PCI Security Standards Council™

PAYMENT CARD INDUSTRY DSS

COMPLIANCE STANDARD

osirium.com

OSIRIUM

HOW OSIRIUM HELPS ADDRESS

PCI DSS COMPLIANCE

PCI Security Standards Council™

INTRODUCTION

The Payment Card Industry Data Security Standard (PCI DSS)[1] is a worldwide information security standard defined by the Payment Card Industry Security Standards Council including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International.

The standard was created for organisations that process card payments to help prevent credit card fraud through increased controls around data and its potential exposure to compromise. The PCI DSS applies to all organisations which hold, process, or exchange cardholder information from any card branded with the logo of one of the card brands.

Validation of PCI DSS compliance can be performed either internally or externally, depending on the volume of card transactions the organisation is handling, but compliance must be re-assessed annually regardless of the size of the organisation.

The PCI DSS standard has recently been updated to v3.2. As well as some clarification and enhancements of the requirements, some of the general principals have also been updated. The 200+ specific requirements and other elements of the DSS are organised into the following:

BUILD AND MAINTAIN A SECURE NETWORK	
1	Install and maintain a firewall configuration to protect cardholder data
2	Do not use vendor supplied defaults for system password and other security parameters
PROTECT CARDHOLDER DATA	
3	Protect stored cardholder data
4	Encrypt transmission of cardholder data across open, public networks
MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM	
5	Protect all systems against malware and regularly update anti-virus software or programs
6	Develop and maintain secure systems and applications
IMPLEMENT STRONG ACCESS CONTROL MEASURES	
7	Restrict access to cardholder data by business need to know
8	Identify and authenticate access to system components
9	Restrict physical access to cardholder data
REGULARLY MONITOR AND TEST NETWORKS	
10	Track and monitor all access to network resources and cardholder data
11	Regularly test security systems and processes
MAINTAIN AN INFORMATION SECURITY POLICY	
12	Maintain a policy that addresses information security for all personnel

About Osirium

Osirium transforms the way organisations manage, protect and implement change across multi-vendor infrastructures. Osirium reduces operational risk and drives IT service performance and compliance by providing role-based management controls and automation to system administration tasks.

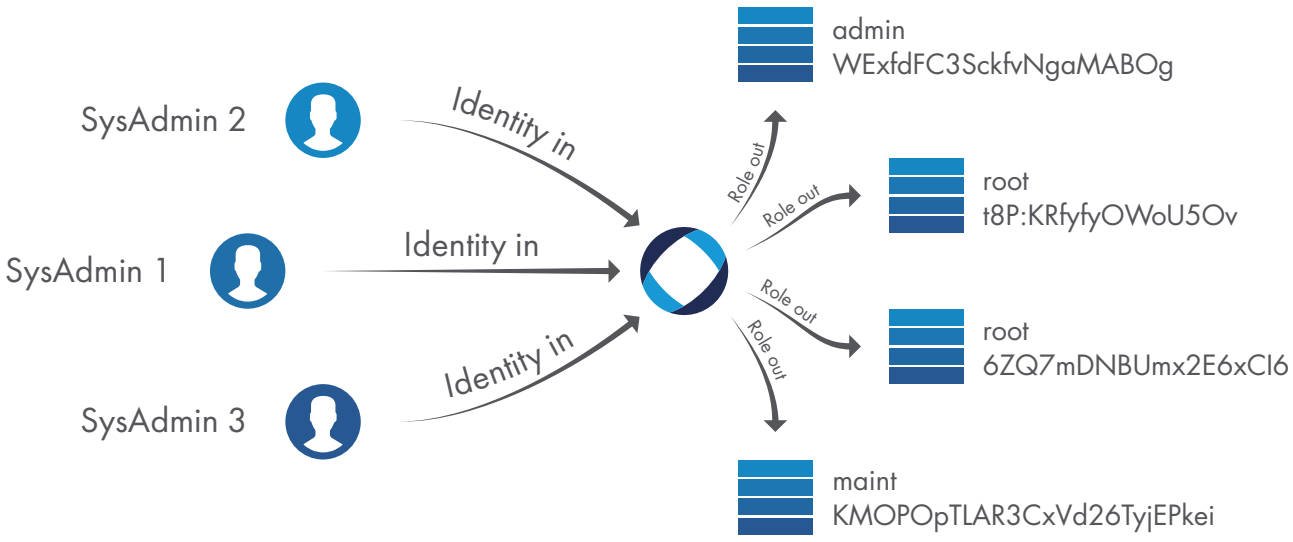
Features of Osirium's PxM Platform include:

- Strong authentication and single sign-on.
- Centrally automates common privileged user tasks.
- Dynamic dashboards and reports for users and devices.
- No disruption to existing systems and processes.
- Quick and easy to deploy and use.

Benefits of Osirium's PxM Platform include:

- Reduces operational risk.
- Saves time and increases productivity of the workforce.
- Strengthens the security of devices.
- Ensures compliance requirements are met.
- Immediately contributes to ROI.

How Osirium works



How Osirium can help satisfy PCI DSS

Osirium can be used to support your organisation's compliance with PCI DSS requirements for the protection of credit-card holder data by enhancing security whilst at the same time reducing operational risk and cost. Osirium achieves these objectives through a combination of Authentication, Access Control, Audit Logging and Automation.

Osirium provides you with the tools to enable you to achieve compliance for privileged user access; it cannot determine if you have met your overall compliance objectives. For this determination you are advised to consult a qualified advisor.

BUILD AND MAINTAIN A SECURE NETWORK

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

Mostly configuring firewall rules will require login access. However once defined, firewall and content managers should be regularly tested for known vulnerabilities. This is where products like Tenable's Nessus can be run from Osirium's PxM Platform as a scheduled task. Nessus will need privileged access to authentication services to test for weaknesses, etc. The elegance of the PxM Platform integration is that no human need know the credential passwords so these can be 128 characters and regularly refreshed

Osirium's PxM Platform can be used to standardise the tasks involved in making firewall changes and in ensuring that these changes get made in a uniform manner. [1.1]

Osirium's PxM Platform can also securely manage backups of device configuration files. [1.2.2]

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

Osirium's PxM Platform protects devices by automatically changing known account passwords away from vendor defaults. Long, strong complex passwords unique per account, per device, provides the ultimate security against 'public password' attacks. This protects against device vendor default passwords and from default third party installation passwords too. All unused accounts can be disabled or deleted by the PxM Platform, providing further protection. [2.1]

Other security parameters can also be managed through Osirium's PxM Platform.
Osirium's PxM Platform can ensure that only secure communication channels are used to manage devices [2.3]

PROTECT CARDHOLDER DATA

3. Protect stored cardholder data

Osirium's PxM Platform can govern access to any cryptographic key sources and ensure that the number of custodians is minimised and all actions are audited at all times. [3.4.1, 3.5.1]

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

5. Protect all systems against malware and regularly update anti-virus software or programs

Osirium's PxM Platform provides foundation protection from malware stealing privileged credentials by removing them completely from admin user systems. By injecting the credentials only when required, no passwords or hash is ever stored on the admin user systems, and therefore cannot be attacked by malware. [5.1.1]

6. Develop and maintain secure systems and applications

Osirium's PxM Platform can enforce separation between development, test and production systems. Access can be granted only when required to the appropriate systems. [6.4.1]

Osirium's PxM Platform can be used to see the bigger picture of who has access to what systems across a wider range of diverse devices more than traditional security measures can. [6.4.2]

Osirium's PxM Platform continually audits (and if required, can delete) all privileged accounts, so no accounts can leak from development or test into production. [6.4.4]

IMPLEMENT STRONG ACCESS CONTROL MEASURES

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

Osirium's PxM Platform secures administrative access to system components through privileged account password management and single sign on. Osirium governs, based on user roles, what they can access, when and what they can do. Osirium provides a full audit trail on activities. [7.1]

Osirium's PxM Platform allows a least privileged model to be both defined and enforced. [7.1.1]

Access to generic or shared privileged user IDs are fully tracked and controlled. More granular account levels can also be managed, providing a true access rights minimum need. [7.1.2-3] The PxM Platform is at its heart an 'access control system' providing control and auditing of privileged user activities. [7.2]

It is extensible (through its templates) to support many different devices, systems and technologies allowing for one single solution to be used to protect all systems within the PCI DSS scope. [7.2.1]

Osirium's PxM Platform's own default access setting is deny-all. [7.2.3]

8. Identify and authenticate access to system components

Osirium's PxM Platform can control all non-consumer users and administrators connecting to and managing all system components. [8.1]

All users have a unique personal ID that is used to access system components. Be it using generic or shared accounts or using PxM Platform managed personalised accounts, all actions are easily traceable back to individuals. [8.1.1]

The process of adding, modifying and deleting all administrative accounts can be automated. A full audit trail of actions is also maintained. [8.1.2]

As a single central point of control, access can be easily revoked across all systems in one place. [8.1.3]

Osirium's PxM Platform reports on all inactive users and accounts within a 90-day period. [8.1.4]

It can be used by internal staff, contractors, consultants and third party support and components vendors alike. All access is traceable back to individual account, identifying each individual or third party and a full audit trail is kept. Explicit time windows can be defined that limit vendor access. Live sessions of vendors accessing systems can be watching in a CCTV style. [8.1.5]

Osirium's PxM Platform enforces failed login attempts. [8.1.6]

Osirium PxM Platform's locked out accounts require administrator resetting. [8.1.7]

Osirium's PxM Platform supports external authentication using industry standard RADIUS. This allows for a variety of strong or multi-factor authentication mechanisms to be used to authenticate the user [8.2]

Osirium's PxM Platform protects all privileged credentials using strong cryptography. [8.2.1]

Osirium's PxM Platform allows for password complexity to be defined on a per-device basis and can be as long and complex as the device will support. (i.e. maximum security). As single sign on is performed for all user access, no individual ever knows the password or has to type it in manual, allowing for passwords to be long and complex. [8.2.3]

Osirium's PxM Platform can enforce and change passwords every 90 days. [8.2.4]

Password histories are managed and enforced. [8.2.5]

Osirium's PxM Platform's user passwords can be forced to be changed on the first use. [8.2.6]

Two factor authentication can be enforced (via RADIUS). [8.3]

Osirium's PxM Platform can be used to change all passwords across all systems if any fear of a compromise is suspected. [8.4]

Osirium's Pxm platform has the ability to work solely with personalised accounts wherever possible. Where group, shared or generic (including service accounts) must be used, the PxM Platform can control access to them and audit their use, maintaining full compliance. [8.5]

If Osirium's PxM Platform were to be used by a service provider (in the PCI DSS sense) then it would enforce unique passwords not only for each customer but for each account on each device at each customer. [8.5.1]

It can also enforce all its controls and auditing on database connections. [8.7]

REGULARLY MONITOR AND TEST NETWORKS

9. Restrict physical access to cardholder data

Osirium's PxM Platform has the ability to discover and manage all privileged accounts on all systems. This stops any attempts at physical access to consoles or terminals of systems components from bypassing the security measures in place for network access. [9]

10. Track and monitor all access to network resources & cardholder data

Osirium's PxM Platform provides an audit trail on what has been done by whom on all system components. This is done through session recording and keystroke capture. [10.1-2]

Osirium's PxM Platform audits all accounts on devices and can alert to any new unauthorised accounts appearing. [10.2.1]

No one can have access to a system with root or administrative privileges without going through Osirium's PxM Platform, so all access is monitored. [10.2.2]

Through session recording, Osirium's PxM Platform monitors all actions and attempted actions on devices. [10.2.3-7]

It provides a full audit trail of its own administrative changes via syslog or secure SIEM. [10.3, 10.3.1-6, 10.5]

Osirium's PxM Platform both supports NTP itself and can also be used to configure NTP settings on all in-scope devices to ensure common, in-sync time sources are used across the board. [10.4, 10.4.1-3]

11. Regularly test security systems and processes

Osirium's PxM Platform can audit device configurations against a template and test for invalid configurations. [11.5]

Contact Details

For more information about how Osirium can assist your organisation in meeting PCI DSS requirements, please contact us at:

Email: info@osirium.com
Web: osirium.com
Phone: +44 (0)118 324 2444

References

[1]PCI Data Security Standard v3.2, available at (as of date of publication):
https://www.pcisecuritystandards.org/security_standards/documents.php

OSIRIUM

11-13 High Street, Theale
Reading RG7 5AH

0118 324 2444
osirium.com