PCI DSS (White Paper)

Achieving PCI DSS Compliance with Vanguard Integrity Professionals Software & Professional Services

Vanguard is the industry leader in z/OS Mainframe Software to ensure enterprise compliance with the PCI DSS standard (Payment Card Industry – Data Security Standard)

IT ISN'T JUST RETAILERS THAT SUFFER PAYMENT CARD DATA BREACHES, GOVERNMENT AGENCIES ARE SUSPECTIBLE AS WELL

MOST CREDIT CARD TRANSACTIONS TODAY ARE STILL PROCESSED ON MAINFRAMES, IS YOURS PCI DSS COMPLIANT?

Contrary to popular misconceptions about their obsolescence, mainframes today still process over 30 billion business transactions per day, including the vast majority of major credit card transactions. Is your mainframe PCI DSS compliant?

WHAT ARE THE COSTS AND CONSEQUENCES OF PCI DSS NONCOMPLIANCE?

Noncompliance Fines

The consequences of not being PCI DSS
Compliant can be as high as $500,000 USD per year, levied by the banks and credit card institutions. Banks may fine based on forensic research they must perform to remediate noncompliance.

Breach Consequences

Even if a company is 100% PCI compliant and validated, a breach in cardholder data may still occur. Cardholder Breaches can result in the following losses for a organization.

- $50-$90 fine per cardholder data compromised
- Suspension of credit card acceptance by a merchant's credit card account provider
- Loss of reputation with customers, suppliers, and partners
- Possible civil litigation from breached customers
- Loss of customer trust which effects future sales

Whom should you trust to help your agency meet PCI DSS Compliance requirements?

RELY ON WHOM THE TOP RETAILERS, INSURERS, FINANCIAL FIRMS AS WELL AS FEDERAL AND STATE GOVERNMENT AGENCIES TRUST WITH THEIR PCI COMPLIANCE: VANGUARD INTEGRITY PROFESSIONALS

Almost half of the Fortune 1000 and many governmental agencies around the world rely on Vanguard's Software solutions and consulting services to ensure their compliance

VANGUARD'S SOFTWARE FOR PCI DSS

Let's look at the 12 requirements of the PCI DSS Standard in more detail, and explore how Vanguard's Software can help your organization achieve compliance more quickly and capably than z/OS and RACF alone.

1. Install and maintain a firewall configuration to protect cardholder data.

The z/OS firewall is controlled by the TCP/IP (PROFILE) member for each TCP/IP Stack and related general resource profiles in the SERVAUTH class. VANGUARD ACTIVE ALERTS can provide you with real time notifications of z/OS firewall security events while VANGUARD ENFORCER can detect changes that might compromise security.

2. Do not use vendor supplied defaults for system passwords and other security parameters.

The PCI DSS mandate stipulates: 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.

Sources of industry accepted system hardening may include, but are not limited to:

- Center for Internet Security (CIS)
- International Organization for Standardization (ISO)
- SysAdmin Audit Network Security (SANS) Institute
- National Institute of Standards Technology (NIST)

NIST tends to be the Gold Standard for achieving system hardening. VANGUARD CONFIGURATION MANAGER ensures your mainframe is hardened according to the NIST checklist requirements. Many of the other aforementioned authorities like CIS refer to the NIST checklist.

Protect Cardholder Data

3. Protect stored cardholder data.

RACF and z/OS cryptographic services are very powerful and if properly configured and maintained provide very strong protection for sensitive customer data.

VANGUARD ADMINISTRATOR enables quick analysis of RACF users, groups and permissions and can ensure least privilege access is achieved and maintained. VANGUARD POLICY MANAGER AND VANGUARD ENFORCER can be used to lock in a compliant configuration while VANGUARD ACTIVE ALERTS can trigger real-time notifications of
suspected attacks on cardholder data.

Maintain a Vulnerability Management Program

4. Use and regularly update anti-virus software.

While mainframes are not generally afflicted by the types of malware that this requirement is intended to cover, it's worth noting that malicious code can be created and deployed on any system including System z. It's therefore worth ensuring that your controls over sensitive libraries such as Authorized Program Facility (APF) libraries are adequate. VANGUARD ANALYZER quickly analyses sensitive libraries and VANGUARD ENFORCER AND VANGUARD CONFIGURATION MANAGER are ideal for detecting unauthorized system configuration changes.

5. Develop and maintain secure systems and applications.

Again, malware common in traditional distributed systems does not afflict System z but this section of the standard also discusses proper separation of environments and reviews against known vulnerabilities. VANGUARD ADMINISTRATOR, VANGUARD ANALYZER AND VANGUARD ADVISOR can help by facilitating a robust permissions regime such as Role-Based Access Control (RBAC) that includes separation of Production and Development systems.
VANGUARD ADVISOR also provides simple Audit reports covering common System z weaknesses and misconfigurations. VANGUARD ADMINISTRATOR will help us to fix these errors while VANGUARD POLICY MANAGER will prevent "drift" and, again, VANGUARD ACTIVE ALERTS can notify of potential breaches.

Implement Strong Access Control Measures

6. Restrict access to cardholder data by business need to know.

Again, a robust, least privilege, role based access control regime is called for and VANGUARD ADMINISTRATOR, VANGUARD ADVISOR AND VANGUARD ANALYZER help massively with its implementation. VANGUARD POLICY MANAGER can then ensure that Users/Groups do not inadvertently get added to sensitive datasets/profiles.

Limiting access to only those that need it without impacting legitimate users or causing service outages is very difficult without VANGUARD because what usage data organizations have is scattered throughout months worth of huge SMF dumps. (And may be incomplete in any case)

VANGUARD CLEANUP AND VANGUARD OFFLINE make this simple and safe to delete swaths of unused permissions. Turn on VANGUARD CLEANUP to capture access information and return in a few months to use VANGUARD OFFLINE to verify proposed changes before changing the RACF database; leaving only those permissions in regular use to review for appropriateness.

7. Identify and Authenticate access to system components.

RACF enforces sign on with user and password but preventing password sharing is tricky. VANGUARD ADMINISTRATOR provides for scheduled enabling and disabling of users or permissions to prevent privileged accounts being misused. VANGUARD ADVISOR allows sophisticated reports to be generated to detect unusual account usage patterns that might indicate password sharing and unauthorized access. VANGUARD ENFORCER can be configured to prevent users from escalating their own privileges and VANGUARD ACTIVE ALERTS can, again, notify key personnel of suspicious activity by e-mail, SMS, or an operator console message.

Regularly Monitor and Test Networks

8. Track and monitor all access to network resources and Cardholder data.

VANGUARD offers VANGUARD AUTHENTICATOR which authenticates users via RACF to access internal systems.

9. Regularly test security systems and processes.

This requirement includes directions to run vulnerability scans regularly and to detect changes to critical system files. Traditionally this is a complicated business on System z but with VANGUARD CONFIGURATION MANAGER it's a snap. Vanguard Configuration Manager checks and reports on hundreds of thousands of control points automatically to provide a level of security review that is virtually impossible using manual methods.

Maintain an Information Security Policy

10. Maintain a policy that addresses information security.

VANGUARD ENFORCER and VANGUARD POLICY MANAGER will help you maintain your security policy and prevent changes that would violate your security policy.

Two Factor Authentication

11. Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all 3rd parties. (PCI 8.3)

VANGUARD offers two multifactor solutions to meet this requirement, VANGUARD ez/Token and VANGUARD TOKENLESS AUTHENTICATION. VANGUARD's ez/Token solution provides a more secure alternative than the usual RACF user ID/password combination. With VANGUARD ez/Token, users substitute a new, one-time passcode in place of a password. Passcodes are generated randomly every 60 seconds. For enhanced security, the passcode can be combined with a PIN number.

VANGUARD TOKENLESS AUTHENTICATION authenticates users by their passwords (something they know) combined with a passcode sent to their personal communication device of choice (something they have).

Encryption

11. Implement additional security features for any required services, protocols or daemons that are considered to be insecure-for example use SSH, S-FTP, TLS or IPSec VPN to protect unsecure services such as NetBIOS, file sharing, telnet, FTP, etc.

VANGUARD ADVISOR is a superb tool to assist in evaluating your compliance with PCI DSS requirements for encryption.

The Payment Card Industry Data Security Standard (PCI DSS) applies to any organization that collects, stores, processes or transmits credit card holder data, or interacts with any third party company that does. VANGUARD leads in helping organizations utilizing z/OS mainframes attain and maintain PCI DSS Compliance.

VANGUARD PROFESSIONAL SERVICES FOR PCI DSS COMPLIANCE

Vanguard Integrity Professionals provides a wide range of enterprise security services that can help ensure PCI DSS Compliance.
Vanguard's Professional Services team can conduct penetration testing to detect system weaknesses and exposures, security assessments to identify vulnerabilities and prioritize risk, as well as remediation services to bring systems into compliance.

WHY VANGUARD?

Vanguard offers the most advanced and integrated portfolio of enterprise security products and services in the world. The portfolio was the first to offer a fully automated baseline configuration scanner for mainframe DISA STIGs – the Gold Standard for Security.

FOR MORE INFORMATION

To learn more about Vanguard Security Solutions, please contact Vanguard Integrity Professionals at (702) 794. 0014 or visit www.go2vanguard.com

The World's largest Financial, Insurance, Government Agencies and Retailers entrust their Security to Vanguard Integrity Professionals.

Corporate Headquarters

Vanguard Integrity Professionals

6625 S. Eastern Avenue – Suite 100

Las Vegas, NV 89119-3930

Telephone: 702.794.0014 Fax: 702.794.0023