Payment Card Industry Data Security Standard (PCI DSS) 4.0 Compliance

Learn how ARCON | Privileged Access Management (PAM) solution helps compliance leaders from payment card industry to comply with PCI DSS 4.0 mandates

Table of content

Overview of Payment Card Processing Environment

In 2004, major credit card companies united to create a common security standard. The Payment Card Industry Security Standards Council (PCI SSC) was formed, and the first version of PCI DSS was introduced. Version 1.0 (December 2004) focused on securing cardholder data through encryption, firewalls, and access controls.

Given the exponential growth in the payment card industry, the compliance framework became mainstream, especially among large merchants, but challenges of high cost, lack of awareness, and complexities for small businesses continued to prevail. During this time, data breaches (e.g., TJX Companies breach in 2006) highlighted the importance of PCI DSS compliance.

After multiple levels of amendments in consecutive years, version 4.0 (March 2024) eventually represents the most significant update in years. It aims to address evolving threats and technologies. It introduces a robust approach to compliance, enabling organizations to implement controls tailored to their payment card processing environments. PCI DSS 4.0 demands added emphasis on authentication and encryption requirements.

About Payment Card Industry Data Security Standard (PCI DSS) 4.0 Compliance

PCI DSS (Payment Card Industry Data Security Standard) compliance refers to security standards established to ensure all organizations accept, process, store, or transmit payment card information (card holders' data) to maintain a secure environment. These standards are designed to protect cardholder data from breaches, theft, and fraud.

PCI DSS is a payment card environment security framework developed by major payment processors to protect customer payment card data. The standard includes several requirements for organizations that handle payment card transactions. These requirements include

- Implementing secure network and system configurations
- Protecting stored data
- Encrypting data during transmission
- Maintaining a vulnerability management program
- Implementing strong access control measures

PCI DSS compliance is also based on the number of card transactions processed and the specific requirements of the card network (e.g., Visa and Mastercard). Every business accepting card payments, regardless of size, must comply with PCI DSS. Compliance can be achieved through self-assessment/ audit (for SMBs) or by third parties for larger organizations. Ensuring good cyber hygiene and taking the assessment seriously can meet compliance requirements.

What are the latest updates in PCI DSS 4.0?

PCI DSS 4.0 has introduced a customized approach that allows organizations to meet security requirements using innovative controls and cutting-edge technology. The new version 4.0 has enhanced flexibility, enabling businesses to tailor their security measures to their unique needs while still adhering to PCI DSS mandates.

PCI DSS 4.0 has merged requirements and updated security monitoring systems to be included inthe incident response plan, ensuring more effective incident response. Organizations are now required to detect, alert, and promptly address failures of critical security control systems. The update represents progress in securing the payment ecosystem against fraud.
There were many changes incorporated into the latest version of the Standard (PCI DSS v3.2.1 to v4.0).

- Protect stored account data (Requirement 3.2)
  Restrict access to system components and cardholder data by business need-to-know
- (Requirement 7)
  Access to system components and data is appropriately defined and assigned to maintain
- segregation of duties (Requirement 7.2)
  Multi-factor authentication (MFA) is implemented to secure access to the Common Data
- Environment - CDE (Requirement 8.4)
  Log and monitor all access to system components and cardholder data (Requirement 10)
  Support Information Security with Organizational Policies and Programs to reduce risks from insider threats and risks associated with third-party service providers (TPSPs) (Requirement 12)

Organizations should consider implementing security measures beyond compliance and aligning with other standards and regulations to build and maintain secure systems. PCI DSS version 3.2.1 has already been phased out and will be replaced by the newly released version 4.0 on March 31st, 2024. The old version, however, will remain active for two years after version 4.0 is published.

Objectives of PCI DSS 4.0

The objectives of PCI DSS 4.0 compliance build on the foundational goals of earlier versions, with enhanced focus on flexibility, risk-based approaches, and keeping up with evolving threats. Below are the primary objectives of PCI DSS 4.0 compliance:

Enhance Security Measures

- **Objective:** Strengthen security controls to address modern cybersecurity threats and better protect payment card data.

Address and Support Evolving Threats and Technologies

- **Objective:** Adapt security requirements to meet the demands of modern payment systems and address emerging technologies.

Promote Flexibility of technology/ strategy and Customization

- **Objective:** Allow organizations to meet compliance through methods that best suit their risk management strategies and business models.

Improve Access Validation Methods and Reporting

- **Objective:** Streamline compliance validation processes to reduce complexity and enhance accuracy.

Strengthen Accountability and Governance

- **Objective:** Increase focus on roles, responsibilities, and accountability for security controls.

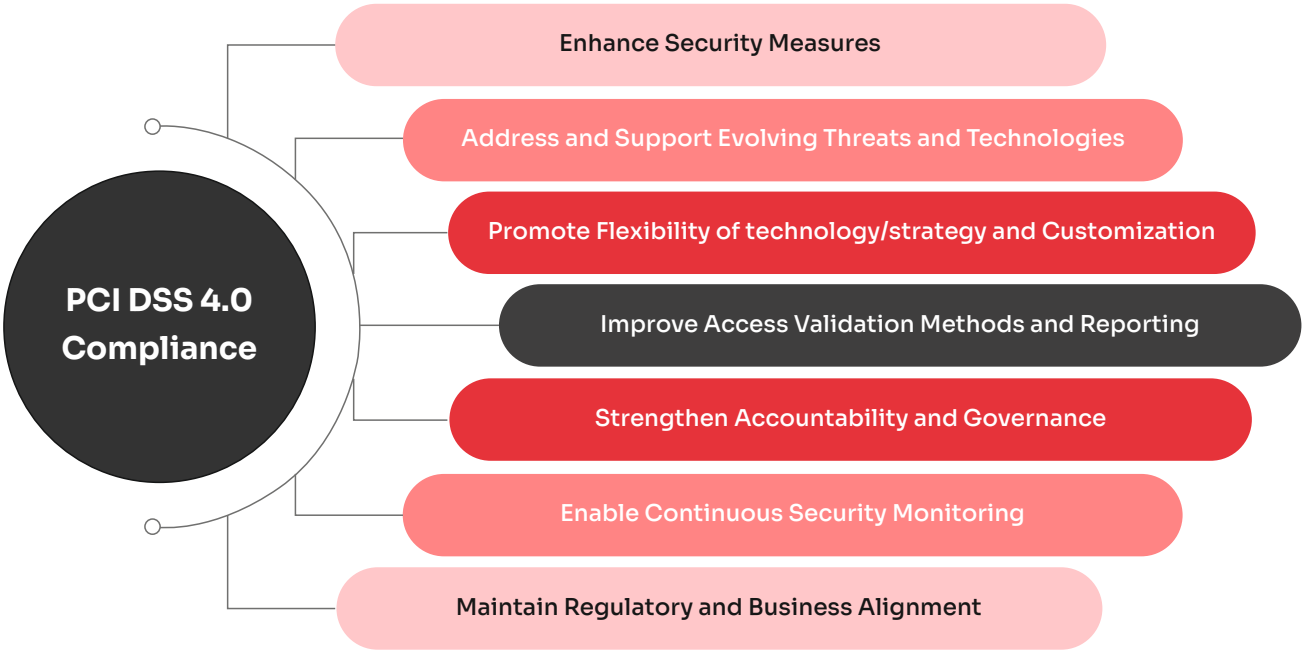
Enable Continuous Security Monitoring

- **Objective:** Transition from point-in-time assessments to continuous security and compliance monitoring.

Maintain Regulatory and Business Alignment

- **Objective:** Align PCI DSS requirements with other global data protection and cybersecurity regulations.

PCI DSS 4.0 compliance aims to balance enhanced security with flexibility, allowing organizations to adapt to changing technologies and threats while maintaining strong protection of payment card data. It emphasizes continuous security, accountability, and alignment with global regulations to create a robust, future-ready payment ecosystem.



Role of ARCON | Privileged Access Management (PAM) in complying with PCI DSS 4.0

ARCON | Privileged Access Management (PAM) is critical in complying with PCI DSS 4.0 by helping organizations secure and manage access to sensitive systems and cardholder data environments (CDE). ARCON | PAM solution addresses several Access Control (Requirement 7 – Implement Strong Access Control Measures) requirements of PCI DSS 4.0, ensuring that access to privileged accounts is tightly controlled, monitored, and logged.

Requirements of PCI DSS 4.0	Does ARCON comply?	Which ARCON solution feature addresses it?
PCI DSS Requirement 3.2: Protect stored account data.	Yes	ARCON | PAM's My Vault tool offers a centralized repository to protect, store and share confidential business information and secrets securely for a defined period.

PCI DSS Requirement 7: Restrict access to system components and cardholder data by business need-to-know	Yes	ARCON | PAM's fine-grained access control restricts users' access only to the authorized card holder systems, applications, and data assets strictly based on their roles. It even allows IT administrators to create policies that restrict specific activities based on "need-to-know" and "need-to-do" basis. As a result, the risks of unauthorized access are mitigated.
PCI DSS Requirement 7.1.1: All security policies and operational procedures that are identified in Requirement 7 are: ○ Documented ○ Kept up to date ○ In use ○ Known to all affected parties	Yes	As a PAM vendor, ARCON always ensures that secure access mechanisms are in place for every IT operational task. Every identity's role and task are well-defined, documented, and updated regularly. Moreover, post-deployment of ARCON | PAM solution, organizations from the payment card industry can automatically comply with the PCI DSS mandates as explained below in the subsequent list of 'requirements.
PCI DSS Requirement 7.1.2: Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood	Yes	Same as above (Requirement 7.1.1.)
PCI DSS Requirement 7.2.1: An access control model is defined and includes granting access as follows: ▪ Appropriate access depending on the entity's business and access needs ▪ Access to system components and data resources that are based on users' job classification and functions ▪ The least privileges required	Yes	With ARCON | PAM, every access to the critical systems in the payment card environment is made through one ADMIN console. It manages entities and access to the target systems/ applications. The solution ensures that the privileged access is granted only on a "need-to-know" and "need-to-do" basis, which is the foundation for robust identity and access control management. It also offers Just-In-Time (JIT) privilege that

(for example, user, administrator) to perform a job function		enforces the principle of least privilege, where access to critical and grants users access only to the resources, they need for their role. It minimizes the chances of misusing unnecessary access rights.
PCI DSS Requirement 7.2.2: Access is assigned to users, including privileged users, based on: ○ Job classification and function ○ Least privileges necessary ○ to perform job responsibilities	Yes	Same as above (Requirement 7.2.1.)
PCI DSS Requirement 7.2.3: Required privileges are approved by authorized personnel	Yes	ARCON | PAM offers a unified admin console for managing entities and access to the target systems/ applications only after authorization. Authorization of access ensures the implementation of an access control framework around people and policies. This way, privileged access is granted only on a “need-to-know” and “need-to-do” basis, which validates the act of authorization.
PCI DSS Requirement 7.2.4: All user accounts and related access privileges, including third-party/ vendor accounts, are reviewed as follows: ○ At least once every six months ○ To ensure user accounts and access remainappropriate based on job function	Yes	ARCON’s Identity Governance model helps IT risk management teams in the payment card environment to – ○ ARCON’s Identity Governance model helps IT risk management teams in the payment card environment to – ○ Provision or de-provision users based on need-based tasks ○ Establish role-wise and time-wise access to the critical systems/ applications ○ Create workflow matrix for IT administrative ease

○ Any inappropriate access is addressed Management ○ Acknowledges that access remains appropriate		○ Build a rule and role-based centralized access control policy ○ Vault, generate and randomizes passwords ARCON | PAM helps govern identities and at the same time uses deep-learning threat detection techniques to assess the level of IT risks. It offers five governance models. ○ User Access Governance ○ Asset Access Governance ○ Asset Group Linking Governance ○ Customized Governance ○ Role Membership Governance With ARCON's User Access Governance, IT infrastructure and security teams can – ○ Configure the review circle of all access given to the users ○ Allow or revoke any privileged account mapped to a particular user ○ Govern the accounts mapped to a particular user at regular intervals ○ Modify the details of the configured user and deleted user ○ Pre-schedule the review process at any specific date
PCI DSS Requirement 7.2.5: All application and system accounts and related access privileges are assigned and managed as follows: ○ Based on the least privileges necessary for the operability of the system or application ○ Access is limited to the systems, applications, or processes that specifically require their use	Yes	ARCON | PAM offers Just-in-time (JIT) Privilege that lays the foundation of the least privilege principle by limiting access to critical systems and enterprise data only to authorized personnel. They provide granular access controls to ensure users have the permissions necessary only when performing their tasks as per their set of roles for a pre-defined period.

PCI DSS Requirement 7.2.5.1: All access by application and system accounts and related access privileges are reviewed as follows: ○ Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) ○ The application/system access remains appropriate for the function being performed ○ Any inappropriate access is addressed ○ Management acknowledges that access remains appropriate	Yes	Governing every Identity in the payment card environment is crucial to ensuring that every access is authorized, genuine, and purpose based. ARCON's Identity Governance (also known as User Access Governance) manages digital identities and their access to critical resources according to policies, procedures, and technologies. Identity Governance assists organizations in the payment card industry in ensuring that the right people have the right level of access to the right resources at the right time for the right reasons. Moreover, ARCON's IG model includes the entire identity lifecycle and adds the below to ensure that every access is appropriate, authorized, and up to date. ○ Identity creation ○ Identity management ○ Identity deletion (when required) ○ Monitoring of identities ○ Review of identities ○ Certification/ Re-certification of access rights
PCI DSS Requirement 7.2.6: All user access to query repositories of stored cardholder data is restricted as follows: ○ Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges.	Yes	Just-In-Time (JIT) Privilege module of ARCON | PAM lays the foundation for the "least privilege" principle and ensures that the right people have the proper access to the right resources during the right time for the right reasons. It also offers Workflow Management, which helps to configure the access approval process for privileged users, user groups, and service groups. This is applicable to

○ Only the responsible administrator(s) can directly access or query repositories of stored CHD		admins as well. Permitting service access through workflow helps to track who has access to which repository and for what purpose. In addition, ARCON's reporting mechanism helps administrators remain audit-ready by providing customized and detailed analytics of every access given to the target systems/ applications.
PCI DSS Requirement 7.2: Access to system components and data is appropriately defined and assigned to maintain segregation of duties.	Yes	ARCON | PAM ensures that every access to critical systems is based on roles (RBAC model). Every identity in the payment card environment has assigned permissions and privileges to individuals or entities based on their roles and responsibilities. As a result, duties are segregated.
PCI DSS Requirement 7.3.1: An access control system(s) is in place that restricts access based on a user's need to know and covers all system components	Yes	ARCON | PAM's fine-grained access control can limit privileged users' access only to the relevant systems, applications, and data assets where the tasks need to be performed. It also allows IT administrators to create policies that restrict specific activities that privileged users can perform on a specific system or application. This way, organizations can maintain control over privileged access and ensure that every access is based on "need-to-know" and "need-to-do" basis. It reduces the risk of insider threats and cyber espionage.
PCI DSS Requirement 7.3.2: The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function	Yes	The fundamental mechanism ofARCON | PAM suggests that the administrators and users with elevated permissions can access infrastructure and critical business assets. So, any sort of unauthorized access or misuse to the systems/ applications might pose catastrophic harm to the organization.

PCI DSS Requirement 7.3.3: The access control system(s) is set to “deny all” by default	Yes	Some key features of ARCON | PAM such as Multi-factor Authentication (MFA), Just-In-Time (JIT) Access, Knight Analytics (Behaviour Analytics), Credential Vaulting, Session Monitoring, Fine-grained Access Control, Reporting and Audit Trails help to build the foundation of Zero Trust Security model.
PCI DSS Requirement 8.4: Multi-factor authentication (MFA) is implemented to secure access to the CDE.	Yes	ARCON | PAM helps to implement MFA for privileged accounts to ensure that only verified and authorized users can access critical systems/ applications. It also supports adaptive authentication mechanisms that allow IT administrators to build the level of security based on the login attempt's relevance. This AI-based technology analyzes the user's geographic location and login behavior, including IP address, device used, typing speed, time to log in, etc., through an authentic and reliable environment. Any deviation from this baseline standard is notified to the administrator, who helps take immediate action on it.
PCI DSS Requirement 10: Log and monitor all access to system components and cardholder data.		ARCON | PAM helps administrators with log details of all privileged user activity, providing comprehensive audit trails to support forensic investigations and compliance audits. It also enables real-time monitoring and flagging off alerts for any anomalous or unauthorized activities in the network zone.

PCI DSS Requirement 12: Support Information Security with Organizational Policies and Programs to reduce risks from insider threats and risks associated with third-party service providers (TPSPs).		ARCON | PAM manages, monitors, and secures third-party vendor access by providing time-based and role-based access to critical systems/ applications. Also, ARCON's highly effective AI-based Knight Analytics tool helps detect anomalies in the logged data based on users' historical records and predict risks based on user activities of insiders or third-party users with the help of machine learning algorithms. It also audits all actions performed by third-party users.

Conclusion

Predictive security threats in payment card processing environments for 2025 will evolve as cybercriminals leverage advanced technologies and exploit vulnerabilities in payment systems.

ARCON | Privileged Access Management is essential for organizations seeking PCI DSS 4.0 compliance. By controlling, monitoring, and securing privileged access to cardholder data environments, PAM helps mitigate risks, meet regulatory requirements, and ensure the integrity of payment systems. It strengthens security and provides the visibility and accountability needed for effective compliance management.

Benefits of ARCON | PAM for PCI DSS 4.0 Compliance:

- **Reduced Risk of Data Breaches:** Limits exposure of cardholder data by restricting access to authorized users
- **Improved Accountability:** Tracks and audits all privileged activities to identify misuse or breaches quickly
- **Enhanced Security Posture:** Protects against credential theft and insider threats
- **Support Zero-Trust Architecture:** Continuously validate access permissions and security configurations to authenticate users and support Zero-Trust architecture.
- **Streamlined Compliance:** Simplifies meeting PCI DSS requirements through centralized access management and reporting

About ARCON

ARCON is a leading enterprise information risk control solution provider, specializing in Privileged Access Management (PAM) and continuous risk assessment solutions. Our mission is to help enterprises identify emerging technology risks and help mitigate them by robust solutions that predict, protect and prevent.