RSH CONSULTING

# RACF & Payment Card Industry (PCI) Data Security Standards

**RUGONE - May 2012**

Robert S. Hansel Lead RACF Consultant R.Hansel@rshconsulting.com 617-969-9050

# Robert S. Hansel

Robert S. Hansel is Lead RACF Specialist and founder of RSH Consulting, Inc., an IT security professional services firm he established in 1992 and dedicated to helping clients strengthen their IBM z/OS mainframe access controls by fully exploiting all the capabilities and latest innovations in RACF. He has worked with IBM mainframes since 1976 and in information systems security since 1981. Mr. Hansel began working with RACF in 1986 and has been a RACF administrator, manager, auditor, instructor, developer, and consultant. He has reviewed, implemented, and enhanced RACF controls for major insurance firms, financial institutions, utilities, payment card processors, universities, hospitals, and international retailers. Mr. Hansel is especially skilled at redesigning and refining large-scale implementations of RACF using role-based access control concepts. He has also created elaborate automated tools to assist clients with RACF administration, database merging, identity management, and quality assurance.

Contact and background information:


- 617-969-8211
- R.Hansel@rshconsulting.com
- www.linkedin.com/in/roberthansel
- www.rshconsulting.com

# PCI Security Standards Council

- Launched in 2006
- Responsible for the development, management, education, and awareness of the PCI Security Standards, including …
  - Data Security Standard (PCI DSS)
  - Payment Application Data Security Standard (PA-DSS)
  - PIN Transaction Security (PTS)
- Founded by five global payment brands -- American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.
  - All five payment brands share equally in the Council's governance and review proposed additions and modifications to the standards
  - Each brand has agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs
  - Each brand recognizes the Qualified Security Assessors (QSAs), PA-QSAs, and Approved Scanning Vendors (ASVs) certified by the Council
- Enforcement of compliance with the PCI DSS and determination of any non-compliance penalties are carried out by the individual payment brands and not by the Council

# PCI DSS

- Developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally
- Provides a baseline of technical and operational requirements designed to protect cardholder data
- Applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers
- Comprised of a minimum set of requirements for protecting cardholder data
  - 12 major requirements
  - 200+ sub-requirements
- Current version: 2.0 October 2010

# PCI DSS Requirements

- **Build and Maintain a Secure Network**
  - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
  - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- **Protect Cardholder Data**
  - Requirement 3: Protect stored cardholder data
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks
- **Maintain a Vulnerability Management Program**
  - Requirement 5: Use and regularly update anti-virus software or programs
  - Requirement 6: Develop and maintain secure systems and applications
- **Implement Strong Access Control Measures**
  - Requirement 7: Restrict access to cardholder data by business need-to-know
  - Requirement 8: Assign a unique ID to each person with computer access
  - Requirement 9: Restrict physical access to cardholder data
- **Regularly Monitor and Test Networks**
  - Requirement 10: Track and monitor all access to network resources and cardholder data
  - Requirement 11: Regularly test security systems and processes
- **Maintain an Information Security Policy**
  - Requirement 12: Maintain a policy that addresses information security for all personnel
- **Additional PCI DSS Requirements for Shared Hosting Providers**
  - Requirement A.1: Shared hosting providers protect cardholder data environment

# PCI DSS Applicability

- Applies when the Primary Account Number (PAN) is stored, processed, or transmitted

- Applies to all system components that are included in or connected to the "cardholder data environment"
  - Cardholder data environment is comprised of people, processes, and technology that handle cardholder data or sensitive authentication data
  - System components include network devices, servers, and applications

- PCI DSS encourages "network segmentation" to limit and isolate the system components involved in handling PAN data from the rest of the entity's network
  - Intended to simplify implementation of controls
  - Reduces cost of compliance
  - z/OS Segmentation
    - Separate zSeries system, Sysplex, LPAR, z/VM machine, DASD configuration
    - Open System Adapter (OSA) configuration, TCP/IP configuration, Policy Agent configuration

# PCI DSS Compliance Process

- Determine what system components are involved in processing PAN data and fall within the scope of PCI DSS requirements
  - Diagram the flow of PAN data within the cardholder data environment
- Assess PCI DSS compliance of the system components
  - Self-Assessment Questionnaire (SAQ)
  - Qualified Security Assessor (QSA)
  - Approved Scanning Vendor (ASV)
  - Document compensating controls
- Reporting - depends on card brand requirements
  - Copy of SAQ and/or attestation of compliance
  - Quarterly scanning results
  - Report on Compliance (ROC)
    - Formal, detailed report - prepared by QSA
    - Description of cardholder data environment and system components
    - Findings and observations

# Requirement 1: Install and maintain a firewall configuration to protect cardholder data

**1.3** Prohibit direct public access between the Internet and any system component in the cardholder data environment.

**1.3.2** Limit inbound Internet traffic to IP addresses within the DMZ.

**1.3.5** Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.

# Requirement 1: Install and maintain a firewall configuration to protect cardholder data

- Implement SERVAUTH EZB.NETACCESS.*sysname*.TCPIP.*safname* profiles and permit access only to internal IP addresses
- Implement NODES profiles to allow inbound jobs only from authorized nodes
  - Define *.USERJ.* UACC(NONE)
- Ensure RACFVARS profile &RACLNDE members only include local NJE nodes
- Define JESINPUT profiles and limit access to NJE and RJE input sources to appropriate users
- Define WRITER profiles and limit access to outbound NJE and RJE destinations to appropriate users

# Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

**2.1** Always change vendor-supplied defaults **before** installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.

**2.2** Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.

**2.2.3** Configure system security parameters to prevent misuse.

# Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

- Change RVARY passwords
- Change IBMUSER password
- Set SETROPTS Options
  - NOADSP
  - NOMODEL
  - Others per later requirements

# Requirement 3: Protect stored cardholder data

**3.1** Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes, as follows.

**3.1.1** Implement a data retention and disposal policy that includes:

- Processes for secure deletion of data when no longer needed

# Requirement 3: Protect stored cardholder data

- Activate SETROPTS ERASE(ALL or NOSECLEVEL)
- If ERASE(NOSECLEVEL), set ERASE on DATASET profiles guarding PCI data

# Requirement 6: Develop and maintain secure systems and applications

**6.2** Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.

- Subscribe to "z/OS Security Alerts" via IBM My notifications.

# Requirement 7: Restrict access to data by business need-to-know

**7.1** Limit access to computing resources and cardholder information to only those individuals whose job requires such access.

**7.1.1** Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities

**7.1.2** Assignment of privileges is based on individual personnel's job classification and function

**7.1.4** Implementation of an automated access control system

# Requirement 7: Restrict access to data by business need-to-know

- Block access by users with OPERATIONS authority to PCI data
- Use Storage Admin privileges instead of OPERATIONS authority (DASDVOL, FACILITY STGADMIN.ADR.STGADMIN profiles) and strictly limit access
- Do not assign PRIVILEGED authority to any Started Task
- Assign TRUSTED authority to Started Tasks where recommended by IBM
- Define FACILITY BPX.DAEMON and PROGRAM ** profile with appropriate program libraries
- Permit access to BPX.DAEMON and BPX.SERVER only to system tasks requiring it
- Assign UID(0) only to system tasks requiring it
- Permit access to BPX.SUPERUSER only to system tasks requiring it (subsitute for UID(0) where possible) and to staff responsible for Unix administration
- Use UNIXPRIV profiles to grant replace Unix Superuser authority
- Permit ALTER access to discrete profiles only when required
- Implement RBAC group access control architecture

# Requirement 7: Restrict access to data by business need-to-know

**7.2** Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

- **7.2.1** Coverage of all system components
- **7.2.2** Assignment of privileges to individuals based on job classification and function
- **7.2.3** Default "deny-all" setting

# Requirement 7: Restrict access to data by business need-to-know

- Activate SETROPTS options
  - PROTECTALL(FAILURES)
  - TAPEDSN [ or PARMLIB(DEVSUPnn) or CA-1 Options equivalents ]
  - WHEN(PROGRAM)
  - CLASSACT(all applicable classes) [ minimally DATASET and TEMPDSN ]
  - RACLIST(all active classes with RACLIST(REQUIRED) classes)
  - NOADDCREATOR
- Restrict UPDATE access to system and APF-authorized datasets to users responsible for z/OS system maintenance
- Implement FACILITY CSV-prefixed profiles to protect and restrict dynamic system configuration changes and restrict access to users responsible for z/OS system maintenance
- Create profiles to protect BLP and tape security bypass authority and restrict access to users with a management justified need for this authority
- Implement OPERCMDS profiles to protect system commands

# Requirement 7: Restrict access to data by business need-to-know

- Implement FACILITY GIM.-prefixed profiles to protect SMPE functions and restrict access to users responsible for z/OS system maintenance
- Define installation classes with DEFAULTUACC(NONE), DEFAULTRC(8), and OPERATIONS(NO)
- Connect users to groups with CONNECT UACC(NONE)
- Remove WARNING from all profiles protecting operating system and PCI datasets and resources
- Do not create Global Access Table entries that undermine dataset and general resource profile protections
- Set UACC(NONE) on all profiles protecting PCI datasets and resources and do not permit access to ID(*)
- Define a catchall of *hlq*.** UACC(NONE) for all High Level Qualifiers associated with PCI datasets
- Create catchall ** profiles in all classes with UACC(NONE)
  - Exclude PROGRAM, FACILITY, and UNIXPRIV

# Requirement 8: Assign a unique ID to each person with computer access

**8.1** Assign all users a unique ID before allowing them to access system components or cardholder data.

**8.4** Render all passwords unreadable during transmission and storage on all system components using strong cryptography.

**8.5** Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows:

- **8.5.1** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
- **8.5.3** Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.
- **8.5.5** Remove/disable inactive user accounts at least every 90 days.
- **8.5.6** Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.
- **8.5.8** Do not use group, shared, or generic accounts and passwords, or other authentication methods.

# Requirement 8: Assign a unique ID to each person with computer access

- If the password encryption exit ICHDEX01 is present, ensure it does not enable password encryption using IBM's proprietary algorithm, and instead either allows or requires use of DES encryption
- Assign SPECIAL only to security staff responsible for RACF administration
- Assign CLAUTH(USER) only to staff responsible for user ID creation
- Permit FIELD class profile UPDATE access only to appropriate users
- Limit access to FACILITY IRR.PASSWORD.RESET and IRR.PWRESET.-prefixed profiles to users responsible for password resets within their domain
- Restrict READ access to TSOAUTH ACCT and UPDATE access to SYS1.UADS to staff responsible for maintaining TSO
- Do not use NOEXPIRE when resetting user passwords
- Activate SETROPTS INITSTATS and INACTIVE(90 or less) or implement a substitute automated process for identifying and deactivating stale IDs
- Set UAUDIT and REVOKE(date) on vendor accounts
- Do not use FACILITY BPX.DEFAULT.USER shared UID

# Requirement 8: Assign a unique ID to each person with computer access

**8.5** Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows: (continued)

**8.5.9** Change user passwords at least every 90 days.

**8.5.10** Require a minimum password length of at least seven characters.

**8.5.11** Use passwords containing both numeric and alphabetic characters.

**8.5.12** Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.

**8.5.13** Limit repeated access attempts by locking out the user ID after not more than six attempts.

**8.5.15** If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

**8.5.16** Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.

# Requirement 8: Assign a unique ID to each person with computer access

- Activate SETROPTS options
  - INITSTATS
  - PASSWORD(INTERVAL(90 or less))
  - PASSWORD(RULE1(LENGTH(7:8 or 8))
  - PASSWORD(RULE1(ALPHANUM(1:8))
  - PASSWORD(HISTORY(4 or more)).
  - PASSWORD(REVOKE(6 or less)).
- Create a CICS Segment for the CICS Default User, named in the DFLTUSER parameter of the CICS Systems Initialization Table (SIT), and specify TIMEOUT(15) and also specify TIMEOUT(15) in the CICS Segments defined for any individual users; may substitute session locks via other software (e.g., VTAM Session Manager options)
- Activate SETROPTS JES(BATCHALLRACF) and JES(XBMALLRACF)

# Requirement 10: Track and monitor all access to network resources and cardholder data

**10.2** Implement automated audit trails for all system components to reconstruct the following events:

- **10.2.2** All actions taken by any individual with root or administrative privileges
- **10.2.3** Access to all audit trails
- **10.2.4** Invalid logical access attempts
- **10.2 5** Use of identification and authentication mechanisms
- **10.2.6** Initialization of the audit logs
- **10.2.7** Creation and deletion of system-level objects

# Requirement 10: Track and monitor all access to network resources and cardholder data

- Set UAUDIT on all non-process users with SPECIAL, OPERATIONS, or UID(0)
- Specify AUDIT(ALL) on all UNIXPRIV class SUPERUSER-prefixed profiles
- Set AUDIT(ALL) on FACILITY class profile BPX.SUPERUSER
- Activate SETROPTS options
  - AUDIT(DATASET FSOBJ IPCOBJ & all other classes)
  - SAUDIT
  - OPERAUDIT
  - CMDVIOL
  - APPLAUDIT
  - LOGOPTIONS(ALWAYS(FSSEC))
  - LOGOPTIONS(FAILURES(all classes)), except for those classes activated for ALWAYS
- Assign AUDITOR only to staff responsible for RACF monitoring and oversight
- If PCI data resides in the z/OS Unix Hierarchical File System, do not define FACILITY class profile BPX.SAFFASTPATH

# Requirement 10: Track and monitor all access to network resources and cardholder data

- Set AUDIT(ALL) on DATASET profiles protecting SMF datasets as well as all archives and backup copies of the same
- Activate the LOGSTRM class and define profiles to protect access to log streams with AUDIT(ALL)
  - Access permitted only to those process IDs that need to write to the log streams
- Set AUDIT(ALL) on DATASET profiles protecting all copies of system console logs
- Ensure installation-written logon routines using RACROUTE REQUEST=VERIFY do not specify parameter LOG=NONE
- Minimally set AUDIT(FAILURES(READ)) on all profiles not covered by more stringent requirements

# Requirement 10: Track and monitor all access to network resources and cardholder data

**10.5** Secure audit trails so they cannot be altered.

**10.5.1** Limit viewing of audit trails to those with a job-related need.

**10.5.2** Protect audit trail files from unauthorized modifications.

**10.7** Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).

# Requirement 10: Track and monitor all access to network resources and cardholder data

- Define DATASET profiles to protect all datasets written to by SMF as well as all archives and backup copies of the same
  - Define with UACC(NONE) and no access permitted to ID(*)
  - Access permitted only to those users who are responsible for monitoring the functioning of the system and for security
- Define DATASET profiles to protect log stream datasets as well as all archives and backup copies of the same
  - Define with UACC(NONE) and no access permitted to ID(*)
  - Access permitted only to those users who are responsible for monitoring the functioning of the system and for security
- Define DATASET profiles to protect all copies of system console messages with UACC(NONE) and no access permitted to ID(*)

# Requirement 11: Regularly test security systems and processes

**11.2** Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

**11.2.1** Perform quarterly internal vulnerability scans.

**11.2.3** Perform internal and external scans after any significant change.

**11.5** Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

# Requirement 11: Regularly test security systems and processes.

- Execute RACF-related z/OS HealthChecker checks
  - Define XFACILIT HZS-prefixed profiles to control the activation and execution of RACF-related z/OS HealthChecker checks
    - Define with UACC(NONE) and no access permitted to ID(*)
    - Permit access only to those users responsible for managing the z/OS operating system and for security
- Implement program signature verification for operating system programs and programs processing PCI data

# References

- PCI Security Standards Council www.pcisecuritystandards.org
  - PCI DSS standards and related documents

- Card Brand Requirements
  - American Express: www.americanexpress.com/datasecurity
  - Discover Financial Services: www.discovernetwork.com/fraudsecurity/disc.html
  - JCB International: www.jcb-global.com/english/pci/index.html
  - MasterCard Worldwide: www.mastercard.com/sdp
  - Visa Inc: www.visa.com/cisp
  - Visa Europe: www.visaeurope.com/ais

- @sec www.atsec.com
  - Payment Card Industry Compliance For Large Computing Systems, July 12, 2010