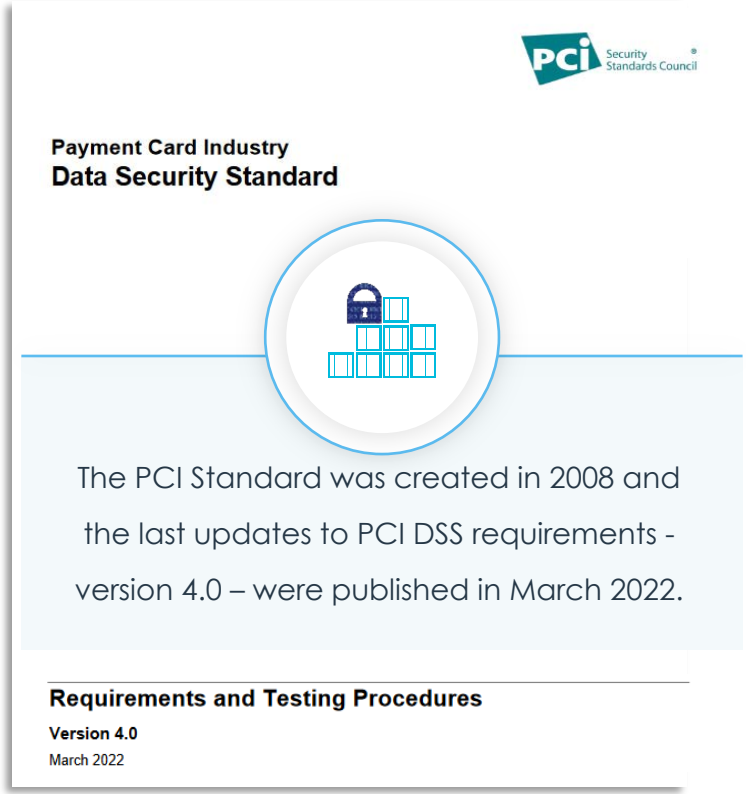
eBook

THALES
Building a future we can all trust

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

cpl.thalesgroup.com

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



- PCI was jointly developed by American Express, Discover, JCB, MasterCard, and Visa.
- It standardizes security controls enforced by businesses processing payment card data.
- The goal of the PCI DSS is to protect cardholder data and sensitive authentication data wherever it is stored, processed, or transmitted.
- The last update to PCI DSS requirements - version 4.0 – were published in March 2022 and became effective as of April 1st 2024.

Goals for PCI DSS 4.0

PCI DSS 4.0 evolves the standard to accommodate changes in technology, risk mitigation techniques, and the threat landscape. It also introduces greater flexibility to support organizations using a broad range of controls and methods to meet security objectives.

Continue to meet the security needs of the payment industry

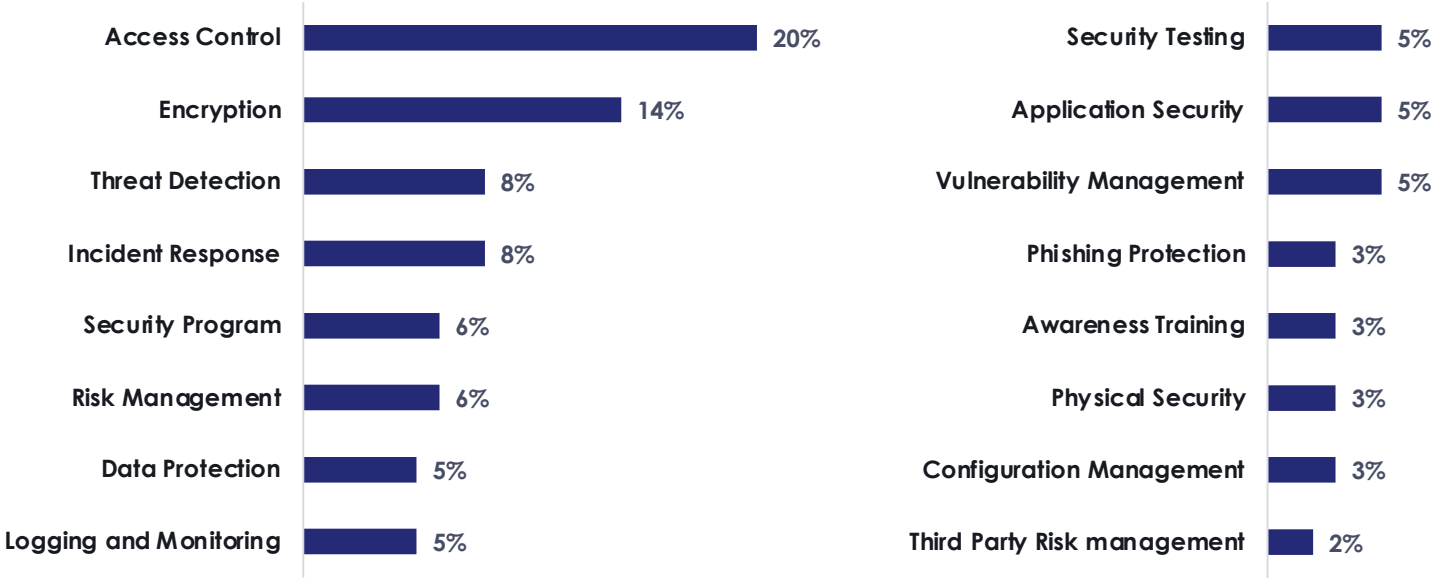
Promote security as a continuous process

Add flexibility for different methodologies

Enhance validation methods

What is new for PCI DSS 4.0?

> There are 64 new requirements introduced in version 4.0. Various security solutions can address many of these security requirements directly or indirectly.

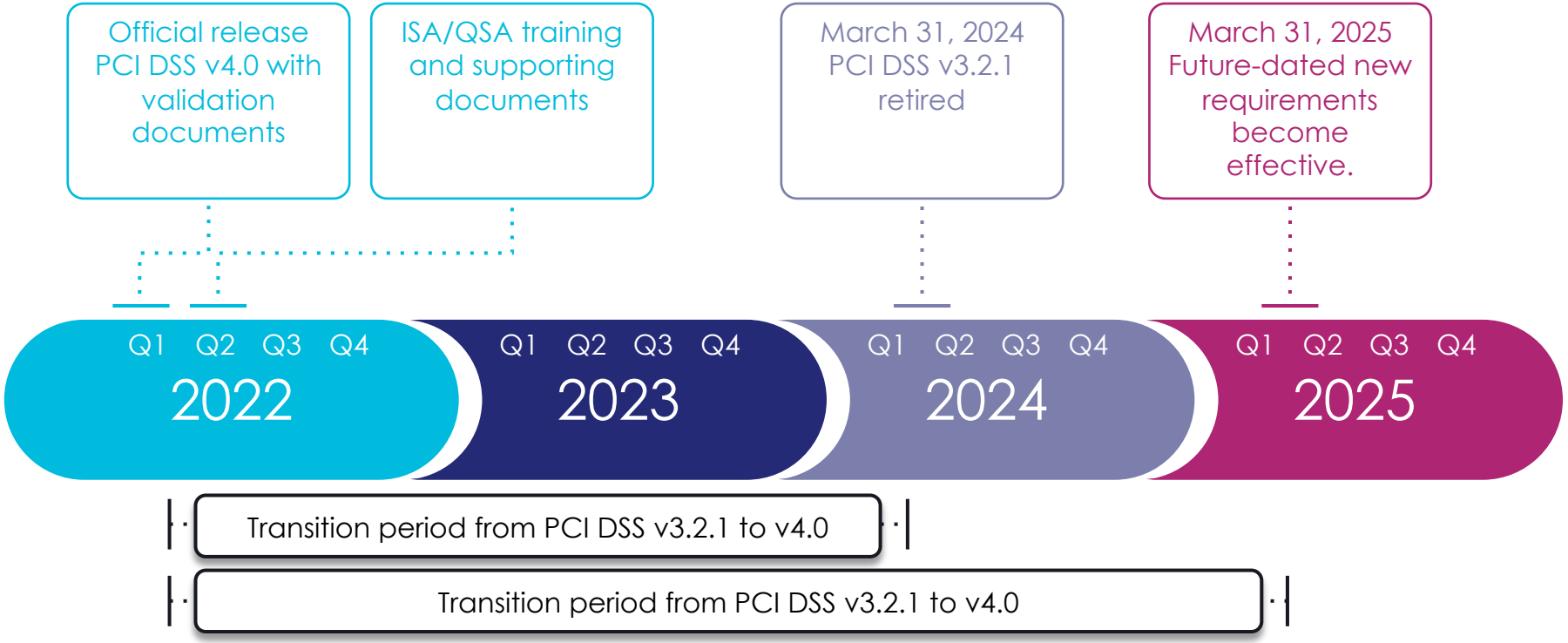


Source: Datos Insights, Understanding and Preparing for PCI DSS 4.0, Jan 2024.

What are the main differences between PCI DSS 3.2.1 and 4.0?

- Expansion of Requirement 8 to implement multi-factor authentication (MFA) for all access into the cardholder data environment.
- Updated firewall terminology to network security controls to support a broader range of technologies used to meet the security objectives traditionally met by firewalls.
- Increased flexibility for organizations to demonstrate how they are using different methods to achieve security objectives.
- Addition of targeted risk analyses to allow entities the flexibility to define how frequently they perform certain activities, as best suited for their business needs and risk exposure.

PCI DSS 4.0 Implementation Timeline



Who Must Comply to PCI DSS

PCI DSS compliance is mandatory for financial institutions, online payment processors, merchants that accept payment cards, and any organization that processes payment card transactions, stores or accesses payment card information, and any service providers that enable business anywhere in the card processing eco-system.

Failure to Comply with PCI DSS 4.0

Penalties can range from:

$5,000 to $100,000

Per month

Depends on:

Volume of transactions

The appropriate PCI DSS level

Amount of time not compliant

> Penalties can also include increased audit requirements and potential shut down of credit card activity by a merchant bank or credit card brand.

Protecting Personal Data

Temporary Data

- Personal Identification Information (PII)
- Authentication credentials

Permanent Data

- Credit Card Chip PIN
- Credit Card Holder's Name
- Credit Card Number
- Permanent Account Number (PAN)

THALES
Building a future we can all trust

How Thales Can Help

Data Security for PCI DSS 4.0

PCI DSS 4.0 Requirements in a Nutshell

Goals	PCI DSS Requirement	Supported by Thales
Build and maintain a secure network and systems	1. Install and maintain network security controls	☐
	2. Apply secure configuration to all system components	☑
Protect cardholder data	3. Protect stored account data	☑
	4. Protect cardholder data with strong cryptography during transmission over open, public networks	☑
Maintain a vulnerability management program	5. Protect all systems and networks from malicious software	☐
	6. Develop and maintain secure systems and software	☑
Implement strong access controls	7. Restrict access to system components and cardholder data by business need to know	☑
	8. Identify users and authenticate access to system components	☑
	9. Restrict physical access to cardholder data	☑
Regularly monitor and test networks	10. Log and monitor all access to systems components and cardholder data	☑
	11. Test security of systems and networks regularly	☑
Maintain an information security program	12. Support information security with organizational policies and programs	☑

How Thales can help

Thales can help organizations comply with PCI by identifying cardholder data across hybrid IT and protecting the data as well as the applications and identities that have access to it.

Application Security

Protect applications and APIs at scale in the cloud, on-premises, or in a hybrid model.

Data Security

Identify, protect, monitor, report, and govern sensitive data across hybrid IT.

Identity & Access Management

Provide seamless, secure and trusted access to applications and digital services.

Thales Application Security solution mapping to PCI DSS 4.0 requirements

Requirement	Main Capabilities	Solutions
Requirement 6: *Develop and Maintain Secure Systems and Software.*		
6.3.2: *Inventory bespoke, custom and third-party software.*	> Discover, inventory, and remediate vulnerabilities in APIs that process, receive, transmit, and store cardholder data with API protection solution.	**API Protection**
6.4.1: *Web apps are protected against known attacks and threats and vulnerabilities are addressed.*	> Detect and block anomalous behavior by the software during execution with RASP solution.	**Runtime application self-protection (RASP)**
6.4.2: *Automated technical solution is deployed to continually detect and prevent attacks on web apps.*	> Inspect all traffic, detect and prevent web-based attacks with WAF. > Prevent DDoS attacks with scalable DDoS attack traffic absorption provided by edge servers.	**Web Application Firewall (WAF)** **DDoS Protection**
6.4.3: *All payment page scripts that are loaded and executed in the consumer's browser are managed.*	> Allow only authorized scripts where the payment page is loaded.	**Client-side Protection**
Requirement 11.6 *Unauthorized changes on payment pages are detected and responded to.*	> Prevent unauthorized changes to payment pages by allowing only authorized scripts.	**Client-side Protection**

Thales Data Security solution mapping to PCI DSS 4.0 requirements

Requirement	Reference Number	Main Capabilities	CipherTrust Platform	Data Security Fabric	Hardware Security Modules	High Speed Encryptors
Requirement 2: *Apply secure configurations to all system components.*	2.2	> Discover, analyze and prioritize vulnerabilities. > Multi-Tenancy and separation of duties. > Encrypted Non-console administrative access.	☐	☑	☑	☑
Requirement 3: *Protect Stored Account Data.*	3.2; 3.3; 3.4; 3.5; 3.6; 3.7	> Discover and classify cardholder data. > Encrypt and tokenize cardholder data. > Protect encryption keys in FIPS 140-2 L3 devices. > Key and secrets lifecycle management.	☑	☑	☑	☐
Requirement 4: *Protect Cardholder Data With Strong Cryptography During Transmission.*	4.2	> Tokenization and encryption of data prior to transmission. > High speed encryption of data in motion.	☑	☐	☑	☑
Requirement 6: *Develop and Maintain Secure Systems and Software.*	6.1; 6.3; 6.5	> FIPS 140-2 L3 root of trust for credentials and keys > Discover, analyze and prioritize vulnerabilities. > Workflows, playbooks, and orchestration for policies and procedures.	☐	☑	☑	☐
Requirement 7: *Restrict Access to System Components and cardholder Data by Need to Know.*	7.1; 7.2	> Deny unauthorized access to protected cardholder data and secrets. > Separation of duties and least privilege access. > Centralized access policies.	☑	☑	☐	☐
Requirement 9: *Restrict Physical Access to Cardholder Data.*	9.4	> Encryption and tokenization of data with destruction of keys.	☑	☐	☐	☐
Requirement 10: *Log and Monitor All Access to System Components and Cardholder Data.*	10.1; 10.2; 10.3; 10.4; 10.5; 10.6	> Complete access audit logs for files, keys, secrets sent to SIEM. > Continuous verification of audit activity 24/7 365. > Machine-learning anomaly detection to identify suspicious behavior.	☑	☑	☑	☐
Requirement 12: *Support Information Security with Organizational Policies and Programs.*	12.5; 12.10	> Locate structured and unstructured regulated data across the cloud, big data, and traditional data stores.	☑	☑	☐	☐

Thales Identity & Access Management solution mapping to PCI DSS 4.0 requirements

Requirement	Reference Number	Main Capabilities	Solutions
Requirement 7.2: *Access to system components and data is appropriately defined and assigned.*	*7.2.1; 7.2.2*	> Centrally manage unique user identities, risk-based authentication policies, and add/revoke access to systems in your Cardholder Data Environment (CDE).	**Workforce Identity & Access Management**
Requirement 8.2: *Identify users and authenticate access to system components.*	*8.2.1; 8.2.2; 8.2.4; 8.2.5; 8.2.6*	> Ensure each user is assigned a unique credential, with a complete set of provisioning rules and policy engines that cover all functionalities with MFA.	**Workforce Identity & Access Management**
Requirement 8.3: *Strong authentication for users and administrators is established and managed.*	*8.3.1; 8.3.3; 8.3.4; 8.3.11*	> Broadest range of authentication methods and form factors help address numerous use cases, assurance levels, and threat vectors. > Centrally managed policies—managed from one authentication back-end delivered in the cloud or on premise. > Methods include context-based authentication combined with step-up capabilities, one-time password (OTP), X.509 certificate-based solutions, and FIDO security keys.	**Broad Range of Authenticators** **Workforce Identity & Access Management**
Requirement 8.4 *Multi-factor authentication (MFA) is implemented to secure access into the CDE.*	*8.4.1; 8.4.2; 8.4.3; 8.5*		
Requirement 8.5 *Multi-factor authentication (MFA) systems are configured to prevent misuse.*			
Requirement 9: *Restrict Physical Access to Cardholder Data.*		> Smart cards can be integrated with various building access technologies to function as both an employee's physical and digital ID.	**Smart Cards**
Requirement 10: *Log and Monitor All Access to System Components and Cardholder Data.*		> Full audit trail of access events as well as automated log export and seamless integrations with SIEM systems to ensure continuous monitoring and compliance.	**Workforce Identity & Access Management**

Thales reduces the complexity of compliance with platforms that protect and manage applications, data, and identities at scale

THALES
Building a future we can all trust

+

imperva
a Thales company

Applications

- Web Application Firewall
- DDoS Protection
- Bot Protection
- API Security

Data

- Encryption
- Tokenization
- Key & Secrets Management
- Hardware Security Modules
- Data Activity Monitoring
- Data Discovery & Classification
- Data Governance
- Threat Detection

Identities

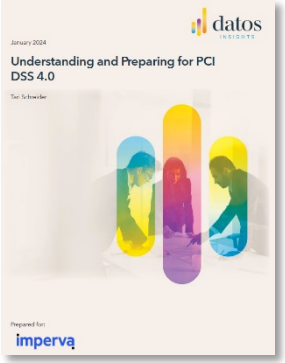
- Customer Identity & Access Management
- Workforce Identity & Access Management
- Broad Range of Authenticators

Next steps

Learn More

White Paper:

Application Security Compliance with PCI DSS 4.0



White Paper:

Data Security Compliance with PCI DSS 4.0

Solution Brief:

Identity & Access Management Compliance with PCI DSS 4.0

Contact Us

> Schedule a demo

> Learn more about our use cases

> Talk to a representative

THALES

Building a future we can all trust

Contact Us

For all office locations and contact information, please visit

cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com