Cyolo

How Cyolo Helps You Achieve Compliance: PCI DSS 4.0

Any company, no matter its size, that transmits customer financial information is required to comply with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. The latest version of this standard, PCI DSS 4.0, was released in November 2020 and is currently being adopted by organizations worldwide.

The main objectives of PCI DSS 4.0 are to improve the overall security posture of organizations and to provide greater flexibility and scalability to accommodate the rapidly evolving payments ecosystem. Some of the key changes introduced in this version include:

- **Emphasis on risk management:** PCI DSS 4.0 places greater emphasis on the need for organizations to conduct a thorough risk assessment and to implement appropriate risk management strategies to address identified vulnerabilities.
- **Simplification of requirements:** The standard has been reorganized and streamlined to make it easier to understand and implement. The number of requirements has been reduced from 12 to 9, and some requirements have been merged or eliminated.
- **Focus on authentication:** PCI DSS 4.0 places greater emphasis on the need for strong authentication mechanisms, including multi-factor authentication (MFA), to protect against credential theft and misuse.

SECURE SOLUTION

With its zero-trust access solution, Cyolo delivers three layers of controls to better manage scenarios in which user access could cause enormous damage to the business. Deploying Cyolo materially helps support PCI DSS 4.0 compliance during an audit.

- **Emphasis on security testing:** The new standard requires more frequent and rigorous security testing, including penetration testing, vulnerability scanning, and code reviews.
- **Greater clarity on service provider responsibilities:** The standard provides clearer guidance on the responsibilities of service providers that process or store cardholder data on behalf of merchants and other organizations.

Overall, PCI DSS 4.0 is designed to provide a more flexible and scalable framework for securing cardholder data, while also promoting a risk-based approach to security. Organizations that accept credit card payments are required to comply with the standard to protect against data breaches and to maintain the trust of their customers.

HOW CYOLO HELPS

Cyolo is designed to give users access to the resources they need while maintaining the zero-trust model. It is built to support the real world, enabling companies to protect their entire network. With Cyolo, you can securely access the resources you need to get your work done, while keeping your network and data safe.

ACCESS CONTROLS

- **Multi-Factor Authentication** to confirm identity
- **Single Sign-On & Password Vault** for password protection
- **Device Posture** check for endpoint security
- **End-to-End Encryption & Continuous Authorization** for true zero trust
- **Identity Federation** to seamlessly validate trust

CONNECTIVITY CONTROLS

- **Onboard & Offboard** application entitlement
- Block **Risky Actions**
- **Pinpoint Access** to specific applications
- Leverage existing tools to **Merge Domains**
- Control **Activity Permissions**
- **Terminate Connection** once work is completed

OVERSIGHT CONTROLS

- Full **Audit Trail** & complete **Access Logs**
- **Supervised Access** for approval and monitoring
- **Session Recording** to ensure compliance
- Rapid **Disaster Recovery** for **Business Continuity**

(Figure 1. Cyolo Zero-Trust Access controls that support compliance with PCI DSS 4.0)

CYOLO ALIGNMENT WITH PCI DSS 4.0 INFORMATION SECURITY CONTROLS

1: INSTALL AND MAINTAIN NETWORK SECURITY CONTROLS
1.3 Network access to and from the cardholder data environment is restricted.
1.4 Network connections between trusted and untrusted networks are controlled.
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.
3: PROTECT STORED ACCOUNT DATA
3.3 Sensitive authentication data (SAD) is not stored after authorization.
3.4 Access to displays of full PAN and ability to copy cardholder data are restricted.
5: PROTECT ALL SYSTEMS AND NETWORKS FROM MALICIOUS SOFTWARE
5.2 Malicious software (malware) is prevented, or detected and addressed.
6: DEVELOP AND MAINTAIN SECURE SYSTEMS AND SOFTWARE
6.4 Public-facing web applications are protected against attacks.
7: RESTRICT ACCESS TO SYSTEM COMPONENTS & CARDHOLDER DATA BY BUSINESS NEED TO KNOW
7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.
7.2 Access to system components and data is appropriately defined and assigned.
7.3 Access to system components and data is managed via an access control system(s).
8: IDENTIFY USERS AND AUTHENTICATE ACCESS TO SYSTEM COMPONENTS
8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.
8.3 Strong authentication for users and administrators is established and managed.
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.
8.6 Use of application and system accounts and associated authentication factors is strictly managed.
10: LOG AND MONITOR ALL ACCESS TO SYSTEM COMPONENTS AND CARDHOLDER DATA
10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.
10.5 Audit log history is retained and available for analysis.
11: TEST SECURITY OF SYSTEMS AND NETWORKS REGULARLY
11.5 Network intrusions and unexpected file changes are detected and responded to.
11.6 Unauthorized changes on payment pages are detected and responded to.
12: SUPPORT INFORMATION SECURITY WITH ORGANIZATIONAL POLICIES AND PROGRAMS
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.
12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.