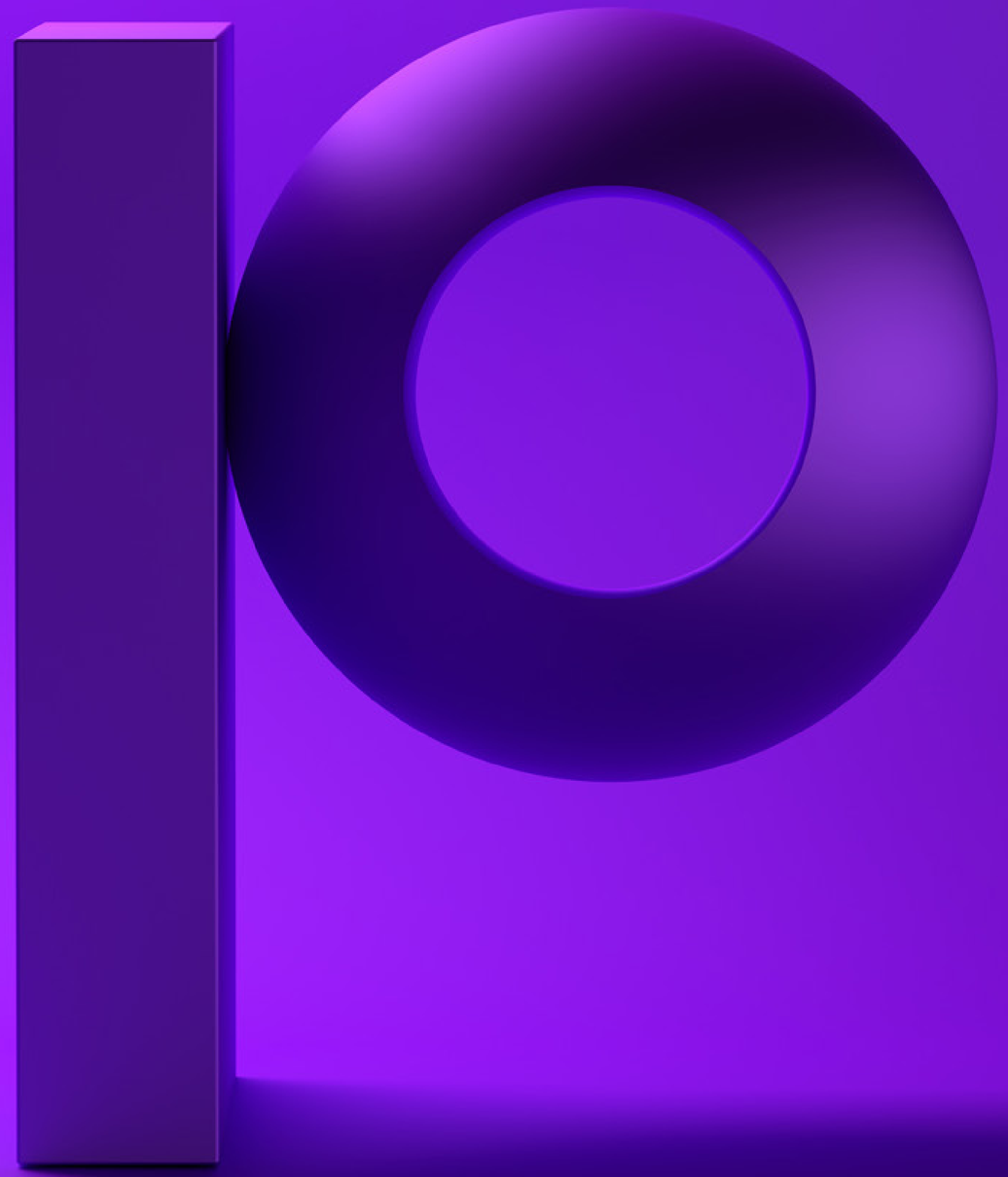
precisely

Best Practices for Maintaining IBM i PCI DSS Compliance



Introduction

If your business processes, stores, or transmits credit or debit card transactions, you're a prime target for cybercrime. Thieves can steal credit card information by hacking into a company's system and downloading payment card data either while it's actively being used in a transaction or while it's at rest in storage.

To add insult to injury data breaches can go undetected for months or years. For example, in April of 2018, a large global retailer announced a data breach involving 5 million customers' payment card information, and the breach wasn't discovered for nearly a year.

Besides the damage to consumers, the costs and consequences of payment card theft for the business are severe. Ponemon Institute reports that the average cost of each stolen record is $148[1], which would have cost the retailer $740 million with that estimate.

To protect consumers from fraud resulting from data theft, the five founding global payment brands - American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc - established a set of industry rules called the Payment Card Industry Data Security Standard (PCI DSS).

The PCI Data Security Standard and other information to help you plan for compliance audits are available for download from the PCI Security Standards Council web site at www.pcisecuritystandards.org.

The process can be confusing for companies preparing for a PCI DSS audit. This eBook is intended to provide tips for achieving compliance with PCI DSS by protecting payment card information in IBM i systems. It does not address the full scope of the regulation and is not intended to provide, and should not be relied on for, legal advice about PCI DSS compliance. If you have specific questions on how this may affect your organization, you should consult your legal advisor.

[1] Ponemon Institute: 2018 Cost of a Data Breach Study (https://www.ibm.com/security/data-breach)

Who's Responsible for Stored Data? PCI Merchant Levels

All merchants who store, process, or transmit cardholder data are subject to PCI compliance regulations.

Level 1 merchants, or merchants with over 6 million transactions a year, or any merchant that has had a data breach, must pass an annual on-site PCI audit from a Qualified Security Assessor (QSA).

Level 2, 3, and 4 merchants, or merchants with up to 6 million transactions a year, must also report their compliance annually but may do so by performing a self-assessment and submitting their Self Assessment Questionnaire (SAQ).

It is recommended that you contact your acquiring bank (the financial institution that processes card payments on your behalf) for reporting responsibilities. To help with this, the PCI Security Standards Council provides an Internal Security Assessor (ISA) certification that aims to train your internal staff on how to conduct a PCI audit.

Any merchant, regardless of size, may be required to pass a PCI audit in the event of a data breach.

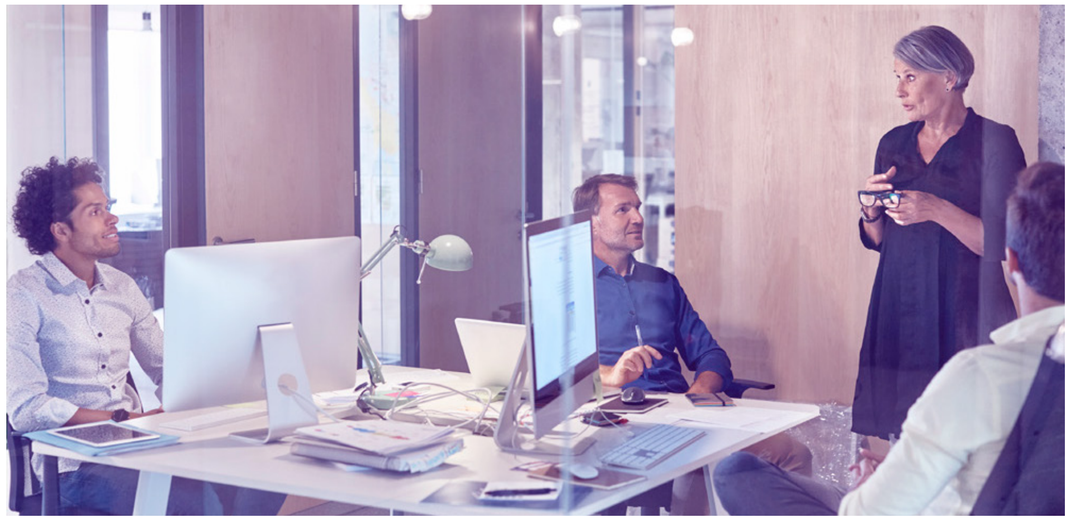
Penalties for Noncompliance

Because PCI DSS is a set of industry standards and not a law, the Security Standards Council doesn't penalize merchants directly. Instead, the acquiring bank can levy monthly fines that range from $5,000 to $100,000 until all noncompliance issues are addressed.

Payment brands such as Visa and MasterCard can also place restrictions on the noncompliant retailer. There are other intangible damages for the merchant as well, particularly if noncompliance leads to a data breach, including brand damage, loss of customer confidence, legal fees, and restitution.

Protecting Payment Card Information

The PCI Data Security Standard contains over 125 pages of requirements that run the gamut from physical security to network security to auditing and reporting. Business process requirements related to breach response planning are also discussed in the standard.



This eBook focuses on key areas for IBM i compliance with PCI DSS requirements and guarding against data breaches, including:

- Assessing security risks
- Monitoring system and database activity
- Detecting compliance deviations and security incidents
- Strengthening login security
- Effectively managing elevated user authority
- Controlling access to systems and data
- Protecting confidential data at-rest from unauthorized access or theft
- Securing data while it is in motion across networks

Assessing Security Risks

Security risk assessments are essential for proactively seeking out security vulnerabilities, a practice required by PCI DSS and many other cybersecurity regulations. IBM i security risk assessment tools and services should check system values, password settings, library authorities, open ports, exit point programs and more to produce reports on potential risks with guidance on how to remediate them.

As a step beyond vulnerability scanning, PCI DSS also requires a methodology for penetration testing. The results of penetration testing help the organization to develop strategies that protect against active attacks.

Monitoring for Compliance Deviations and Security Incidents

PCI DSS requires businesses to monitor access to their systems and data. IBM i journals and log files should be configured to capture information on all systems and data access. These audit logs are required to be retained and must be protected from tampering.

Security monitoring and reporting solutions leverage powerful filtering, query and mapping capabilities to analyze the content of IBM i journals and log files, producing alerts and reports on compliance events in real time. Those events might include decryption of sensitive data, data accesses outside business hours, views of a sensitive spool file, changes to authorization lists, and much more.

Solutions that forward security and compliance events to a SIEM solution such as IBM QRadar, Splunk, LogRhythm and others allow for IBM i security data to be correlated, analyzed, and reported upon with security data from other platforms.

Strengthening Login Security

PCI DSS contains many requirements related to passwords and idle user management. Many of these basic password and login management settings, such as the maximum number of failed logins allowed or required password change interval, can be configured through system settings available in the IBM i OS.

To further strengthen login security, PCI DSS requires multi-factor authentication for users accessing the Card Data Environment (CDE) from a remote location as well as for all administrative users accessing the CDE outside the console.

Multi-factor authentication requires two or more identifying factors to prove a user's identity before access is granted. These factors can be something the user knows (such as a password or PIN), something they have (such as a cell phone or a token device), or something they are (such as a thumbprint or iris scan.) The requirement for at least two authentication factors substantially reduces the chance of an intruder gaining access to a system and its data.

Learn more about multi-factor authentication: Download our white paper *Multi-Factor Authentication for IBM i*

Managing Elevated User Authority

PCI DSS also requires that access to highly privileged user profiles be restricted. To protect against data breaches, IBM i users should only have the minimum authorities required to do their jobs. Use of powerful profiles that include *SECADM, *ALLOBJ or other powerful authorities should be granted only as needed and on a time-limited basis. Automating the process of granting and revoking user authorities via an elevated authority management tool supports strict privilege management requirements and reduces the risk of human error inherent in manual processes.

Learn more about elevated authority management: Download our eBook *Managing Elevated IBM i Authorities: Best Practices in Data Security and Compliance*

Controlling Access to Systems and Data

Reliable control of access to systems and data is also called for by PCI DSS to keep unauthorized people out of your IBM i environment and maintain tight control over what authorized users can do. Unauthorized access via sockets and network protocols (e.g., ODBC, FTP, DRDA, etc.) can be prevented using rules-based exit programs that cover network and socket exit points.

Because exit programs can be difficult to create and maintain, many shops choose to use third-party solutions that significantly streamline these tasks and provide the ability to trigger alerts should suspicious activity be detected. A comprehensive solution will also control access through open source database protocols, command lines, and more.

Learn more about access control: Download our white paper *Four Powerful Ways to Use Exit Points for Securing IBM i Access*

Protecting Data at Rest and In Motion

If a hacker should break through all other lines of defense and gain access to your IBM i data, having proper data privacy technology in place will render the data useless to them. That is why PCI DSS requires that data protection measures be in place. Obscuring payment card information can be done using a mix of five critical elements: encryption, masking, tokenization, anonymization, and secure file transfer.

Encryption

Encryption combines the implementation of one or more publically available algorithms with a secret piece of data called an encryption key. Together, the algorithm and the encryption key turn plain text into unreadable text or ciphers.

Encryption can be used to protect data at rest in an IBM i database, IFS files, spooled files or on backup tapes. Beginning with IBM i 7.1, encrypting Db2 data for IBM i was significantly simplified through the introduction of Field Procedures, or FieldProc.

All encryption isn't equal, however. The Advanced Encryption Standard (AES) is an advanced encryption algorithm that replaces the older Data Encryption Standard (DES). AES is a block cipher that is so secure that it's used by the U.S. government to protect classified information. Whatever encryption technology you use, ensure that it leverages AES and not the old DES algorithm.

The US National Institute of Standards and Technology (NIST) also offers certifications for AES implementations. The use of solutions that have been validated by independent testing houses to meet published AES implementation standards is a smart decision.

PCI DSS also requires robust encryption key management practices. Encryption keys should have a managed lifecycle that includes creation, activation, use, rotation, expiration, retirement and destruction after a period of time. PCI DSS also requires that encryption key management include separation of duties and dual-control processes in which two or more people are involved with managing encryption keys.

Learn more about encryption and key management. Download *IBM i Encryption with FieldProc and Assure Encryption: Protecting Data at Rest*

Tokenization

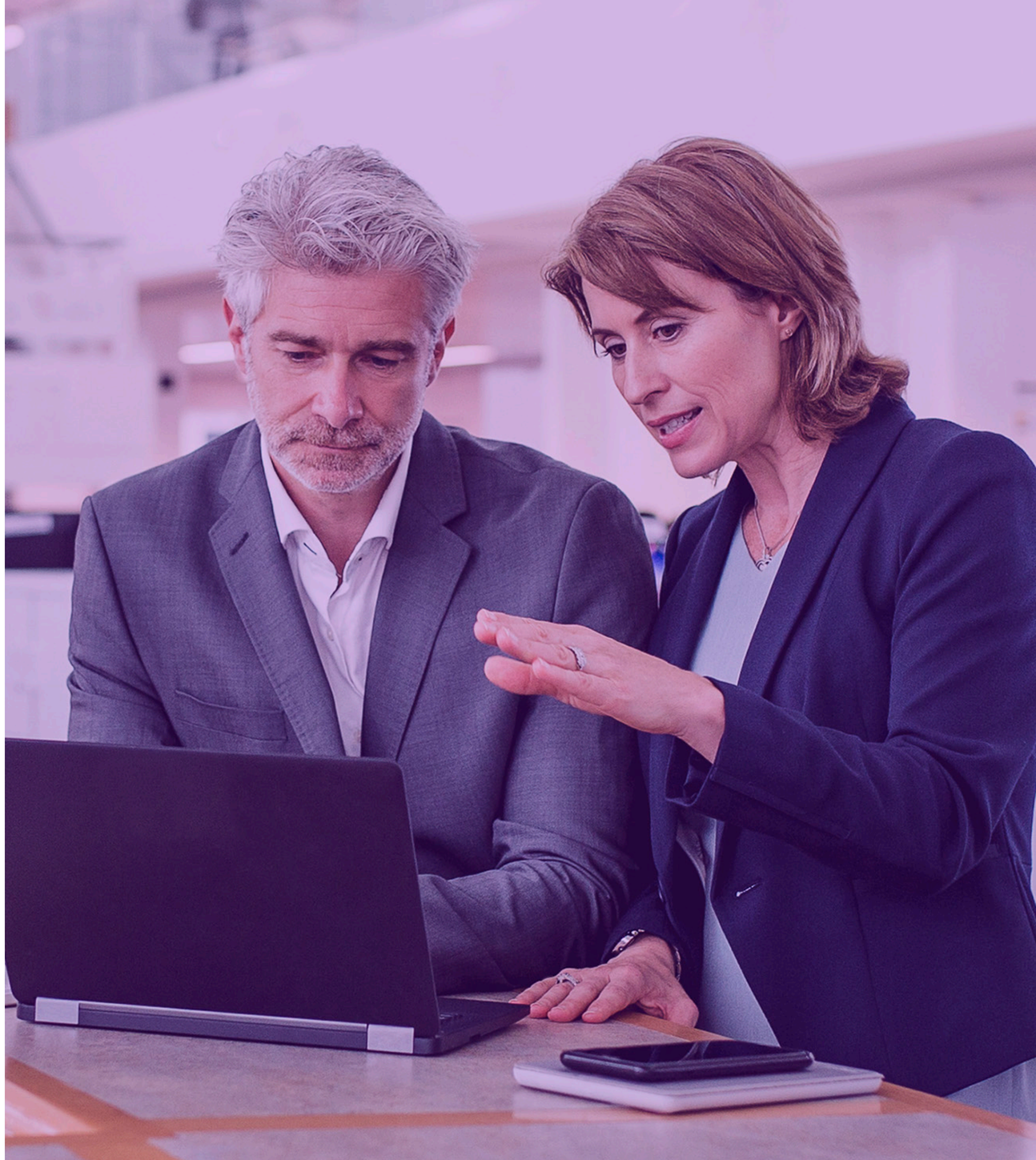
Tokenization substitutes sensitive data such as credit card or bank account numbers with non-sensitive, format-preserving token values. Generally, there is a repository, called a token vault, that contains the original numbers and maps the tokens to the sensitive data.

Unlike encryption, tokenization cannot be algorithmically reversed to find the original value. In other words, tokens have no relationship to the data they replace, so they can't be "cracked." Instead, the initial value is stored in a vault that must be isolated, encrypted, and secure.

Since tokenization separates sensitive data in the token vault from the production environment, it's an effective way to remove servers from the scope of compliance. The server hosting the token vault becomes the focus of compliance efforts.

Tokenization isn't required by PCI DSS yet, but a subcommittee has been established. Both encryption and tokenization address the security of IBM i data at rest.

Learn more about Tokenization. Download *Encryption, Tokenization, and Anonymization for IBM i: A Quick Guide to Protecting Sensitive Data*



Masking

The PCI Data Security Standard contains over 125 pages of requirements that run the gamut from physical security to network security to auditing and reporting. Business process requirements related to breach response planning are also discussed in the standard.

PCI DSS allows for showing only the last four or first six digits of a credit card number. Any encryption or tokenization solution should have masking capabilities that only display a portion of the original data after decryption or retrieval.

Anonymization (Pseudonymization)

Anonymization (also called pseudonymization) is similar to tokenization except that it permanently replaces sensitive data at rest with token values, eliminating the token vault.

This is sometimes referred to as using non-recoverable tokens. Anonymization is an effective means of protecting the privacy of data being used on test or dev systems or data being shared with third parties.

Secure File Transfer

Secure file transfer is required to protect entire files containing sensitive information as they move over internal or external networks. Files are generally transferred using forms of FTP to encrypt data both before and after transfer, and optionally, to keep the data encrypted at the target.

Secure file transfer processes done with third-party solutions provide strong encryption, sound key management processes, and a variety of features that streamline and automate file transfer processes

Learn more: *The Essential Guide to Secure and Managed File Transfers on the IBM i*

Precisely Can Help

With proven security solutions for IBM i and a deep bench of experts whose focus is to stay up to date on security vulnerabilities, best practices, and mitigation technologies, Precisely is here to help you implement a solution that meets your PCI DSS compliance needs. Beyond compliance with external regulations, Precisely can also assist with building out layers of security that meet additional internal security requirements.

Fortify your system and database access control, file and field security, and auditing and reporting with our best-in-class security capabilities that include:

- Network access, database access, and command access control
- Encryption, tokenization, and anonymization
- Secure file transfer
- Elevated authority management
- Multi-factor authentication
- System and database monitoring and reporting
- Model-based compliance management
- SIEM integration
- And more

To learn more about Precisely's security products and services, visit www.precisely.com

precisely

Precisely is the global leader in data integrity, providing accuracy and consistency in data for 12,000 customers in more than 100 countries, including 90 percent of the Fortune 100. Precisely's data integration, data quality, location intelligence, and data enrichment products power better business decisions to create better outcomes. Learn more at www.precisely.com.

www.precisely.com