XYPRO®
Mission Critical Security

Payment Card Industry Data Security Standard

PCI DSS Version 3.2.1 to 4.0
Summary of Changes for HPE NonStop™ Systems

January 2023 v1.0

INTRODUCTION

PCI DSS Compliance and the HPE NonStop™ Systems

The Payment Card Industry Data Security Standard (PCI DSS) is a set of policies designed to protect cardholders against misuse of their personal information. The standard is widely adopted across the payment card industry. The entire PCI DSS standard can be found at https://www.pcisecuritystandards.org/.

This paper shows the changes from PCI DSS v3.2.1 to PCI DSS v4.0 and identifies items applicable to the HPE NonStop™ Server. Places where XYPRO solutions help comply with this standard are highlighted throughout.

PCI DSS v4.0 Application to HPE NonStop™ Systems

PCI DSS must be implemented by service providers and merchants to secure the cardholder data and its environment in an effective and consistent manner.

Because this standard must apply to a diverse array of service providers and merchants, which can range from multinational, multibillion-dollar organizations to small community banks and even smaller merchants, PCI DSS v4.0 requirements are stated as simply as possible, without specific details of how the goal of the standard is to be achieved. Note that this is a change from earlier versions of the standard, which were much more prescriptive. Also note that some of the new requirements apply immediately to v4.0 assessments while others are being treated as best practices until 31 March 2025.

The first step that any organization using HPE NonStop™ Systems should take in meeting these standards is to understand what has changed in version 4.0 and how those changes apply to their environment. The updates provide added flexibility in how an organization meets the standards when cutting-edge technologies have been implemented to address emerging threats. What does this mean for your organization?

While the 12 requirements remain the same overall, they include 64 new requirements and a new Customized Approach for implementing and validating PCI DSS.

A strongly recommended second step is to use **XYPRO's XYGATE SecurityOne Suite (XS1)** for HPE NonStop™ server monitoring. This security software suite, with its flexible and easy-to-use user interface, greatly assists in determining the differences between the current security configuration of a NonStop server system and those required to meet the security standards defined by PCI DSS v4.0.

In addition to this white paper, there are several resources to assist you in evaluating the next level of detail on compliance implementation. These include the HPE NonStop Security Hardening Guide and other HPE NonStop security white papers, individual product manuals, and the XYPRO books, *Securing Your HP NonStop Server: A Practical Handbook* (ISBN: 978-1555583149) and *Securing HP NonStop Servers In An Open Systems World: TCP/IP, OSS and SQL* (ISBN: 78-1555583446).

The following table gives an overview of the changes from PCI DSS v3.2.1 to PCI DSS v4.0, with an explanation of how **XYPRO's XYGATE SecurityOne Suite** and other XYGATE products help meet the compliance requirements for payment card applications in the NonStop Server areas of the enterprise.

PCI DSS SUMMARY OF CHANGES

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
Requirement 1 - Install and Maintain Network Security Controls			
Requirement 1- General		Updated principal requirement title to reflect the focus on "network security controls." Replaced "firewalls" and "routers" with "network security controls" to support a broader range of technologies used to meet the security objectives traditionally met by firewalls.	
1.1.5	1.1.2	Replaced requirement for "Description of groups, roles, and responsibilities for management of network components" with general requirement for roles and responsibilities for Requirement 1.	This requirement can be met with corporate policies, procedures, and documentation.
1.1	1.2.1	Refocused former "null" requirement (all content pointed to other requirements) on defining, implementing, and maintaining configuration standards for network security control rulesets.	Use ***XYGATE CMON*** to implement and maintain network security controls. Use ***IPTABLES*** to implement and maintain network security controls on Cluster IO Modules (CLIMs).
1.1.1	1.2.2	Clarified that changes are managed in accordance with the change control process defined at Requirement 6.5.1.	Use ***XYGATE SecurityOne Suite – Access Control and ServiceNow Integration*** for change control.
1.1.4		Removed redundant requirement.	Removed
1.1.6	1.2.5 1.2.6	Separated into two requirements to clarify intent of each.	This requirement can be met with corporate policies, procedures, and documentation.
1.1.7	1.2.7	Clarified the intent of reviewing configurations of network security controls at least once every six months.	This requirement can be met with corporate policies, procedures, and documentation.
1.2		Removed "null" requirement (all content pointed to other requirements).	Removed
1.2.2	1.2.8	Clarified the intent of securing configuration files.	Use ***XYGATE SecurityOne Suite - Access Control and ServiceNow Integration*** to provide configuration change control validation. Use ***XYGATE SecurityOne Suite - Object Security*** to provide strong object separation.
1.2.1 1.3.4	1.3.1 1.3.2	Separated Requirement 1.2.1. into two requirements to clarify the intent of each. Removed redundant Requirement 1.3.4.	U***se XYGATE User Authentication*** to restrict access by IP address.
1.2.3	1.3.3	Clarified the intent of implementing network security controls between wireless networks and the CDE.	This requirement involves network configuration external to the HPE NonStop System.

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
1.3	1.4.1	Refocused a former null requirement (all content pointed to other requirements). Clarified that the intent is to implement controls between trusted and untrusted networks.	This requirement involves network configuration external to the HPE NonStop System.
1.3.1 1.3.2 1.3.5	1.4.2	Merged requirements to clarify that the intent is to restrict inbound traffic from untrusted networks.	Use ***XYGATE User Authentication*** to restrict access by IP address. Use ***XYGATE Merged Audit*** to report on and manage audited events. Use ***IPTABLES*** to implement and maintain network security controls on Cluster IO Modules (CLIMs).
1.3.6	1.4.4	Clarified the intent is that system components storing cardholder data are not directly accessible from untrusted networks.	This requirement involves network configuration external to the HPE NonStop System.
1.4	1.5.1	Clarified that the intent is to implement security controls on any computing device that connects to both untrusted networks and the CDE.	This requirement involves network configuration external to the HPE NonStop System.
Requirement 2 - Apply Secure Configurations to All System Components			
Requirement 2 - General		Updated principal requirement title to reflect that the focus is on secure configurations in general, and not just on vendor-supplied defaults.	
	2.1.2	**New requirement** for roles and responsibilities. ***This requirement is effective immediately for all v4.0 assessments***	This requirement can be met with corporate policies, procedures, and documentation.
2.1	2.2.2	Clarified that the intent is to understand whether vendor default accounts are in use and to manage them accordingly.	Use ***XYGATE SecurityOne – File Integrity Monitor*** to monitor user accounts and passwords. Use ***XYGATE Password Quality*** to force system password changes.
2.2.1	2.2.3	Clarified the intent of the requirement for managing primary functions that require different security levels.	This requirement can be met with corporate policies, procedures, and documentation.
2.2.2 2.2.5	2.2.4	Combined requirements to align similar topics.	Use ***XYGATE SecurityOne Suite*** to monitor services in use. Use ***XYGATE Merged Audit*** to display audited events.
2.2.3	2.2.5	Clarified that the intent of the requirement is if any insecure services, protocols, or daemons are present.	This requirement can be met with corporate policies, procedures, and documentation.
2.1.1	2.3.1 2.3.2	Split requirement for changing all wireless vendor defaults into two requirements to clarify the focus of each.	This requirement involves network configuration external to the HPE NonStop System.
2.4	12.5.1	Moved requirement to align related content.	Use ***XYGATE SecurityOne Suite*** to inventory system components on the HPE NonStop that are in scope for PCI DSS.

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
2.6		Removed "null" requirement (all content pointed to other requirements).	Removed
Requirement 3 - Protect Stored Account Data			
Requirement 3 - General		Updated principal requirement title to reflect the focus on account data.	
	3.1.2	**New requirement** for roles and responsibilities. ***This requirement is effective immediately for all v4.0 assessments.***	This requirement can be met with corporate policies, procedures, and documentation.
3.1	3.2.1	**New requirement bullet** to address SAD stored prior to completion of authorization through implementation of data retention and disposal policies, procedures, and processes. ***This bullet is a best practice until 31 March 2025.***	This requirement can be met with corporate policies, procedures, and documentation.
	3.3.2	**New requirement** to encrypt SAD that is stored electronically prior to completion of authorization. ***This requirement is a best practice until 31 March 2025.***	Not applicable to the HPE NonStop System.
3.2.a 3.2.b	3.3.3	**New requirement** to address former testing procedures that any storage of SAD by issuers is limited to that which is needed for a legitimate issuing business need and is secured. ***This requirement is a best practice until 31 March 2025.***	This requirement can be met with corporate policies, procedures, and documentation.
3.3	3.4.1	Clarified that PAN is masked when displayed such that only personnel with a business need can see more than the BIN/last four digits of the PAN.	Masking to restrict PAN display to the minimum number of digits can be met with tools outside of the XYGATE product offering.
12.3.10	3.4.2	**New requirement** for technical controls to prevent copy and/or relocation of PAN when using remote-access technologies. Expanded from former Requirement 12.3.10. ***This requirement is a best practice until 31 March 2025.***	This requirement can be met with corporate policies, procedures, and documentation.
3.4	3.5.1	Removed pads from the "Index tokens and pads" bullet for rendering PAN unreadable.	Use ***XYGATE SecurityOne Suite – Access Control*** for PAN masking in audit logs. Use ***XYGATE Key Management*** and ***XYGATE File Encryption*** for strong cryptography & associated key management. Use ***NonStop Volume Level Encryption (VLE)*** to physically secure data at rest.
	3.5.1.1	**New requirement** for keyed cryptographic hashes when hashing is used to render PAN unreadable. ***This requirement is a best practice until 31 March 2025.***	Use ***XYGATE SecurityOne Suite – Access Control*** for PAN masking in audit logs. Use ***XYGATE Key Management*** and ***XYGATE File Encryption*** for strong cryptography & associated key management.

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
			Use ***NonStop Volume Level Encryption (VLE)*** to physically secure data at rest.
	3.5.1.2	**New requirement** that disk-level or partition-level encryption is used only to render PAN unreadable on removable electronic media or, if used on non-removable electronic media, the PAN is also rendered unreadable via a mechanism that meets Requirement 3.5.1. ***This requirement is a best practice until 31 March 2025***.	Use ***XYGATE SecurityOne Suite – Access Control*** to secure access to PAN data. Use ***XYGATE Key Management*** and ***XYGATE File Encryption*** for strong cryptography & associated key management. Use ***NonStop Volume Level Encryption (VLE)*** to physically secure data at rest.
3.5.1	3.6.1.1	**New requirement bullet for service providers only** to include in the documented description of the cryptographic architecture that use of the same cryptographic keys in production and test environments is prevented. ***This bullet is a best practice until 31 March 2025.***	This requirement can be met with corporate policies, procedures, and documentation.
Requirement 4 - Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks			
Requirement 4 - General		Updated principal requirement title to reflect the focus on "strong cryptography" to protect transmissions of cardholder data.	
	4.1.2	**New requirement** for roles and responsibilities. ***This requirement is effective immediately for all v4.0 assessments***.	This requirement can be met with corporate policies, procedures, and documentation.
4.1	4.2.1	**New requirement bullet** to confirm certificates used for PAN transmissions over open, public networks are valid and not expired or revoked. ***This bullet is a best practice until 31 March 2025.***	Use ***XYGATE Host Encryption*** and ***XYGATE Encryption Library File Encryption*** to encrypt all varieties of data transmission. Use the following HPE products available from HPE to comply with this requirement • ***NonStop SSH (+SFTP)*** • ***NonStop SSL (+FTPS)*** • ***NonStop IPSec*** • ***iTP Secure WebServer*** • ***NonStop HTTP Server*** • ***NonStop CORBA (TLS/SSL)*** • ***NonStop SOAP (TLS/SSL)*** • ***Java-based products*** • ***Open System Management (OSM)*** • ***MR-Win6530 (NSC)***
	4.2.1.1	**New requirement** to maintain an inventory of trusted keys and certificates. ***This requirement is a best practice until 31 March 2025***.	Use ***XYGATE SecurityOne Suite - Object Security*** to secure keys and certificates at the resource level.
Requirement 5 - Protect All Systems and Networks from Malicious Software			

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
Requirement 5 - General		Updated principal requirement title to reflect the focus on protecting all systems and networks from malicious software. Replaced “anti-virus” with “anti-malware” throughout to support a broader range of technologies used to meet the security objectives traditionally met by anti-virus software.	
	5.1.2	**New requirement** for roles and responsibilities. ***This requirement is effective immediately for all v4.0 assessments***.	This requirement can be met with corporate policies, procedures, and documentation.
5.1.2	5.2.3	Clarified requirement by changing focus to “system components that are not at risk for malware.”	Use ***XYGATE SecurityOne Suite*** to monitor changes to system components.
	5.2.3.1	**New requirement** to define the frequency of periodic evaluations of system components not at risk for malware in the entity’s targeted risk analysis. ***This requirement is a best practice until 31 March 2025***.	This requirement can be met with corporate policies, procedures, and documentation.
5.2	5.3.1 5.3.2 5.3.4	Split one requirement into three to focus each requirement on one area: • Keeping the malware solution current via automatic updates, • Performing periodic scans and active or real-time scans (with a new option for continuous behavioral analysis), • Generation of audit logs by the malware solution.	Use ***XYGATE SecurityOne – File Integrity Monitor*** to monitor for changes to subvolumes containing program files, such as $SYSTEM.SYSnn , to detect the introduction of possible malware and for continuous behavioral analysis and real-time scans.
	5.3.2.1	**New requirement** to define the frequency of periodic malware scans in the entity’s targeted risk *analysis.* ***This requirement is a best practice until 31 March 2025.***	This requirement can be met with corporate policies, procedures, and documentation.
	5.3.3	**New requirement** for a malware solution for removable electronic media. ***This requirement is a best practice until 31 March 2025***.	Use ***XYGATE SecurityOne Suite*** to monitor for the introduction of possible malware and for continuous behavioral analysis and real-time scans.
	5.4.1	**New requirement** to detect and protect personnel against phishing attacks. ***This requirement is a best practice until 31 March 2025***.	This requirement can be met with corporate policies, procedures, and documentation.
Requirement 6 - Develop and Maintain Secure Systems and Software			
Requirement 6 - General		Updated principal requirement title to include “software” rather than “applications.” Clarified that Requirement 6 applies to all system components, except for Requirement 6.2, which applies only to bespoke and custom software.	

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
	6.1.2	**New requirement** for roles and responsibilities. ***This requirement is effective immediately for all v4.0 assessments**.*	This requirement can be met with corporate policies, procedures, and documentation.
6.3	6.2.1	Moved requirement for developing software securely to align all software development content under Requirement 6.2.	This requirement can be met with corporate policies, procedures, and documentation.
6.3	6.2.1	Replaced “internal and external” with “bespoke and custom” software. Clarified that this requirement applies to software developed for or by the entity for the entity’s own use and does not apply to third-party software.	This requirement can be met with corporate policies, procedures, and documentation.
6.5	6.2.2	Moved the elements of Requirement 6.5 for training of software developers to align all software development content under Requirement 6.2. Clarified training requirements for software development personnel.	This requirement can be met with corporate policies, procedures, and documentation.
6.3.2	6.2.3 6.2.3.1	Moved requirement for reviewing custom software prior to release to align all software development content under Requirement 6.2. Split requirement to separate general code review practices from those needed if manual code reviews are performed.	This requirement can be met with corporate policies, procedures, and documentation.
6.5.1 – 6.5.10	6.2.4	Moved requirements for addressing common coding vulnerabilities to align all software development content under Requirement 6.2. Combined methods to prevent or mitigate common software attacks into a single requirement and generalized the language describing each type of attack.	This requirement can be met with corporate policies, procedures, and documentation.
6.1 6.2	6.3	Moved requirements for identifying security vulnerabilities and protecting system components from vulnerabilities via patching under Requirement 6.3.	This requirement can be met with corporate policies, procedures, and documentation.
6.1	6.3.1	Added a bullet to clarify applicability to vulnerabilities for bespoke and custom and third-party software.	This requirement can be met with corporate policies, procedures, and documentation.
	6.3.2	**New requirement** to maintain an inventory of bespoke and custom software. ***This requirement is a best practice until 31 March 2025**.*	This requirement can be met with corporate policies, procedures, and documentation.
6.6	6.4.1	Moved requirement for addressing new threats and vulnerabilities for public-facing web applications under Requirement 6.4.	This requirement can be met with corporate policies, procedures, and documentation.

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
	6.4.2	**New requirement** to deploy an automated technical solution for public-facing web applications that continually detects and prevents web-based attacks. This new requirement removes the option in Requirement 6.4.1 to review web applications via manual or automated application vulnerability assessment tools or methods. ***This requirement is a best practice until 31 March 2025***.	Use ***XYGATE SecurityOne Suite*** to monitor for changes to subvolumes containing program and application files to detect the introduction of possible malware and for continuous behavioral analysis and real-time scans. Use ***XYGATE SecurityOne – Appliance Sentry Monitor*** to monitor changes to CLIM program and application files. Use ***IPTABLES*** to implement and maintain network security controls on CLIMs.
	6.4.3	**New requirement** for management of all payment page scripts that are loaded and executed in the consumer's browser. ***This requirement is a best practice until 31 March 2025***.	Not Applicable to the HPE NonStop System.
6.3.1 6.4 6.4.1 – 6.4.6	6.5.1 – 6.5.6	Moved and combined requirements for changes to system components under Requirement 6.5.	Use ***XYGATE SecurityOne Suite*** to verify that change control mechanisms are in use. Use ***XYGATE SecurityOne Suite - Access Control and ServiceNow Integration*** to provide change control validation. Use ***XYGATE SecurityOne Suite - Object Security*** to provide strong object separation. Use ***XYGATE $CMON Process*** to control execution CPU resource allocation.
6.4	6.5.3 6.5.4 6.5.5 6.5.6	Removed requirement for specific documented procedures and added testing procedures to verify policies and procedures to each related requirement.	Use ***XYGATE SecurityOne Suite - Access Control*** to provide change control validation. Use ***XYGATE SecurityOne Suite - Object Security*** to provide strong object separation. Use ***XYGATE CMON*** to control execution CPU resource allocation.
6.4.1	6.5.3	Changed term from "development/test and production" to "production and pre-production" environments.	Use ***XYGATE SecurityOne Suite - Access Control*** to enforce access controls between pre-production and production systems.
6.4.2	6.5.4	Changed term from "development/test and production" to "production and pre-production" environments. Changed term "separation of duties" and clarified that separation of roles and functions between production and pre-production is intended to provide accountability so that only approved changes are deployed.	Use ***XYGATE SecurityOne Suite - Access Control and ServiceNow Integration*** to ensure that only reviewed and approved changes are deployed.
6.4.3	6.5.5	Changed term from "testing or development" to "pre-production" environments. Clarified that live PANs are not used in pre-production environments except where all applicable PCI DSS requirements are in place.	This requirement can be met with corporate policies, procedures, and documentation.

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
Requirement 7 - Restrict Access to System Components and Cardholder Data by Business Need to Know			
Requirement 7 – General		Updated principal requirement title to include system components and cardholder data.	
	7.1.2	**New requirement** for roles and responsibilities. ***This requirement is effective immediately for all v4.0 assessments.***	This requirement can be met with corporate policies, procedures, and documentation.
7.1	7.2.1 7.2.2 7.2.3	Removed requirement for specific documented procedures and added testing procedures to verify policies and procedures to each related requirement.	Use ***XYGATE SecurityOne Suite - Access Control*** to provide access by least privilege. Use ***XYGATE SecurityOne Suite - Object Security*** to limit access to objects to only authorized individuals. Use ***XYGATE Process Control*** to manage processes without granting individual access to objects. Use ***XYGATE User Authentication*** to enforce authentication controls.
7.1.1	7.2.1	Clarified requirement is about defining an access control model.	Use ***XYGATE SecurityOne Suite - Access Control*** to provide access by least privilege. Use ***XYGATE SecurityOne Suite - Object Security*** to limit access to objects to only authorized individuals. Use ***XYGATE Process Control*** to manage processes without granting individual access to objects. Use ***XYGATE User Authentication*** to enforce authentication controls.
7.1.2 7.1.3	7.2.2	Combined requirements for assigning access based on job classification and function, and least privileges.	Use ***XYGATE SecurityOne Suite - Access Control*** to provide access by least privilege. Use ***XYGATE SecurityOne Suite – Object Security*** to limit access to objects by authorized individuals only. Use ***XYGATE Process Control*** to manage processes without granting individual access to objects. Use ***XYGATE CMON*** to control execution CPU resource allocation.
7.1.4	7.2.3	Clarified requirement is about approval of required privileges by authorized personnel.	This requirement can be met with corporate policies, procedures, and documentation.
	7.2.4	**New requirement** for review of all user accounts and related access privileges. **This requirement is a best practice until 31 March 2025**.	The actual review can be met with corporate policies, procedures, and documentation Use ***XYGATE SecurityOne Suite - Access Control*** and ***XYGATE SecurityOne Suite - Object Security*** to provide the materials to be used in the review process.

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
	7.2.5	**New requirement** for assignment and management of all application and system accounts and related access privileges. **This requirement is a best practice until 31 March 2025**.	Use ***XYGATE SecurityOne Suite - Access Control*** to provide access by least privilege. Use ***XYGATE SecurityOne Suite - Object Security*** to provide strong object separation. Use ***XYGATE CMON*** to control execution CPU resource allocation.
	7.2.5.1	**New requirement** for review of all access by application and system accounts and related access privileges. **This requirement is a best practice until 31 March 2025**.	Use ***XYGATE SecurityOne Suite - Access Control*** to provide access by least privilege. Use ***XYGATE SecurityOne Suite - Object Security*** to limit access to objects to only authorized individuals.
8.7	7.2.6	Moved requirement since it aligns better with the content in Requirement 7.	Use ***XYGATE SecurityOne Suite - Access Control*** to provide access by least privilege. Use ***XYGATE SecurityOne Suite – Object Security*** to provide strong object separation. Use ***XYGATE $CMON Process*** to control execution CPU resource allocation.
7.2		Removed "null" requirement (all content pointed to other requirements).	Removed
Requirement 8 – Identify Users and Authenticate Access to System Components			
Requirement 8 – General		Standardized on terms "authentication factor" and "authentication credentials." Removed "non-consumer users" and clarified in the overview that requirements do not apply to accounts used by consumers (cardholders).	
		Removed note in overview that listed requirements that do not apply to user accounts with access to only one card number at a time to facilitate a single transaction and added that note to each related requirement.	
	8.1.2	**New requirement** for roles and responsibilities. ***This requirement is effective immediately for all v4.0 assessments***.	This requirement can be met with corporate policies, procedures, and documentation.
8.1.1	8.2.1	Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Use ***All XYGATE modules*** to address the risk posed by shared User IDs. Use ***XYGATE Safeguard Manager*** to administer User IDs. Use ***XYGATE SecurityOne Suite*** to monitor and provide security alerts.
8.5	8.2.2	Changed focus of requirement to allow use of shared authentication credentials, but only on an exception basis.	Use ***All XYGATE modules*** to address the risk posed by shared User IDs.

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
		Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Use ***XYGATE SecurityOne Suite – Access Control*** to provide keystroke logging to attribute every action to an individual user.
8.5 8.5.1	8.2.2 8.2.3	Moved requirements for group, shared, or generic accounts and for service providers with remote access to customer premises under Requirement 8.2.	Use ***All XYGATE modules*** to address the risk posed by shared User IDs
8.1.8	8.2.8	Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Use ***XYGATE SecurityOne Suite – Access Control*** to enforce re-authentication of privileged sessions.
8.2	8.3.1	Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Use ***XYGATE User Authentication*** configured with LDAP or RSA for user authentication. Use ***XYGATE SecurityOne Suite - Access Control*** for timeout management. Use ***XYGATE Password Quality*** for password complexity rule enforcement.
8.1.6 8.1.7	8.3.4	Merged requirements and moved under Requirement 8.3 Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. Increased the number of invalid authentication attempts before locking out a user ID from six to 10 attempts.	Use ***XYGATE User Authentication*** to enforce lockout of failed authentication attempts.
8.2.6	8.3.5	Clarified that this requirement applies only if passwords/passphrases are used as an authentication factor to meet Requirement 8.3.1.	Use ***XYGATE Safeguard Manager*** *and* ***XYGATE Identity Connector for CyberArk*** to administer passwords. Use ***XYGATE Password Quality*** *and* ***XYGATE Identity Connector for CyberArk*** to enforce password complexity rules.
8.2.3	8.3.6	**New requirement** to increase password length from a minimum length of seven characters to minimum length of 12 characters (or if the system does not support 12 characters, a minimum length of eight characters). ***This requirement is a best practice until 31 March 2025***. Clarified that, until **31 March 2025**, passwords must be a minimum length of at least seven characters in accordance with v3.2.1 Requirement 8.2.3. Clarified that this requirement applies only if passwords/passphrases are used as an authentication factor to meet Requirement 8.3.1. Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Use ***XYGATE Password Quality*** *and* ***XYGATE Identity Connector for CyberArk*** to enforce password complexity rules.

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
8.2.5	8.3.7	Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Use ***XYGATE User Authentication*** to prompt for password change. Use ***XYGATE Password Quality*** *and* ***XYGATE Identity Connector for CyberArk*** to administer password policies**.**
8.4	8.3.8	Moved content about communicating user authentication policies and procedures under Requirement 8.3.	This requirement can be met with corporate policies, procedures, and documentation.
8.2.4	8.3.9	Clarified that this requirement applies only if passwords/passphrases are used as an authentication factor to meet Requirement 8.3.1. Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. Added a note that requirement does not apply to service providers' customer accounts but does apply to accounts for service provider personnel.	Use ***XYGATE SecurityOne Suite*** to analyze user accounts and passwords dynamically. Use ***XYGATE User Authentication*** to prompt for password change. Use ***XYGATE Password Quality*** to administer password changes. Use ***XYGATE Identity Connector*** to manage passwords at the enterprise level.
		Added the option to determine access to resources automatically by dynamically analyzing the security posture of accounts, instead of changing passwords/passphrases at least once every 90 days.	Use ***XYGATE SecurityOne Suite*** to analyze user accounts and passwords dynamically.
8.2.4.b	8.3.10	Moved content from a former testing procedure to a requirement for service providers to provide guidance to customers about changing passwords/ passphrases. Added a note that this requirement will be superseded by Requirement 8.3.10.1 once Requirement 8.3.10.1 becomes effective.	This requirement can be met with corporate policies, procedures, and documentation.
	8.3.10.1	**New requirement for service providers only** – if passwords/passphrases are the only authentication factor for customer user access, then passwords/passphrases are either changed at least once every 90 days or access to resources is automatically determined by dynamically analyzing the security posture of the accounts. ***This requirement is a best practice until 31 March 2025***. Added a note that this requirement does not apply to accounts of consumer users accessing their payment card information. Added a note that this requirement will supersede Requirement 8.3.10 once it becomes effective, and until that date, service providers may meet either Requirement 8.3.10 or 8.3.10.1.	Use ***XYGATE SecurityOne Suite*** to analyze user accounts and passwords dynamically. Use ***XYGATE User Authentication*** to prompt for password change. Use ***XYGATE Password Quality*** to administer password change. Use ***XYGATE Identity Connector*** to manage passwords at the enterprise level.

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
8.6	8.3.11	Moved requirement about authentication factors such as physical or logical security tokens, smart cards, and certificates under Requirement 8.3.	Use ***XYGATE User Authentication*** to ensure only the intended user can use the token or certificate to gain access.
8.3		Removed "null" requirement (all content pointed to other requirements).	Removed
	8.4.2	**New requirement** to implement multi-factor authentication (MFA) for all access into the CDE. ***This requirement is a best practice until 31 March 2025***. Added a note to clarify that MFA is required for both types of access specified in Requirements 8.4.2 and 8.4.3; and that applying MFA to one type of access does not replace the need to apply another instance of MFA to the other type of access.	Use ***XYGATE User Authentication*** and the ***XYGATE User Authentication App MFA Add-on*** to enable MFA for both direct and remote access to systems and applications.
	8.5.1	**New requirement** for secure implementation of multi-factor authentication systems. ***This requirement is a best practice until 31 March 2025***.	This requirement can be met with corporate policies, procedures, and documentation.
	8.6.1	**New requirement** for management of system or application accounts that can be used for interactive login. ***This requirement is a best practice until 31 March 2025***.	Use ***XYGATE SecurityOne Suite*** to assess authentication and access control information. Use ***XYGATE SecurityOne Suite*** - ***Access Control*** to provide timeout management. Use ***XYGATE SecurityOne Suite - Access Control and ServiceNow Integration*** to validate access requests. Use ***XYGATE User Authentication*** to manage user authentication methods. Use ***XYGATE Password Quality*** to enforce password complexity rules.
	8.6.2	**New requirement** for not hard-coding passwords/passphrases into files or scripts for any application and system accounts that can be used for interactive login. ***This requirement is a best practice until 31 March 2025***.	This requirement can be met with corporate policies, procedures, and documentation.
	8.6.3	**New requirement** for protecting passwords/passphrases for application and system accounts against misuse. ***This requirement is a best practice until 31 March 2025***.	Use ***XYGATE Password Quality*** to administer and enforce mandatory password changes and complexity.

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
8.7	7.2.6	Moved requirement since it aligns better with the content in Requirement 7.	Use ***XYGATE SecurityOne Suite - Access Control*** to provide action control. Use ***XYGATE SecurityOne Suite - Object Security*** to access to objects by authorized individuals only. Use ***XYGATE Merged Audit*** to display audit details. Use ***XYGATE Report Manager*** to report on audit logs.
Requirement 9 - Restrict Physical Access to Cardholder Data			
Requirement 9 – General		In the overview, clarified the three different areas covered in Requirement 9 (sensitive areas, CDE, and facilities). Throughout, clarified whether each requirement applies to the CDE, sensitive areas, or facilities.	Not Applicable to the HPE NonStop System.
Requirement 10 - Log and Monitor All Access to System Components and Cardholder Data			
Requirement 10 – General		Updated principal requirement title to reflect focus on audit logs, system components, and cardholder data. Clarified that these requirements do not apply to user activity of consumers (cardholders). Replaced “Audit trails” with “Audit logs” throughout.	
	10.1.2	**New requirement** for roles and responsibilities. ***This requirement is effective immediately for all v4.0 assessments***.	This requirement can be met with corporate policies, procedures, and documentation.
10.2		Removed “null” requirement (all content pointed to other requirements).	Removed
10.5		Removed “null” requirement (all content pointed to other requirements).	Removed
10.5.1 – 10.5.5	10.3.1 – 10.3.4	Moved audit log protection requirements under Requirement 10.3.	Use ***XYGATE SecurityOne Suite - Object Security*** to limit access to log files. Use ***XYGATE Merged Audit*** to facilitate audit log inspection. Use ***XYGATE Report Manager*** to report on audit logs.
10.5.3 10.5.4	10.3.3	Combined requirements to align similar topics.	Use ***XYGATE Merged Audit*** to facilitate audit log inspection. Use ***XYGATE Report Manager*** to report on audit logs.
10.6		Removed “null” requirement (all content pointed to other requirements).	Removed

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
10.6.1 – 10.6.3	10.4.1 – 10.4.3	Moved requirements for audit log reviews under Requirement 10.4.	Use ***XYGATE Merged Audit*** to facilitate audit log inspection. Use ***XYGATE Report Manager*** to report on audit logs.
	10.4.1.1	**New requirement** for the use of automated mechanisms to perform audit log reviews. ***This requirement is a best practice until 31 March 2025***.	Use ***XYGATE Merged Audit*** to send messages to a SIEM and to alert on specified activities. Use ***XYGATE SecurityOne Suite*** to monitor audit logs, alert on specified activities and send messages to a SIEM.
	10.4.2.1	**New requirement** for a targeted risk analysis to define the frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) ***This requirement is a best practice until 31 March 2025***.	This requirement can be met with corporate policies, procedures, and documentation.
10.7	10.5.1	Moved requirement for audit log history to 10.5.1.	Use ***XYGATE Merged Audit*** to facilitate audit log inspection.
10.4 10.4.1 – 10.4.3	10.6.1 – 10.6.3	Moved and reorganized requirements for time synchronization under 10.6.	Time synchronization can be met with tools outside of the XYGATE product offering.
10.8	10.7.1	Moved requirement *for service providers* to detect, alert, and promptly address failures of critical control systems to Requirement 10.7.1.	This requirement can be met with corporate policies, procedures, and documentation.
	10.7.2	**New requirement** for all entities to detect, alert, and promptly address failures of critical security control systems. ***This requirement is a best practice until 31 March 2025***. This new requirement applies to all entities – it includes two additional critical security controls not included in Requirement 10.7.1 for service providers.	This requirement can be met with corporate policies, procedures, and documentation.
10.8.1	10.7.3	**New requirement** to respond promptly to failures of any critical security controls. For service providers: this is current PCI DSS v3.2.1 requirement. For all other (non-service provider) entities: this is a new requirement. ***This requirement is a best practice (for non-service providers) until 31 March 2025***.	This requirement can be met with corporate policies, procedures, and documentation.
Requirement 11 - Test Security of Systems and Networks Regularly			
Requirement 11 – General		Minor update to principal requirement title.	

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
	11.1.2	**New requirement** for roles and responsibilities. ***This requirement is effective immediately for all v4.0 assessments***.	This requirement can be met with corporate policies, procedures, and documentation.
11.1	11.2.1	Clarified the intent of the requirement is to manage both authorized and unauthorized wireless access points. Clarified that this requirement applies even when a policy exists to prohibit the use of wireless technology.	Wireless monitoring can be met with tools outside of the XYGATE product offering.
	11.3.1.1	**New requirement** to manage all other applicable vulnerabilities (those not ranked as high-risk or critical) found during internal vulnerability scans. ***This requirement is a best practice until 31 March 2025***.	This requirement can be met with corporate policies, procedures, and documentation.
	11.3.1.2	**New requirement** to perform internal vulnerability scans via authenticated scanning. ***This requirement is a best practice until 31 March 2025***.	Use ***XYGATE SecurityOne Suite - Appliance Sentry Module*** for HPE NonStop Console and CLIM scanning.
11.2.3	11.3.1.3 11.3.2.1	Separated requirement to perform internal and external vulnerability scans and rescans after any significant changes into a requirement for internal scans (11.3.1.3) and external scans (11.3.2.1).	Vulnerability scanning can be met with tools outside of the XYGATE product offering.
11.3	11.4.1	Clarified the following: The methodology is defined, documented, and implemented by the entity. • Penetration testing results are retained for at least 12 months. The methodology includes a documented approach to assessing and addressing risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. The meaning of testing from inside the network (internal penetration testing) and from outside the network (external penetration testing).	This requirement can be met with corporate policies, procedures, and documentation.
11.3.3	11.4.4	Clarified that penetration test findings are corrected in accordance with the entity's assessment of the risk posed by the security issue.	This requirement can be met with corporate policies, procedures, and documentation.
	11.4.7	**New requirement for multi-tenant service providers** to support their customers for external penetration testing. ***This requirement is a best practice until 31 March 2025***.	This requirement can be met with corporate policies, procedures, and documentation.

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
	11.5.1.1	**New requirement for service providers** to use intrusion-detection and or intrusion-prevention techniques to detect, alert on/prevent, and address covert malware communication channels. ***This requirement is a best practice until 31 March 2025***.	Intrusion prevention can be met with tools outside of the XYGATE product offering.
	11.6.1	**New requirement** to deploy a change-and-tamper-detection mechanism to alert for unauthorized modifications to the HTTP headers and contents of payment pages as received by the consumer browser. ***This requirement is a best practice until 31 March 2025***.	This requirement can be met with corporate policies, procedures, and documentation.
11.2		Removed "null" requirement (all content pointed to other requirements).	Removed
11.1.2	12.10.5	Moved requirement for incident response procedures if unauthorized wireless access points are detected to align with other incident response items.	This requirement can be met with corporate policies, procedures, and documentation.
11.5.1	12.10.5	Moved requirement to respond to alerts generated by the change-detection solution to align with other incident response items.	Use ***XYGATE SecurityOne Suite*** to monitor and alert on incidents. Use ***XYGATE Merged Audit*** to display and alert on audited events.
Requirement 12 - Support Information Security with Organizational Policies and Programs			
Requirement 12 - General		Updated principal requirement title to reflect that the focus is on organizational policies and programs that support information security.	
12.2		Removed requirement for a formal organization-wide risk assessment and replaced with specific targeted risk analyses (12.3.1 and 12.3.2).	Removed
12.4	12.1.3	Added formal acknowledgment by personnel of their responsibilities.	This requirement can be met with corporate policies, procedures, and documentation.
12.5 12.5.1 – 12.5.5	12.1.4	Clarified that responsibilities are formally assigned to a Chief Information Security Officer or other knowledgeable member of executive management. Merged requirements for formally assigning responsibility for information security.	This requirement can be met with corporate policies, procedures, and documentation.

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
12.3 12.3.1 – 12.3.9	12.2.1	Clarified the intent of the requirement is for acceptable use policies for end-user technologies. Merged and removed requirements to focus on explicit management approval, acceptable uses of technologies, and a list of hardware and software products approved by the company for employee use.	This requirement can be met with corporate policies, procedures, and documentation.
12.3.10	3.4.2	Removed requirement and added new Requirement 3.4.2 for technical controls to prevent copy and/or relocation of PAN when using remote-access technologies.	This requirement can be met with corporate policies, procedures, and documentation.
	12.3.1	**New requirement** to perform a targeted risk analysis for any PCI DSS requirement that provides flexibility for how frequently it is performed. ***This requirement is a best practice until 31 March 2025***.	This requirement can be met with corporate policies, procedures, and documentation.
	12.3.2	**New requirement for entities using a Customized Approach** to perform a targeted risk analysis for each PCI DSS requirement that the entity meets with the customized approach. ***This requirement is effective immediately*** *for all entities undergoing a v4.0 assessment and using a customized approach.*	This requirement can be met with corporate policies, procedures, and documentation.
	12.3.3	**New requirement** to document and review cryptographic cipher suites and protocols in use at least once every 12 months. ***This requirement is a best practice until 31 March 2025***.	This requirement can be met with corporate policies, procedures, and documentation.
	12.3.4	**New requirement** to review hardware and software technologies in use at least once every 12 months. ***This requirement is a best practice until 31 March 2025***.	This requirement can be met with corporate policies, procedures, and documentation.
12.11 12.11.1	12.4.2 12.4.2.1	Moved requirements for reviews to confirm that personnel are performing PCI DSS tasks in accordance with policies and procedures under Requirement 12.4, to align with other requirements for managing PCI DSS compliance activities.	This requirement can be met with corporate policies, procedures, and documentation.
2.4	12.5.1	Moved under Requirement 12.5 to align with other requirements for documenting and validating PCI DSS scope.	Use ***XYGATE SecurityOne Suite*** to inventory system components on the HPE NonStop that are in scope for PCI DSS.
	12.5.2	**New requirement** to document and confirm PCI DSS scope at least every 12 months and upon significant change to the in-scope environment. ***This requirement is effective immediately for all v4.0 assessments***.	This requirement can be met with corporate policies, procedures, and documentation.

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
	12.5.2.1	**New requirement for service providers** to document and confirm PCI DSS scope at least once every six months and upon significant change to the in-scope environment. ***This requirement is a best practice until 31 March 2025***.	This requirement can be met with corporate policies, procedures, and documentation.
	12.5.3	**New requirement for service providers** for a documented review of the impact to PCI DSS scope and applicability of controls upon significant changes to organizational structure. ***This requirement is a best practice until 31 March 2025***.	Use ***XYGATE SecurityOne Suite*** for on-demand monitoring of all systems, objects and users after significant organizational changes.
12.6	12.6.1	Clarified that the intent is that all personnel are aware of the entity's information security policy and their role in protecting cardholder data.	This requirement can be met with corporate policies, procedures, and documentation.
	12.6.2	**New requirement** to review and update (as needed) the security awareness program at least once every 12 months. ***This requirement is a best practice until 31 March 2025***.	This requirement can be met with corporate policies, procedures, and documentation.
12.6.1 12.6.2	12.6.3	Merged requirements for security awareness training.	This requirement can be met with corporate policies, procedures, and documentation.
	12.6.3.1	**New requirement** for security awareness training to include awareness of threats and vulnerabilities that could impact the security of the CDE. ***This requirement is a best practice until 31 March 2025***.	This requirement can be met with corporate policies, procedures, and documentation.
	12.6.3.2	**New requirement** for security awareness training to include awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1. ***This requirement is a best practice until 31 March 2025.***	This requirement can be met with corporate policies, procedures, and documentation.
12.8		Removed "null" requirement (all content pointed to other requirements).	Removed
12.8.1 – 12.8.5	12.8.1 – 12.8.5	Replaced "Service Provider" with Third-Party Service Provider (TPSP). Clarified that the use of a PCI DSS compliant TPSP does not make an entity PCI DSS compliant, nor does it remove the entity's responsibility for its own PCI DSS compliance.	This requirement can be met with corporate policies, procedures, and documentation.
12.8.2	12.8.2	Replaced "Service Provider" with Third-Party Service Provider (TPSP).	This requirement can be met with corporate policies, procedures, and documentation.
12.8.3	12.8.3	Replaced "Service Provider" with Third-Party Service Provider (TPSP).	This requirement can be met with corporate policies, procedures, and documentation.

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
12.8.4	12.8.4	Replaced "Service Provider" with Third-Party Service Provider (TPSP). Clarified that where an entity has an agreement with a TPSP for meeting PCI DSS requirements on behalf of the entity, the entity must work with the TPSP to make sure the applicable PCI DSS requirements are met. If the TPSP does not meet those applicable PCI DSS requirements, then those requirements are also "not in place" for the entity.	This requirement can be met with corporate policies, procedures, and documentation.
12.8.5	12.8.5	Replaced "Service Provider" with Third-Party Service Provider (TPSP). Clarified that the information about PCI DSS requirements managed by the TPSP and the entity should include any that are shared between the TPSP and the entity.	This requirement can be met with corporate policies, procedures, and documentation.
	12.9.2	**New requirement for service providers** to support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5. ***This requirement is effective immediately for all v4.0 assessments***.	This requirement can be met with corporate policies, procedures, and documentation.
12.10		Removed "null" requirement (all content pointed to other requirements).	Removed
12.10.1	12.10.1	Replaced "system breach" and "compromise" with "suspected or confirmed security incident."	This requirement can be met with corporate policies, procedures, and documentation.
12.10.3	12.10.3	Replaced "alerts" with "suspected or confirmed security incidents."	This requirement can be met with corporate policies, procedures, and documentation.
12.10.4	12.10.4	Replaced "system breach" with "suspected or confirmed security incidents."	This requirement can be met with corporate policies, procedures, and documentation.
	12.10.4.1	**New requirement** to perform a targeted risk analysis to define the frequency of periodic training for incident response personnel. ***This requirement is a best practice until 31 March 2025***.	This requirement can be met with corporate policies, procedures, and documentation.
12.10.5 11.1.2 11.5.1	12.10.5	Merged requirements and updated the security monitoring systems to be monitored and responded to as part of the incident response plan to include the following: • Detection of unauthorized wireless access points (former 11.1.2), • Change-detection mechanism for critical files (former 11.5.1), **New requirement bullet** for use of a change- and tamper-detection mechanism for payment pages (relates to new requirement 11.6.1). ***This bullet is a best practice until 31 March 2025.***	Use ***XYGATE SecurityOne Suite*** to monitor file integrity and alert on changes to critical files. Use ***XYGATE SecurityOne Suite - Access Control and ServiceNow Integration*** for change control.

v3.2.1	v4.0	Description of Change	How to Comply on HPE NonStop™
	12.10.7	**New requirement** for incident response procedures to be in place and initiated upon detection of stored PAN anywhere it is not expected. ***This requirement is a best practice until 31 March 2025*.**	This requirement can be met with corporate policies, procedures, and documentation.

This document contains confidential and/or legally privileged information. It is intended for XYPRO Technology Corporation, Channel Partner and HPE NonStop Systems Customer Use only. If you are not an intended recipient as identified on the front cover of this document, you are strictly prohibited from reviewing, redistributing, disseminating, or in any other way using or relying on the contents of this document.

January 2023