACA Serving IT Governance Professionals
San Francisco Chapter

Agenda

I. General Overview of Visa's IT Audit Approach
II. Standardization: Within the IT Audit Approach and the IT Environment
III. Approach for Standardizing the IT Environment
IV. Auditing Against Technical Security Requirements
V. Audit Exception Reporting Process
VI. Audit Issue Remediation Process

CONVERGEMERGE

ISACA Serving IT Governance Professionals
San Francisco Chapter

Section I

General Overview of Visa's IT Audit Approach

General Overview: Visa's IT Platform

- Visa's business model is very technology-oriented. A large and complex IT environment is maintained including the following platforms:
  - Distributed (UNIX, Windows)
  - Mainframe (zOS, TPF)
  - Network (Cisco routers, firewalls, switches etc)
  - Database (SQL, UDB, DB2 etc)
  - Workstations

General Overview: Visa's IT Audit Work Programs

- Visa's IT Audit System Configuration Work Programs usually consider the following high-level audit scope areas:
  - Governance
  - Access Management
  - System Management
  - Vulnerability Management
- Sub-scope areas are then defined based on the individual platform

Visa's IT Audit Work Program: Governance

- The following sub-scope areas comprise this section of the Work Program:
  - Management Reporting
  - Process and Procedure Documentation
  - Technical Security Requirements*
  - Replacement Materials Process (Anti-Fraud Control) (for those platforms where this is relevant)
  - Business Continuity Planning

*** This sub-scope area will be examined in more depth later in this presentation**

Sample High Level Test Approach: Distributed Platform - Governance

Sub-Scope Areas	Audit Objectives	Test Approach / High Level Test Plan
▪**Management Reporting**	▪Determine if a reporting process has been established to provide management with visibility into the status and security posture of the global systems infrastructure environment.	▪Inquire and examine documentation to evidence that a reporting process is in place to provide management with a perspective of the global systems infrastructure environment, including operational and security issues.
▪**Process and Procedure Documentation**	▪Determine if system management processes and procedures are formally documented and maintained.	▪Inquire and examine documentation to evidence that system management processes and procedures are formally documented and maintained.
▪**Technical Security Requirements**	▪Determine if a process has been established for maintaining Technical Security Requirements.	▪Inquire and examine documentation to evidence that a process has been established to maintain current Technical Security Requirements (TSR) and to determine if additional TSRs are required.
▪**Replacement Parts Management**	▪Determine if a process has been established to manage and track replacement system parts.	▪Inquire and examine documentation to evidence that a process has been established to manage and track replacement system parts. ▪**Fraud Considerations**: Inadequate controls in the replacement parts management process may lead to theft and misappropriation of replacement system parts.
▪**Business Continuity Planning**	▪Determine if procedures and resources to ensure continuity of the systems operations during a business interruption have been established.	▪Inquire and examine documentation to evidence that procedures and resources to ensure continuity of the system operations during a business interruption (geographical) have been established.

Visa's IT Audit Work Program: Access Management

- The following sub-scope areas comprise this section of the Work Program:
  - Privileged User Access Management (processes for additions, modifications and periodic review)
  - Logging and Monitoring of Privileged User Access

Note: Visa assesses general user access in various other audits

Sample High Level Test Approach: Distributed Platform - Access Management

Sub-Scope Areas	Audit Objectives	Test Approach / High Level Test Plan
▪**Privileged User Access Management**	▪Determine if a process for managing privileged user access to systems has been established.	▪Inquire and examine documentation to evidence that a process for managing privileged user access to systems has been established, including access creation, modification, and revalidation. ▪Select a sample of users with system administrator or other privileges and assess whether the access management process has been followed.
▪**Logging of Privileged User Activities**	▪Determine if audit trails of activities performed with privileged access are logged.	▪Inquire and examine documentation to evidence that a mechanism is in place to log privileged user activities, that sufficient information is recorded to establish accountability, and that logs are retained and safeguarded.

Visa's IT Audit Work Program: System Management

- The following sub-scope areas comprise this section of the Work Program:
  - Standard System Build
  - System Commissioning
  - System Decommissioning
  - Configuration Compliance with Technical Security Requirements*
  - System Inventory Management

*** This sub-scope area will be examined in more depth later in this presentation**

Sample High Level Test Approach: Distributed Platform - System Management

Sub-Scope Areas	Audit Objectives	Test Approach / High Level Test Plan
▪**Standard System Build**	▪Determine if a system build process has been established to standardize the systems infrastructure environment.	▪Inquire and examine documentation to evidence that a process has been established to standardize system builds, and that the builds are compliant with security requirements.
▪**System Commissioning**	▪Determine if systems are deployed into production following a standard system commissioning process.	▪Inquire and examine documentation to evidence that a standard process for deploying systems into production has been established. ▪Select a sample of systems and assess whether the production deployment process has been followed.
▪**System Decommissioning**	▪Determine if systems are removed from production following a standard system decommissioning process, including secure deletion of stored information and reclaim of software licenses.	▪Inquire and examine documentation to evidence that a standard process for removing systems from production has been established, and that the process includes steps for performing secure deletion of stored information. ▪Select a sample of systems and assess whether the system hard drives have been securely deleted and software licenses have been reclaimed.
▪**Configuration Compliance with Security Requirements**	▪Determine if a process to monitor compliance of system configurations with the Visa security requirements has been established.	▪Inquire and examine documentation to evidence that a process to monitor compliance of system configurations with the Visa security requirements has been established. ▪Select a sample of web servers and assess whether configurations are compliant with the security requirements.
▪**System Inventory Management**	▪Determine if an accurate inventory of production systems is maintained and includes information necessary to adequately support the systems infrastructure management processes.	▪Inquire and examine documentation to evidence that a process to maintain an inventory of production systems has been established. ▪Observe records maintained in the inventory and assess whether information necessary to adequately support the management of systems are present.

Visa's IT Audit Work Program: Vulnerability Management

- The following sub-scope areas comprise this section of the Work Program:
  - Patch and Version Management
  - Anti-Virus*
  - System Vulnerability Scanning*
  - Unauthorized Software*

* Several of these sub-scope areas are specific to the Distributed, Network and/or Workstation Platforms

Sample High Level Test Approach: Distributed Platform - Vulnerability Management

Sub-Scope Areas	Audit Objectives	Test Approach / High Level Test Plan
▪Patch Management	▪Determine if a patch management process has been established to identify, evaluate, and implement patches to ensure that known security weaknesses are addressed in a timely manner.	▪Inquire and examine documentation to evidence that a process to identify, evaluate, and implement system patches has been established. ▪Assess whether patches are evaluated and implement per policy.
▪Anti-Virus	▪Determine if anti-virus software is deployed on Windows servers, is actively running with the current virus definitions.	▪Inquire and examine documentation to evidence that a process has been established for deploying anti-virus software on Windows servers and ensuring that it is actively running with the current virus definitions. ▪Select a sample of Windows servers and assess whether an anti-virus software has been installed, and is actively running with the current virus definitions.
▪File Integrity Monitoring	▪Determine if a process to ensure the integrity of critical files has been established.	▪Inquire and examine documentation to evidence that a process has been established to ensure the integrity of critical system and application files.
▪System Vulnerability Scanning	▪Determine if system vulnerability scans are performed monthly and if identified vulnerabilities are addressed in a timely manner.	▪Inquire and examine documentation to evidence that a process to identify and mitigate security vulnerabilities within systems has been established.
▪Unauthorized Software	▪Determine if a process to detect and remove unauthorized software has been established.	▪Inquire and examine documentation to evidence that a process has been established to detect and remove unauthorized software.

Section II

Standardization: Within the IT Audit Approach and the IT Environment

Standardization: Within The IT Audit Approach

- Benefits
  - Maximizes efficiencies through “create once, use many” approach
  - Ensures a consistent approach applied by individual auditors, audit teams and across platforms, over time
- Challenges
  - Requires periodic re-evaluation to ensure latest emerging risks are identified and appropriately addressed

Standardization: Within The IT Environment

- Benefits
  - Lower costs
    - Reduces support costs & downtime
  - Easy to maintain
  - Facilitates integration between systems
  - Security concerns are mitigated
    - Timely remediation
    - Remote oversight
- Challenges
  - Establishing standards in global environment
  - Limitations of selected vendors
  - Requires Client Cooperation
    - Documenting standard configuration requirements
    - Commitment to build devices and maintain them against the standard configurations

Section III

Approach for Standardizing the IT Environment

Defining Standard Requirements

- Establish security requirements and policies
  - Technology Security Requirements (TSR's)
- What are TSR's?
  - TSR's are detailed guidelines containing specific measures (configuration settings and parameters) for securing individual technology platforms
- Why are they important?
  - Organization policies are usually too high level!
    - For example, an organization policy might require users to use strong passwords but may not specify actual password requirements such as upper/lower case etc.
  - TSR's provide consistent hardening requirements for engineering staff to follow when maintaining platforms

Implementing Standard Requirements

- Establish processes to enable initial and ongoing compliance with the TSR's and policies. These include:
  - TSR implementation process
    - Incorporate TSR settings into Device Build processes
    - Define a method for bringing all existing relevant devices in the environment into compliance
  - TSR monitoring and exception tracking process – method for maintaining ongoing compliance

Process for Defining TSR's

- Stakeholders whose input to the content of TSR's should include Systems Engineering, Operations, Security, Compliance, Risk Management, Application Business Owners, Chief Technology Office and Internal Audit organizations
- Consider industry standards such as:
  - ISO standards, PCI-DSS, NSA, CIS, NIST, DoD etc
- This process can be audited in the Governance section of the Audit Work Program

Typical Content of TSR's

- Introduction
  - Background, compliance requirements, audience, exception process etc
- Roles and Responsibilities
  - Responsible parties, Separation Of Duties requirements, baseline security practices
- Main body
  - Configuration requirements, specific security settings and parameters, and other recommendations.
- TSR's may also contain suggested attack prevention methods

Example: Windows Server TSR

- Example of the content for the Main Body content for a Windows Server TSR:

No.	Security Policy	Value	Win2000	Win2003	Win2008
3.1.1.1	Enforce Password History (Number of Passwords Remembered)		√	√	√
3.1.1.2	Maximum Password Age (Number of Days)		√	√	√
3.1.1.3	Minimum Password Age (Number of Days)	1	√	√	√
3.1.1.4	Minimum Password Length (Number of characters)	7	√	√	√
3.1.1.5	Password must meet complexity requirements. Password Complexity Definition: password must contain at least three of the following four character groups: • English uppercase characters (A through Z) • English lowercase characters (a through z) • Numerals (0 through 9) • Non-alphabetic characters (such as !, $, #, %) This setting is required for local user accounts. All other accounts will adhere to policy definitions set at the Active Directory level.	Enabled	√	√	√

***Values have been altered to protect Visa proprietary information.**

Implementing TSR's

- Implement processes in the system life cycle to incorporate TSR's:
  - Initial Commissioning
    - Build process
      - Should include a Checklist containing all TSR requirements
  - Major Changes to Existing Devices or Software
    - SDLC Methodology should include a checkpoint where TSR requirements are reviewed and confirmed as having been appropriately addressed
  - For Standard Day-to-Day Changes to Existing Devices or Software
    - Personnel who approve these changes should be closely familiar with the types of information in the TSR's for that platform

TSR Compliance Monitoring

- IT organization develops monitoring processes, and defines frequency of execution (real-time alerting is best practice!)
- Leverage industry tools to automate monitoring
  - Distributed: Sun O/S, AIX, Windows (ECM and ESM)
  - Network routers/switches: NetDoctor
  - Firewall: ADM and Skybox
- Configure tools to flag potential TSR violations
  - Example:
    - Passwords that do not meet complexity requirements
    - Generic userid's and passwords

TSR Exception Validation and Tracking

- IT organization develops a process to validate exception flags
  - Management must refine event triggers to provide relevant data
  - Manual process may be needed to weed out “false positive” results
- Tracking, escalation and remediation of exceptions
  - Clear audit trail should be maintained to demonstrate systemic approach to managing out-of-compliance settings

Section IV

Auditing Against TSR's

Auditing Against TSR's

- IA department should consider performing detailed testing to verify compliance with established TSR's
- Recommended Audit Approach:
  - Select a sample of devices or configurations that are appropriate for the audit objective or that comply with audit department sampling methodologies
  - Evaluate each device within the sample for compliance with TSR's

Auditing Against TSR's

- Step 1:
  - Select a sample of devices or configurations that are appropriate for the audit objective or that comply with audit department sampling methodologies
  - Sampling approach may be:
    - Random Sampling
      - e.g. Using a random number generator
    - Judgmental sampling
      - e.g. external facing devices, systems in core production zone

Auditing Against TSR's

- Step 2: Select review approach for evaluating compliance
  - Three common approaches can be used to verify TSR compliance:
    - Manual approach
    - Automated approach
    - Hybrid approach

Auditing Against TSR's

- Manual TSR Audit Approach comprises two actions:
  - Shoulder Surfing/Observation
  - Manual Review
    - Export configuration files into text files
    - Analysis of configuration outputs against TSR's configuration settings

Auditing Against TSR's

- Manual Approach
  - Benefits
    - Low cost
    - Easy to perform
    - Good for small environments/small populations
    - Easily Adaptable for TSR's updates
    - Less Intrusive
  - Challenges
    - Very time consuming
    - Not Scalable
    - Prone to inconsistency and errors
      - Human Error

Auditing Against TSR's

- Automated Approach
  - Leverage reporting from client-owned (Engineering group, etc); tools can be configured to report on TSR settings
  - Multiple Tools available in the Market
    - Features include
      - Trend Analysis
      - Real Time Scans
      - Scan on Demand
      - User friendly reporting
      - Automated Work-paper Management

Auditing Against TSR's

- Automated Approach
  - Benefits
    - Highly scalable
    - Management reporting
    - Provides recommended solution
    - Non Technical Staff can perform testing
  - Challenges
    - Expensive
    - Complexity of configuring tool based on companies environment
    - Highly intrusive
      - Performance impact
    - Require Vendor Support
    - Need to validate that results have integrity and have not been tampered with by clients

Auditing Against TSR's

- Hybrid Approach*
  - Combination of automated tools and manual analysis
    - Develop a script to pull TSR-related fields of system configuration
    - Setup testing matrix based on TSR
    - Document script results into testing matrix manually

* This approach is commonly deployed at Visa

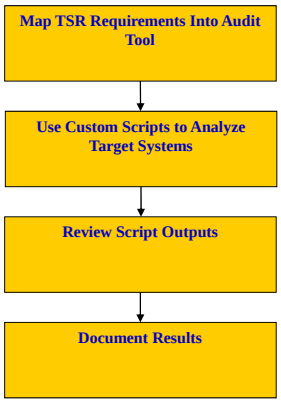
Auditing Against TSR's

- Hybrid Approach
  - Benefits
    - Scalable
    - Lower cost
    - Vendor support not required
  - Challenges
    - Creation of Custom Scripts
    - Intrusive to the production systems and network

Audit Approach Comparison

	Scalability	Complexity	Skill Set Required	Degree of Intrusiveness	Cost	Vendor Support
Manual Approach	Not Scalable	Lower Complexity	Experienced IT Auditor	Low	Low	Not Required
Automated Approach	Highly Scalable	Highly Complex to Setup	Non Technical Staff /IT Auditor	Highest	High Initial Cost	Required
Hybrid Approach	Scalable	Complex to Create Custom Scripts	Experienced IT Auditor	High	Low	Not Required

Hybrid Approach - Overview



Configuration Auditing: Hybrid Approach

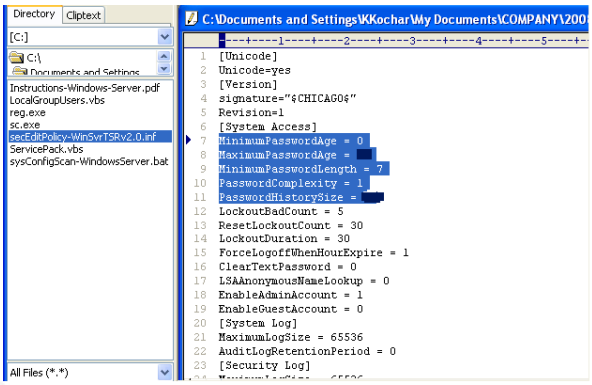
- Windows Server TSR Example

No.	Security Policy	Value	Win2000	Win2003	Win2008
3.1.1.1	Enforce Password History (Number of Passwords Remembered)		√	√	√
3.1.1.2	Maximum Password Age (Number of Days)		√	√	√
3.1.1.3	Minimum Password Age (Number of Days)	1	√	√	√
3.1.1.4	Minimum Password Length (Number of characters)	7	√	√	√
3.1.1.5	Password must meet complexity requirements. Password Complexity Definition: password must contain at least three of the following four character groups: • English uppercase characters (A through Z) • English lowercase characters (a through z) • Numerals (0 through 9) • Non-alphabetic characters (such as !, $, #, %) This setting is required for local user accounts. All other accounts will adhere to policy definitions set at the Active Directory level.	Enabled	√	√	√

*Values have been altered to protect Visa proprietary information

Configuration Auditing: Hybrid Approach

- Step 1 – Map TSR Requirements into Audit Tool:
  - For Windows, secedit tool is recommended



*Values have been altered to protect Visa proprietary information

Configuration Auditing: Hybrid Approach

- Step 2 – Use Custom Scripts to Analyze Target Systems:
  - Generate output for Internal Audit's review

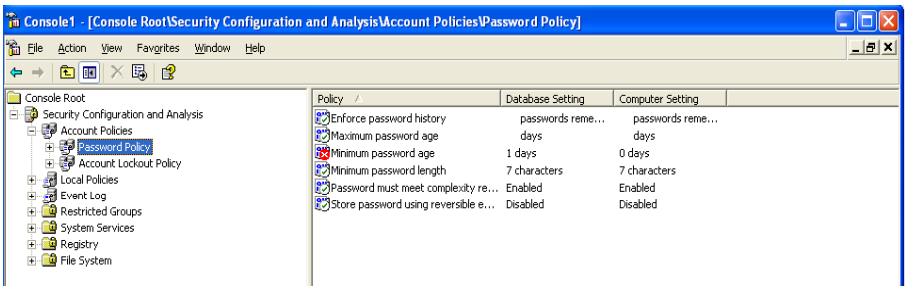
```
rem ----------------------------
rem   Begin System Config Scan
rem ----------------------------


echo Performing Windows server configuration scan using script version: %SCRIPT_VER%...

rem ----------------------------
rem   Gather SecEdit analysis
rem ----------------------------
secedit /analyze /db %RESULTS_PATH%\%COMPUTERNAME%-Secedit-Check.sdb /cfg %INF_FILE% /log %RESULTS_PATH%\%COMPUTERNAME%-Secedit-Check.log
secedit /export /mergedpolicy /cfg %RESULTS_PATH%\%COMPUTERNAME%-Secedit-Config.txt
```

Configuration Auditing: Hybrid Approach

- Step 3 – Review the Script output…
  - In our example, secedit presents the data in a GUI:



*Values have been altered to protect Visa proprietary information

Configuration Auditing: Hybrid Approach

- Step 4 – Document the script results within the Audit Work-paper

Test Case #	Control Objective	Reference		Windows Server 1 Notes/Exceptions	Windows Server 2 Notes/Exceptions
			General Information		
			Hostname		
			IP Address		
			Operating System		
			Location		
			Function		
			Date Tested		
			Client Representitive		
			Technology Security Requirement (TSR) Version		
User Management					
1.1	Password History is enforced	3.1.1.1	Enforce password history: XX passwords	Y	Y
1.2	Maximum password age is enforced	3.1.1.2	Max password age: XX days	Y	Y
1.3	Minimum password age is enforced	3.1.1.3	Min password age: 1 days	Y	Y
1.4	Minimum password lenght is enforced	3.1.1.4	Min password length: 7 characters	N - password length set to 4 character minimum	Y
1.5	Password complexity is enforced	3.1.1.5	Passwords must meet complexity requirements: Enabled Complexity Definition: password must contain at least three of the following four character groups: • English uppercase characters (A through Z) • English lowercase characters (a through z) • Numerals	Y	N - No requirement for upper and lowercase.

*Values have been altered to protect Visa proprietary information

Section V

Audit Exception Reporting Process

Exception Reporting Process

- Exceptions
  - Extract exceptions from testing matrices and other work program test results
  - Risk ranking the exceptions (High, Medium, Low, Improvement Suggestions)
- Audit Issue Memo and Audit Report
  - Individual audit issue memo is document and issued to responsible management
  - Audit report assesses collective impact of exceptions and is addressed to senior and executive management

Section VI

Audit Issue Remediation Process

Remediation Process

- Common Methods
  - Obtain samples of system configuration to evidence that remediation has occurred
    - Consider reviewing change tickets
    - Consider shoulder surfing to validate settings
  - Run the scripts on selected samples
  - Obtain certification or attestation from engineers that remediation has been implemented
    - This may be appropriate for lower-risk exceptions and where it is known that another audit will be scheduled in the near future.

Q & A