bluezone | integrated compliance fabric

PAYMENT SECURITY

# PCI COMPLIANCE

## REGULATORY ALIGNMENT BRIEF

Enhance your security profile and comply wit all 12 PCI Data Security Standard requirements in a single solution.

/// BLUEZONE

# ACCELERATE AND OPTIMIZE PCI COMPLIANCE

## PCI Background

## Detailed requirements to secure system components that support cardholder data environments.

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a minimum set of technical and operational requirements designed to protect cardholder data.

PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks.

The primary account number (PAN) is the defining factor in the applicability of PCI DSS requirements: they are in effect if PAN is stored, processed, or transmitted over the network. In addition, local, regional or sector laws and regulations may require some further protection of personally identifiable information (PII) and other data elements (for example, cardholder name or service code), or define an entity's disclosure practices related to private consumer information.

The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the merchant should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data and ensuring they are included in the PCI DSS scope. Multiple techniques exist for reducing the scope of the PCI audit, ranging from the traditional network segmentation to the most innovative PAN isolation outside of the IT environment.

## Specification Overview

# Guidance to assist merchants, service providers and financial institutions in protecting cardholder data.

PCI DSS requirements apply to all technical system components, such as network devices, compute servers, storage arrays and applications that are included in, or connected to, the cardholder data environment (CDE). System components also include virtualization elements, such as virtual machines, virtual switches/routers, virtual appliances, virtual desktops and hypervisor platforms.

The cardholder data environment is comprised of people, processes and technology that handle *account data* comprised of the following:

| Cardholder Data |
| --- |
| Primary Account Number (PAN) |
| Cardholder Name |
| Expiration Date |
| Service Code |

| Sensitive Auhentication Data |
| --- |
| Track Data (on a magnetic stripe or smart chip) |
| Card Verification Code (CAV, CVC, CVV or CID) |
| Personal Identification Number (PIN) |

If cardholder name, service code or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they should be sufficiently protected, while only the PAN must be rendered unreadable. Sensitive authentication data must not be stored.

The DSS requirements are grouped into 12 high-level categories maintained to achieve the following information security objectives:

- Build and maintain secure networks and systems
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

PCI DSS standard also provides detailed guidelines and best practices to assist entities prepare for, conduct and report on the results of the assessment.

The DSS requirements apply to organizations where account data is stored, processed or transmitted. Some of the requirements may also be applicable to entities that have outsourced payment operations or management of their CDE to third parties; in this case, the entity is responsible for ensuring that the account data is protected by the third party per the DSS requirements. There are two options for third-party service providers to validate compliance:

- Annual, self-initiated assessment
- Multiple, on-demand assessments

To ensure security controls stay in effect, the DSS requirements must be implemented into business-as-usual (BAU) activities as part of an entity's overall security strategy. This enables the entity to monitor the validity of their security controls on an ongoing basis, and maintain their compliant CDE in between the assessments. Examples of how to incorporate PCI DSS into BAU activities include:

- Monitoring of security controls
- Ensuring that all failures in security controls are detected and responded to in a timely manner
- Reviewing changes to the CDE related systems and processes prior to completing the change
- Assessing the impact of organizational mergers and acquisitions to the PCI scope
- Performing periodic reviews and issuing reports to confirm that PCI DSS controls continue to be in place and secure processes are followed
- Reviewing hardware and software technologies at least annually, to confirm that they continue to be supported by the vendor

PCI Security Standards Council provides programs for two kinds of independent experts to help entities undergo their periodic PCI assessment:

- Qualified Security Assessor (QSA) – conducts a review and certification of PCI compliance
- Approved Scanning Vendor (ASV) - performs external vulnerability scans of CDE systems

All system components and business processes in the PCI DSS scope, along with compensating controls, must be documented, reviewed and validated by the assessor on an annual basis, followed by the Report on Compliance (ROC) submission.

Regulatory Alignment

# Protecting cardholder data with bluezone takes over the burden of PCI compliance certification.

An industry-leading bluezone solution tremendously reduces the footprint of your sensitive cardholder data, therefore minimizing compliance delivery costs and expediting the overall PCI DSS certification process. The perimeter of your PAN is limited to the on-premise or hosted bluezone environment, eliminating your own information systems and applications from the scope of PCI DSS assessment.

The bluezone environment itself, subject to strict information security controls and the associated procedures, complies with the DSS 3.1 requirements through the following built-in capabilities:

| PCI DSS Requirement | Capabilities and Benefits |
|---|---|
| **Build and Maintain a Secure Network** | |
| **1 Install and maintain a firewall configuration to protect cardholder data** | |
| **1.1** Establish and implement firewall and router configuration standards. | ♦ Firewall rules and routes are modified according to product documentation<br>♦ Access to bluezone components can be validated with the standard tools |
| **1.2** Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. | ♦ Access to all components is denied, and allowed only via a new rule/route<br>♦ The is no concept of a "trusted network" inside bluezone environment<br>♦ All inbound and outbound traffic is restricted by the network firewall |
| **1.3** Prohibit direct public access between the Internet and any system component in the cardholder data environment. | ♦ Employs a DMZ model with NAT and service layer load balancing<br>♦ Includes TLS offload and external connection termination to prevent direct public access to internal bluezone components<br>♦ Operates segregated platform clusters in a private IP space |
| **1.5** Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties. | ♦ Product documentation and operational policies and procedures for the hosted service are available for distribution to the authorized personnel |
| **2 Do not use vendor-supplied defaults for system passwords and other security parameters** | |
| **2.1** Always change vendor-supplied defaults before installing a system on the network. | ♦ Each bluezone component installation includes a set of unique keys<br>♦ Service-specific credentials are customized in the configuration files and encrypted at the application server startup time |
| **2.2** Develop configuration standards for all system components; assure they address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. | ♦ System and business services deployed in bluezone implement best practices of information security industry standards, including PKI, RSA cryptography, NIST security guidelines and W3C security recommendations<br>♦ Adopts ISO/IEC 27000 and Common Criteria security management techniques<br>♦ All bluezone components segregate primary processing functions in separate physical and logical architectural tiers |
| **2.3** Encrypt all non-console administrative access using strong cryptography. | ♦ Major bluezone components offer a web-based administration, where access can be secured via HTTPS to the external TLS termination point |
| **2.4** Maintain an inventory of system components that are in scope for PCI DSS. | ♦ All hardware and software components of bluezone are well documented<br>♦ The currency of product documentation and hosted service procedures is maintained by the vendor and data center facility provider, respectively |
| **2.5** Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are well documented and in use. | ♦ Product documentation and operational policies and procedures for the hosted service are available for distribution to the authorized personnel |

| PCI DSS Requirement | Capabilities and Benefits |
|---|---|
| **2.6** Shared hosting providers must protect each entity's hosted environment and cardholder data. | ♦ Each hosted instance of bluezone runs on a dedicated hardware<br>♦ Access to a hosted environment is completely isolated and self-contained<br>♦ Audit trails are unique to each hosted environment and component |
| **Protect Cardholder Data** | |
| **3 Protect stored cardholder data** | |
| **3.1** Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes. | ♦ Provides data removal methods to comply with retention policies<br>♦ Includes card data search capabilities based on effective expiry date |
| **3.2** Do not store sensitive authentication data after authorization (even if encrypted). | ♦ Optionally, stores account number, card type and expiry date<br>♦ Does not store card verification codes (CAV, CVC, CVV or CID)<br>♦ Does not store personal identification numbers (PIN) |
| **3.3** Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). | ♦ Tokenizes card account number in field-preserving format<br>♦ Returns card Issuer Identification Number (IIN) upon request<br>♦ Returns card mask (last two or four visible digits) upon request |
| **3.4** Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs). | ♦ Uses strong, military-grade cryptography to protect PAN, with the associated key management processes and procedures<br>♦ Uses one-way hashes based on strong cryptography for account number comparison and data integrity |
| **3.5** Implement procedures to protect keys used to secure cardholder data against disclosure and misuse. | ♦ Asymmetric encryption keys are kept in protected key stores<br>♦ Key store credentials are generated and securely maintained by the vendor, separate from the data store access credentials<br>♦ Offers software and hardware security module (HSM) key stores |
| **3.6** Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data. | ♦ Key management procedures are described in product documentation<br>♦ Encryption keys are exposed only to the authorized operational personnel |
| **3.7** Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties. | ♦ Product documentation and operational policies and procedures for the hosted service are available for distribution to the authorized personnel |
| **4 Encrypt transmission of cardholder data across open, public networks** | |
| **4.1** Use strong cryptography and security algorithms to safeguard sensitive cardholder data during transmission over public networks. | ♦ Uses HTTPS for secure online access to financial networks<br>♦ Uses SFTP for secure batch file transfer to processing gateways<br>♦ Supports SIPS secure transport for carrier services access<br>♦ Supports IPsec and SSH tunneling for additional protection |
| **4.2** Never send unprotected PANs by end-user messaging technologies. | ♦ Allows PAN transfer only over secure protocols<br>♦ Encrypts PAN at the message level for online access<br>♦ Encrypts PAN at the file level for batch file transfer |
| **4.3** Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties. | ♦ Product documentation and operational policies and procedures for the hosted service are available for distribution to the authorized personnel |
| **Maintain a Vulnerability Management Program** | |
| **6 Develop and maintain secure systems and applications** | |

| PCI DSS Requirement | Capabilities and Benefits |
|---|---|
| **6.2** Ensure that all system components and software are protected from known vulnerabilities. | ♦ Installs on the latest versions of OS and application servers<br>♦ Employs runtime component-based packaging to isolate from the vulnerabilities of the underlying system infrastructure |
| **6.3** Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, logging), and based on industry best practices. | ♦ Eliminates the need for client application development in scope of PCI DSS assessment and audit<br>♦ Data center service supports proximity hosting, 24/7 monitoring and rapid-fire incident response<br>♦ Software components are developed according to relevant PCI, ISO/IEC and NIST information security guidelines |
| **6.4** Follow change control processes and procedures for all changes to system components. | ♦ Provides separate development and/or integration bluezone environments<br>♦ PAN-processing components are tested with the card number generator, i.e. production account numbers are never used for quality assurance |
| **6.5** Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes. | ♦ System components and business services are developed and tested using secure coding techniques and vulnerability detection methods<br>♦ Employs engineering principles and best practices guidelines for IT security<br>♦ Strong cryptographic functions are used to protect service and data access |
| **6.6** For public-facing web systems, address new vulnerabilities on an ongoing basis and ensure they are protected against known attacks. | ♦ Supports web application firewalls to prevent external web-based attacks<br>♦ Supports reverse proxy servers with TLS termination (for HTTP, SIP) to prevent direct public access to business services |
| **6.7** Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties. | ♦ Product documentation and operational policies and procedures for the hosted service are available for distribution to the authorized personnel |
| **Implement Strong Access Control Measures** | |
| **7 Restrict access to cardholder data by business need to know** | |
| **7.1** Limit access to system components and cardholder data to only those individuals whose job requires such access. | ♦ Access to financial networks is based on merchant-specific identifiers, customer numbers and security codes<br>♦ Access to bluezone web-based administration consoles is granted by role membership and permissions |
| **7.2** Establish an access control system for system components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. | ♦ Includes industry-standard authentication and authorization services integrated with a centralized LDAP security store<br>♦ Access privileges are assigned based on the granted business roles<br>♦ Each bluezone component is secured as "deny all" and independent of others<br>♦ Integration with external financial networks is configured to fail unless access credentials are installed and present sufficient privileges |
| **7.3** Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties. | ♦ Product documentation and operational policies and procedures for the hosted service are available for distribution to the authorized personnel |
| **8 Identify and authenticate access to system components** | |
| **8.1** Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components. | ♦ Each client/partner system and administrative user is assigned a unique ID<br>♦ User ID/credential management is governed by the documented procedures<br>♦ Access to terminated systems and end-users can be revoked in real-time<br>♦ Administrative access is available only on demand as authorized<br>♦ Session management controls expire inactive access |

| PCI DSS Requirement | Capabilities and Benefits |
|---|---|
| **8.2** In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of: something that you know, something that you have, and something that you are. | ♦ All passwords and key phrases are transmitted over secure protocols<br>♦ Access credentials are issued based on the initial identity validation<br>♦ New passwords are checked for various strength characteristics<br>♦ Includes password policy management, such as locking, matching and aging<br>♦ Temporary end-user passwords require reset at the initial use |
| **8.3** Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance). | ♦ Remote access by administrative users requires two-factor authentication integrated with the centralized security store |
| **8.4** Document and communicate authentication policies and procedures to all users. | ♦ Password management policies are documented on per bluezone instance<br>♦ Digital certificate revocation lists ensure the expiry of system-level access |
| **8.5** Do not use group, shared, or generic IDs, passwords, or other authentication methods. | ♦ Generic or shared system IDs are not allowed throughout the environment<br>♦ Unique ID and credentials are used for each client/partner system |
| **8.6** Where other authentication mechanisms are used, they must be assigned to an individual account, with physical and/or logical controls to ensure only the intended account can use that mechanism to gain access. | ♦ Access privileges are granted based on the end-user authentication<br>♦ System IDs and credentials are provisioned based on the approval process<br>♦ Administrative access is tied to an individual part of the operational team |
| **8.7** All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted. | ♦ Direct access to cardholder data by individual end-users is prohibited<br>♦ A "zero retention" tokenization method does not store cardholder data<br>♦ With the persistence based tokenization option, direct access to digital vault is not allowed; only secure programmatic retrieval of cardholder data is in effect |
| **8.8** Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties | ♦ Product documentation and operational policies and procedures for the hosted service are available for distribution to the authorized personnel |
| **9 Restrict physical access to cardholder data** | |
| **9.1** Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. | ♦ Physical access to a hosted service is subject to the data center procedures, which include: system-level ticketing, facility entry via authorization by the onsite security personnel, HID cards, PIN entry and biometric devices<br>♦ Facility entrance/exit points are monitored by surveillance cameras 24 × 7 |
| **9.2** Develop procedures to easily distinguish between onsite personnel and visitors. | ♦ Each visitor of a data center facility is required to wear a daily badge issued at the security desk prior to entering the hosting premises<br>♦ Permanent onsite technicians are required to wear a uniform |
| **9.3** Control physical access for onsite personnel to sensitive areas. | ♦ Access to a bluezone cage is protected with a pinpad and biometric device<br>♦ Access to a bluezone cabinet is protected with a PIN-entry lock<br>♦ Client personnel are allowed access only to their specific cabinet |
| **9.4** Implement procedures to identify and authorize visitors. | ♦ Unescorted visitor access to a bluezone data center facility is prohibited<br>♦ Visitor logs are maintained for over 3 months, with an on-demand inspection |
| **9.5** Physically secure all media. | ♦ Unauthorized external backups of encrypted cardholder data are not allowed |
| **9.6** Maintain strict control over the internal or external distribution of any kind of media. | ♦ Sending digital media, with encrypted cardholder data or otherwise, outside of the data center facility is prohibited<br>♦ Any relocation of a bluezone instance is subject to an approval process |

| PCI DSS Requirement | Capabilities and Benefits |
|---|---|
| **9.7** Maintain strict control over the storage and accessibility of media. | ♦ Digital media is subject to inventory part of the bluegrid engineering<br>♦ Annual reviews of digital media capture any storage capacity changes |
| **9.8** Destroy media when it is no longer needed for business or legal reasons. | ♦ Encrypted cardholder data on disk is rendered unrecoverable prior to hardware disposal in case of service decommissioning or device repairs |
| **9.10** Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties. | ♦ Data center operational policies and procedures for the hosted service are available for distribution to the authorized personnel |
| **Regularly Monitor and Test Networks** | |
| **10 Track and monitor all access to network resources and cardholder data** | |
| **10.1** Implement audit trails to link all access to system components to each individual user. | ♦ Access to bluezone components ensures audit trail to an individual user<br>♦ System IDs and digital certificates are issued to client/partner personnel based on the approval process and subject to revocation upon expiry |
| **10.2** Implement automated audit trails for all system components to reconstruct all individual accesses to cardholder data and other events. | ♦ Invalid logical access attempts are logged<br>♦ Initialization and destruction of audit trails is logged<br>♦ Creation and removal of all system-level objects is logged |
| **10.3** Record at least the following audit trail entries for all system components for each event: user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component or resource. | ♦ Supports all fields required by PCI DSS for audit trail<br>♦ Supports widely used common and combined access log formats, as well as pattern-based or other custom formats<br>♦ Log layout patterns are managed via configuration files<br>♦ Supports console, rolling file, e-mail and SYSLOG server logging targets |
| **10.4** Using time-synchronization technology, synchronize all critical system clocks and times to ensure critical systems have the correct and consistent time. | ♦ Includes a centralized NTP service which obtains time from designated, industry-accepted time sources<br>♦ Access to the time data is granted only to the trusted internal NTP clients |
| **10.5** Secure audit trails so they cannot be altered. | ♦ Includes a centralized SYSLOG service collecting audit trail logs<br>♦ Audit trail logs are protected from unauthorized access |
| **10.6** Review logs and security events for all system components to identify anomalies or suspicious activity. | ♦ Includes event management facility with an ability to monitor system security events and all access to cardholder data, and issue alerts upon violation<br>♦ Provides a web-based console for ad-hoc security log search and analysis |
| **10.7** Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived or restorable from backup). | ♦ All log files support live rollover based on time interval or size<br>♦ Audit trails can be configured for three-month immediate availability and one year restorable from log archives<br>♦ Longer retention periods are limited only by available disk space and your information security policies |
| **10.8** Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties. | ♦ Product documentation and operational policies and procedures for the hosted service are available for distribution to the authorized personnel |

PCI Solution Summary

# Limit the exposure of cardholder data within or outside your organization IT infrastructure.

A unique, innovative bluezone solution reduces the footprint of cardholder data, leaving only benign, non-sensitive customer information behind. A self-contained, engineered environment becomes your secure transport to the world, with privacy controls applied to credit and debit cards.

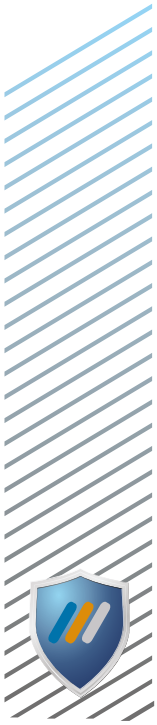
The solution allows you to centrally and uniformly manage all traffic of financial interest, whether it is exchanged between your partner organizations or with your clients involved in the automated transaction flow. In a secure, integrated bluezone environment you can quickly and safely manage your cardholder data with minimal administration and maintenance effort. As a result, the cost and timeline to meet your PCI compliance are reduced practically by an order of magnitude.

Such significant benefits have become possible due to a concept of capturing sensitive data at the network perimeter, preventing it from ever entering and "contaminating" the computing systems and network devices in your IT environment.

The encrypted and tokenized cardholder data is no longer in the scope of PCI DSS compliance audit, or at risk of being lost or compromised. The complex business processes and inter-connected information systems no longer require redesign.

In the era of cloud computing having evolved as a model for enabling ubiquitous and convenient access to a pool of digital resources, the bluezone solution managed to combine both elasticity of the cloud and security of financial data. A "zero trust" approach, where the so called "trusted network" no longer exists, was laid in the foundation of a small-footprint cardholder data environment with access to components strictly on a need-to-know basis.

In a nutshell, your applications and infrastructure have been eliminated from the exposure to cyber-threat. Those systems and processes remaining in the PCI DSS scope have been reduced to carefully engineered and validated portable cloud accessed securely regardless of who initiates the network communication and where it originates.




## Reliable, simple, affordable. Certified.

An instance of the zone is powered by bluegrid, the industry's first integrated security system engineered to address the complexity and cost of PCI, among other regulatory standards.

The compact, portable cloud service is based on a high-density component architecture covering network, servers, storage and applications which support large transaction volumes and carrier-grade communication throughput.

Every component of bluezone provides built-in redundancy to meet continuous service availability, fault tolerance and scalability for growth. PCI compliance is now simple and sustainable.

## Contact

Phone 1.888.414.5739
E-mail info@bluezonex.com
Web www.bluezonex.com

bluezone

10 Four Seasons Place, Fl. 10
Toronto, Ontario M9B 6H7