Witham Laboratories

Building confidence in payment systems

Knightcraft Technology
Information Security Consultants

A Witham Laboratories (QSA) and Knightcraft Technology White Paper

PCI DSS Compliance for HP NonStop Servers

PCI DSS Version 1.2.1

Document Version 1.0 (US Letter Format)

23rd September 2010

CONTENTS

TRADEMARK ACKNOWLEDGEMENTS

The following are trademarks or service marks of Hewlett-Packard Company:

NonStop Kernel	NonStop SQL	PATHCOM	SCF
Enscribe	Event Management Service (EMS)	SAFECOM	SPOOLCOM
Guardian	Distributed System Management (DSM)	NETBATCH	FUP
PATHWAY	SAFEGUARD	TACL	NonStop

The following are trademarks or service marks of XYPRO Technology Corporation:

XYGATE Password Quality (XPQ)
XYGATE Safeguard Manager (XSM)
XYGATE Security Compliance Wizard (XSW)
XYGATE File Encryption (XFE)
XYGATE Key Manager (XKM)
XYGATE Access Control (XAC)
XYGATE Safeguard Reports (XSR)
XYGATE Merged Audit (XMA)
XYGATE Process Control (XPC)
XYGATE Object Security (XOS)
XYGATE Host Encryption (XHE)
XYGATE CMON (XCM)
XYGATE User Authentication (XUA)
XYGATE Encryption Library (XEL)
XYGATE Report Manager (XRM)
XYGATE Master Installer (XMI)
XYGATE
XYPRO

The following are trademarks or service marks of ACI Worldwide:

BASE24 BASE24-eps

The following are trademarks or service marks of Fidelity National Information Services, Inc:

CONNEX

The following are trademarks or service marks of Oracle Corporation:

GoldenGate

The following are trademarks or service marks of Network Technologies International, Inc.:

DRNet

The following are trademarks or service marks of Gravic, Inc.:

Shadowbase

The following are trademarks or service marks of EMC Corporation:

RSA enVision ACE/Server SecurId

All other brand or product names, trademarks or registered trademarks are acknowledged as the property of their respective owners.

PCI Security Standards Council, LLC (the Council) is the owner of the copyright of the material known as PCI Data Security Standards (PCI DSS). PCI DSS is the exclusive property of the Council.

COPYRIGHT

INTRODUCTION

Many HP NonStop™ Servers are used for processing payment card transactions and as such are subject to the Payment Card Industry (PCI) Data Security Standard (DSS). The PCI DSS sets forth twelve categories of requirements related to system and network security, encryption of data and auditing of user access and actions. It details not only requirements that must be achieved through configuration, but also specifies documentation and procedural requirements that must be adhered to in order to be compliant with the standard.

This document provides guidance for addressing PCI DSS compliance in relation to an HP NonStop server. A summary of the standard is provided for each section along with recommendations that address the various requirements. A matrix is provided for each section, giving an indication of what a QSA will likely require during a PCI DSS assessment for the individual sub requirements.

Witham Laboratories is an independent PCI QSA Company and as such does not endorse any specific commercial product. Furthermore, Witham Laboratories does not receive any material gain from any product that our clients choose to implement to assist with PCI DSS compliance or system security in general.

In cases where compliance cannot be easily or readily achieved using standard HP NonStop tools, this document illustrates how compliance can be assisted by use of XYGATE® security and auditing software. Organizations should consider implementing XYGATE or a similar solution where requirements cannot be achieved using standard HP NonStop tools such as Guardian or Safeguard.

This document includes recommendations only as they relate to the HP NonStop server. Sections that do not typically relate to the NonStop are included for completeness, but are marked as Not Applicable. To achieve PCI DSS compliance, an organization must address all of the requirements.

DISCLAIMER

This paper reflects the opinions and recommendations of the authors only and does not in any way represent the views or endorsements of Hewlett-Packard, XYPRO Technology Corporation, PCI Security Standards Council or any other organization.

This document is a guide to assist you in your compliance efforts and should be treated as a guide only. It does not guarantee that you will necessarily be compliant by following the recommendations herein. You should seek professional advice to determine your organization's specific situation and exactly what needs to be done for your organization to achieve compliance. Your status in regards to PCI DSS compliance will ultimately be determined by your QSA.

FEEDBACK

While best efforts have been made by the authors to ensure technical accuracy, the software industry is renowned for the speed at which new and innovative ways for achieving goals emerge and are implemented. Industries change and products change accordingly.

We will be endeavoring to keep this document as up to date as possible, taking in any changes to the PCI DSS specification and changes in regards to NonStop platform software.

We welcome your feedback. If you have any comments, corrections or suggestions for inclusion in the next version of the document, please submit feedback at http://www.knightcraft.com.

PCI DSS VERSION

This document applies to PCI DSS version 1.2.1, July 2009. The full specification can be obtained from the PCI SSC website at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

The PCI SSC website contains a number of other documents that may be helpful in interpreting the PCI DSS specification. These supporting documents are located at https://www.pcisecuritystandards.org/security_standards/pci_dss_supporting_docs.shtml.

PCI DSS version 2.0 is scheduled for publication on 28 October 2010. Note that this document will be updated in accordance with updates to the PCI DSS specification and subscriber feedback.

Please go to www.knightcraft.com to download the latest version of this document or to provide feedback.

USEFUL REFERENCES

- HP NonStop Technical Library (http://h20000.www2.hp.com/bizsupport/TechSupport/Product.jsp?lang=en&cc=us&taskId=101&contentType=SupportManual&docIndexId=64255&prodTypeId=15351&prodCatId=407843)
- *HP NonStop Server Security- A Practical Handbook*, by XYPRO Technology Corporation (ISBN: 1-55558-314-8)
- *Securing HP NonStop Servers in an Open Systems World*, by XYPRO Technology Corporation (ISBN: 1-55558-344-X)

For the full list of resources used by the authors in writing this document, please see the Resources section.

INTENDED AUDIENCE

The intended audience for this document is as follows:

- Technical or security personnel responsible for ensuring that the applicable HP NonStop server environments within an organization satisfy PCI DSS compliance.
- QSAs responsible for performing PCI DSS compliance assessments on organizations that use HP NonStop servers for processing, storing or transmitting payment card data.
- Auditors of HP NonStop servers looking for technical information on security of HP NonStop servers.
- Technical or security personnel looking to improve security and auditability of their HP NonStop servers, even if they operate in an environment that is not subject to PCI DSS.

THE AUTHORS

Greg Swedosh is a Senior Security Consultant and the owner of **Knightcraft Technology**, who specialize in providing security, audit and compliance consultancy services for the HP NonStop (Tandem) Server platform. Knightcraft Technology is also a distributor of XYGATE software and a part of the XYPRO Technology Corporation support team. Greg is a co-author of the book *Securing HP NonStop Servers in an Open Systems World* and has presented in a number of countries on security for the HP NonStop server platform. [Website: www.knightcraft.com].

Dr. Sajal Islam is a Senior Security Engineer with **Witham Laboratories**, and a leading independent consultant in information security with specialist expertise in the payments sector. Witham Laboratories is certified by PCI as a Qualified Security Assessor Company, PA QSA company, an Approved Scanning Vendor (ASV) and is one of only eight laboratories around the world that is accredited to assess devices against the PCI PIN Transaction Security (PCI PTS) standard. [Website: www.withamlabs.com].

XYGATE SOFTWARE

XYGATE is a suite of software modules from **XYPRO Technology Corporation** designed to provide enhanced security and auditing functionality for the HP NonStop server environment. In cases where PCI DSS compliance could not be readily achieved using standard HP tools, this document illustrates how compliance can be assisted by the relevant XYGATE software modules.

Further information on XYGATE software can be found on the XYPRO website at www.XYPRO.com.

WHAT IS PCI DSS COMPLIANCE?

If an organization stores, processes or transmits cardholder data, then it is subject to the requirements of PCI DSS.

For an organization to be considered compliant with the PCI DSS, **the organization must be compliant with ALL requirements specified in the standard** or have approved compensating controls in place.

Once an organization has achieved PCI DSS compliance, they must ensure that they continue to be compliant.

Full and detailed information on PCI DSS can be obtained from the PCI SSC web site www.pci.securitystandards.org

COMPENSATING CONTROLS

Compensating controls[1] may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See Navigating PCI DSS[2] for the intent of each PCI DSS requirement.)
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)
4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

For further details on compensating controls including procedures for applying for compensating controls, see the PCI Data Security Standard v1.2 Appendices B and C.

---

[1] *Appendix B – Compensating Controls*, from PCI Data Security Standard v1.2

[2] *Navigating the PCI DSS Document (https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf)*

THE ASSESSMENT PROCESS – WHAT TO EXPECT

For each requirement of the PCI DSS specification, different items of information (artifacts) may be required by the QSA performing the assessment. This could be any combination of the following:

- Proof of system settings or configuration
- Review of documentation
- Interview by a QSA
- Witnessing of current state or actions performed
- Analysis of network traffic

During a PCI DSS assessment a QSA will examine each requirement as specified in the standard and will assess whether the requirement is "In Place" or "Not In Place".

For a schematic diagram showing the PCI DSS assessment process, see PCI Data Security Standard Version 1.2.1, Appendix F.

CARDHOLDER DATA ELEMENTS

The following table[3] identifies the various data elements or items of sensitive cardholder information. The table indicates whether it is permissible under PCI DSS for each data element to be stored on the system, if protection is required and if it needs to be rendered unreadable as per PCI DSS Requirement 3.4.

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	**Yes**
	Cardholder Name[1]	Yes	Yes[1]	No
	Service Code[1]	Yes	Yes[1]	No
	Expiration Date[1]	Yes	Yes[1]	No
Sensitive Authentication Data[2]	Full Magnetic Stripe Data[3]	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

1. *These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder data environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.*
2. *Sensitive authentication data must not be stored after authorization (even if encrypted).*
3. *Full track data from the magnetic stripe, magnetic stripe image on the chip, or elsewhere.*

[3] *PCI DSS Applicability Information*, from PCI Data Security Standard v1.2

Note that the "Service Code" is also known as the "Service Restriction Code". See ISO 8583 Financial transaction card originated messages — Interchange message specifications (*http://en.wikipedia.org/wiki/ISO_8583#Data_elements*) for a detailed list of cardholder data elements.

Depending on the nature and design of the application being used, there are a number of places on an HP NonStop server where cardholder data may be located. All of these locations should be protected in accordance with PCI DSS. Typical locations where cardholder data may be stored are:

- Cardholder database. Often the PAN (cardholder number) is used as a primary key.
- Transaction logfiles
- TMF auditdumps and audittrails
- Backup media
- Data replication transaction queues (for example those associated with GoldenGate®, DRNet®, Shadowbase® etc.)
- Application trace files
- Communication line/process trace files
- Saveabend (or other memory dump) files

While "off the shelf" financial applications such as BASE24™ and CONNEX™ are user customizable, with organizations receiving source code for the software, customization tends to normally be in regards to different message formats and interfaces. The storage locations of cardholder data will often still be found in the standard locations. There may however be non-standard locations where cardholder data is also stored, depending on specific organizational requirements and industry practices. There should be no assumptions made that all cardholder data on the system and in the network is protected, on the basis that a new version of a card processing application is "encryption enabled". A full analysis needs to be conducted of all possible locations where cardholder data may exist and a determination made as to whether all data elements are protected as required by PCI DSS.

As well as data at rest, cardholder data in transit must be protected. It is typical for an acquirer's financial switching application to accept transactions in to the application from merchants in an external message format, convert the transaction to an internal message format for processing, and then reconvert to another external message format for sending on to the relevant financial organization or issuer. Depending on the mechanisms used, this may provide a number of potential areas that need consideration in determining if cardholder data is suitably protected. For example, if processes involved in the handling of cardholder data were for some reason to abend, would saveabend files be produced and if so, would they suitably protected? Are the processes themselves protected so that they can't be put into debug by an unauthorized user?

The internal format of the message is often used as the "official" record of the transaction and may be used for reporting to financial institutions. In certain instances, it may be necessary for an organization to store this data to satisfy legal or regulatory requirements. If such reporting procedures are in place, this may indicate an extra location or locations where cardholder data is stored or transmitted.

Another area to consider is at the point where card transactions enter or exit the application. Often there will be a trace facility (either application level or at the communications level via SCF) that will enable the reading of the raw transaction, including cardholder data, by certain personnel. This may be in place for application troubleshooting and support purposes. Any such facility should be considered as to what cardholder information is readable and how it relates to PCI DSS compliance. Suitable protection in accordance with the standard should be put into place.

PREPARATION FOR A PCI DSS ASSESSMENT

In preparation for tackling PCI DSS compliance, there are preliminary steps that will help achieve the goal. Much of this information may be required by a QSA and it will also assist in determining what areas need to be addressed for the various sections of the standard.

- Many of the PCI DSS requirements relate to documentation, including all of Requirement 12 (with its 40+ sub-requirements). Take an inventory of all existing documentation related to:
  - Roles and responsibilities
  - System description, configuration, management
  - User management and associated policies and procedures
  - Security description, configuration, management, incident handling
  - Application design, development, implementation, configuration
  - Operational policies and procedures
  - Media handling
  - Change management
  - Any other documentation that may possibly relate to the HP NonStop server environment within your organization. You'll probably need it!

  Beginning the PCI DSS readiness process with Requirement 12: Maintain a Policy that Addresses Information Security for Employees and Contractors, is a good way to become familiar with what is involved with PCI DSS. Satisfying this requirement alone is potentially a very large task and having an understanding right up front will assist with the other requirements of the standard, as all of them have a large focus on documentation.
- Prepare a network diagram of the HP NonStop server(s) identifying all access points in and out of the system(s).
- Prepare a high level diagram of applications that process card payments indicating the flow of transactions and where data is stored. This will assist in identifying all locations where cardholder data is stored, processed or transmitted.
- Identify and document the critical components and details of the environment where cardholder information is stored, processed or transmitted, such as:
  - The HP NonStop servers that process card payments or store or transmit cardholder data.
  - The operating system versions of each of the HP NonStop servers.
  - The core functions provided by each of the HP NonStop servers.
  - Each file/table on the relevant systems containing cardholder data. See the Cardholder Data Elements section for details of which fields are regarded as sensitive cardholder data and how they need to be treated to comply with PCI DSS.
  - For each cardholder data element, determine if it is secured (for example encryption or tokenization) and if there is an audit trail captured of any attempts to access the data element.

A QSA will not typically analyze all systems when performing an assessment but will take a representative sample of the organization's nodes on which to analyze configuration, documentation and procedures. The sample will be defined at the commencement of the assessment.

The QSA will however, likely want to see ALL of your documentation!

PRIVILEGED USERIDS

PCI DSS refers in a number of requirements to “Privileged Userids”. The userid on an HP NonStop server that invariably comes to mind is that of the all powerful SUPER.SUPER. There are however other userids or aliases on an HP NonStop server that should also be considered as privileged userids. These potentially include:

- SUPER.SUPER
- All SUPER group userids
- Security administrator userid (typically the owner of SUPER.SUPER and Safeguard records)
- Operator userids used for backup and restore
- XYGATE owner userid
- Third party security software userid
- Application/Data owner userids
- Application builder userids (i.e. userids for implementing new application object code)
- Any aliases of the above userids

Further to the above, any application specific userids (that is, userids for logging in to the application such as BASE24 or CONNEX) that have elevated privileged access within the application, should also be dealt with as “privileged userids”. Actions that privileged application userids may be able to perform include addition or modification of other application userids, configuration of screen and function access to users and access to functions enabling the viewing of cardholder data (for example transaction trace functionality).

SECURITY AUDIT LOGS

When considering security audit logs in the context of PCI DSS requirements, audit logs from the following subsystems/programs/applications should be taken into account:

- Safeguard
- XYGATE
- Third party software security logs
- Application security logs, for example BASE24 OMF logs
- EMS logs if they are used as the repository for application or utility security logs
- System console audit logs

REQUIREMENT 1: INSTALL AND MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA

REQUIREMENT INTRODUCTION

The introduction for requirement 1 of PCI DSS states:

> *Firewalls are computer devices that control computer traffic allowed between a company's network (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within a company's internal trusted network. The cardholder data environment is an example of a more sensitive area within the trusted network of a company.*
>
> *A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.*
>
> *All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employees' Internet access through desktop browsers, employees' e-mail access, dedicated connection such as business to business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.*

REQUIREMENT DESCRIPTION

Much of Requirement 1 of PCI DSS deals with areas typically outside of the HP NonStop server, predominantly in regards to firewalls and network security. Typically responsibility for the configuration and management of these aspects of the organization are dealt with by a network or infrastructure department.

When considering the requirements relating to workstations or laptops, the system console and any system monitoring consoles (for example a Prognosis console) must be taken into account, as well as user workstations and laptops used for accessing the HP NonStop server.

All PCI DSS requirements for this section of the specification are listed here for the sake of completeness. Requirements where there may be specific relevance to the HP NonStop server environment have been annotated accordingly.

THE REQUIREMENT

Req. No	PCI DSS Requirement	Testing Procedure	Remark
1.1	*Establish firewall and router configuration standards that include the following:*	*Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:*	
1.1.1	*A formal process for approving and testing all network connections and changes to the firewall and router configurations.*	*Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.*	*Not applicable specifically to the HP NonStop server.*
1.1.2 **1.1.2.a**	*Current network diagram with all connections to cardholder data, including any wireless networks.*	*Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks.*	*Not applicable specifically to the HP NonStop server.*
1.1.2.b	*Current network diagram with all connections to cardholder data, including any wireless networks.*	*Verify that the diagram is kept current.*	*Not applicable specifically to the HP NonStop server.*
1.1.3	*Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.*	*Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. Verify that the current network diagram is consistent with the firewall configuration standards.*	*Not applicable specifically to the HP NonStop server.*
1.1.4	*Description of groups, roles, and responsibilities for logical management of network components.*	*Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components.*	*Not applicable specifically to the HP NonStop server.*
1.1.5 **1.1.5.a**	*Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.*	*Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.*	*Not applicable specifically to the HP NonStop server.* *Use of services, protocols and ports on the HP NonStop server is dealt with in Requirement 2.2.2.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
1.1.5.b	*Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.*	*Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service. An example of an insecure service, protocol, or port is FTP, which passes user credentials in clear-text.*	*Not applicable specifically to the HP NonStop server.* *Use of services, protocols and ports on the HP NonStop server is dealt with in Requirement 2.2.2.*
1.1.6 **1.1.6.a**	*Requirement to review firewall and router rule sets at least every six months.*	*Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.*	*Not applicable specifically to the HP NonStop server.*
1.1.6.b	*Requirement to review firewall and router rule sets at least every six months.*	*Obtain and examine documentation to verify that the rule sets are reviewed at least every six months.*	*Not applicable specifically to the HP NonStop server.*
1.2	*Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.* *Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*	*Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment, as follows:*	
1.2.1 **1.2.1.a**	*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*	*Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented.*	*Not applicable specifically to the HP NonStop server.*
1.2.1.b	*Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.*	*Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.*	*Not applicable specifically to the HP NonStop server.*
1.2.2	*Secure and synchronize router configuration files.*	*Verify that router configuration files are secure and synchronized—for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), have the same, secure configurations.*	*Not applicable specifically to the HP NonStop server.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
1.2.3	*Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.*	*Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.*	*Not applicable specifically to the HP NonStop server.*
1.3	*Prohibit direct public access between the Internet and any system component in the cardholder data environment.*	*Examine firewall and router configurations, as detailed below, to determine that there is no direct access between the Internet and system components, including the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment*	
1.3.1	*Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.*	*Verify that a DMZ is implemented to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.*	*Not applicable specifically to the HP NonStop server.*
1.3.2	*Limit inbound Internet traffic to IP addresses within the DMZ.*	*Verify that inbound Internet traffic is limited to IP addresses within the DMZ.*	*Not applicable specifically to the HP NonStop server.*
1.3.3	*Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.*	*Verify there is no direct route inbound or outbound for traffic between the Internet and the cardholder data environment.*	*Not applicable specifically to the HP NonStop server.*
1.3.4	*Do not allow internal addresses to pass from the Internet into the DMZ.*	*Verify that internal addresses cannot pass from the Internet into the DMZ.*	*Not applicable specifically to the HP NonStop server.*
1.3.5	*Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.*	*Verify that outbound traffic from the cardholder data environment to the Internet can only access IP addresses within the DMZ.*	*Not applicable specifically to the HP NonStop server.*
1.3.6	*Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)*	*Verify that the firewall performs stateful inspection (dynamic packet filtering). [Only established connections should be allowed in, and only if they are associated with a previously established session (run a port scanner on all TCP ports with "syn reset" or "syn ack" bits set—a response means packets are allowed through even if they are not part of a previously established session).]*	*Not applicable specifically to the HP NonStop server.*

Req. No	***PCI DSS Requirement***	***Testing Procedure***	***Remark***
1.3.7	*Place the database in an internal network zone, segregated from the DMZ.*	*Verify that the database is on an internal network zone, segregated from the DMZ.*	*Not applicable specifically to the HP NonStop server.*
1.3.8	*Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies—for example, port address translation (PAT).*	*For the sample of firewall and router components, verify that NAT or other technology using RFC 1918 address space is used to restrict broadcast of IP addresses from the internal network to the Internet (IP masquerading).*	*Not applicable specifically to the HP NonStop server.*
1.4 ***1.4.a***	*Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.*	*Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization's network, have personal firewall software installed and active.*	*This requirement is not specifically applicable to the HP NonStop server itself. However, most access to an HP NonStop server is via workstations or laptops which would be subject to this requirement. This requirement also includes the system console, operations monitoring consoles and so on, if they are connected to the internet.*
1.4.b	*Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.*	*Verify that the personal firewall software is configured by the organization to specific standards and is not alterable by mobile computer users.*	*This requirement is not specifically applicable to the HP NonStop server itself. However, most access to an HP NonStop server is via workstations or laptops which would be subject to this requirement. This requirement also includes the system console, operations monitoring consoles and so on, if they are connected to the internet.*

REQUIREMENT 2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS AND OTHER SECURITY PARAMETERS

REQUIREMENT INTRODUCTION

The introduction for requirement 2 of PCI DSS states:

> *Malicious individuals (external and internal to a company) often use vendor-default passwords and other vendor-default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.*

REQUIREMENT DESCRIPTION

Requirement 2 deals with the need to ensure that unauthorized access to the system cannot be obtained by exploiting known vendor defaults. On an HP NonStop server, this may be in terms of userids, passwords or default configurations of the various subsystems.

The requirement goes further to specify that it is necessary to "configure system security parameters to prevent misuse". This small sentence effectively means that you must have all subsystems secured correctly and in accordance with best practices to ensure that only authorized users have access to the system and its components. This will include ownership of the various entities as well as their security or access settings.

It is also a part of the requirement for all configuration items to be fully documented in a System Configuration Standards document. This is a large task and should be allocated appropriate resource and time.

CHANGE DEFAULT SETTINGS

When an HP NonStop server is shipped, the userids NULL.NULL and SUPER.SUPER are provided as the owner of a logged off TACL process and as the owner of the operating system respectively.

In Guardian check that:

- NULL.NULL userid has been disabled or deleted.
- SUPER.SUPER password has been changed from that set by the HP engineer during the initial system build.

The default password settings that ship with an HP NonStop server are very basic to non-existent. It is imperative that these are changed to a more robust configuration.

In Safeguard check that:

- Password encryption has been set to HMAC256.
- Safeguard global password configuration items are appropriately set for minimum password length (minimum 7) and password history (minimum 4).
- Password complexity settings should be set.

DEFAULT SYSTEM CONSOLE SETTINGS

The system console typically ships with only one user configured and that user is configured with Administrator privileges. Potentially there is no password set. The system console is a powerful entry point to the HP NonStop server and should be secured accordingly. If a user has administrator access to the console, they would have the required power, for example, to install a keystroke logging program. It is quite likely that at some stage they would then be able to capture the SUPER.SUPER or other privileged userid and password information at that machine. This would give that person unauthorized privileged powers on the HP NonStop server.

At a minimum, the following measures should be put in place:

- Individual non-administrator userids should be added for all users who have authorized access to the console.
- The default Administrator user account name should be changed and the password secured. userids with administrator privileges should only be used under controlled situations as per PCI DSS requirements.
- The console should be viewed as a potentially vulnerable access point to the HP NonStop server. Ensure that all PCI DSS requirements that may relate to Microsoft Windows machines are strictly adhered to.

For HP's recommendations on how the system console should be secured, see the *HP NonStop Security – NSC Security Program*[4] webpage on HP's website.

While not necessarily subject to PCI DSS requirements (as no cardholder data can be accessed through this route), it is best practice to change the password for the root userid for the Low-Level-Link application on the system console workstation also.

SYSTEM CONFIGURATION STANDARDS

It is necessary for the organization to have a System Configuration Standards document that contains at least the following:

- All subvolumes present on the system that are required to "rebuild" the system and applications that process cardholder data.
- Description of all Guardian security, Safeguard, XYGATE or other security software configuration.
- Description of how to rebuild application(s) and recover/migrate application data.
- Description of all other required system build components.
- Details of what programs should be installed
- Details of what processes should be running

References that may help in the production of this documentation include the following:

- *Security Management Guide* (NonStop Technical Library).
- *HP NonStop Server Security- A Practical Handbook*, by XYPRO Technology Corporation (ISBN: 1-55558-314-8)
- *Securing HP NonStop Servers in an Open Systems World*, by XYPRO Technology Corporation (ISBN: 1-55558-344-X)

XYGATE Security Compliance Wizard (XSW) can be used to help create the appropriate documentation. All of the Best Practice recommendations contained in the two handbooks listed above are pre-configured into the software and are automatically run against existing system configuration settings. Reports of the recommended settings, the current settings and any mismatches can be easily generated.

SINGLE FUNCTION SERVER

Requirement 2 specifies that each server (i.e. system) must perform only one function. This is often not the case on an HP NonStop server. Systems are often used to run multiple applications, often with different functions. In essence, for an HP NonStop server, if multiple applications are running on the same system, there must be a logical separation of application environments as follows:

[4] HP NonStop Security – NSC Security Program (http://www.hp.com/go/nonstop/security/NSCSecurity)

- Different subvolumes for different applications
- Each application environment should be owned by a unique userid
- Application processes should run under application specific userid
- Application subvolumes should not exist on $SYSTEM or other system type volumes such as TMF or DSMSCM volumes
- Safeguard protection of the different environments configured with strong access control
- Non-card payment processing applications running on the system should be secured to the same standard as those applications that are processing card payments and which are subject to PCI DSS.
- No cross access from one functional application to another.
- No write or create access to application data or objects from personal userids.

SERVICES AND PROTOCOLS

All required services and protocols must be documented as to what they do and why they are needed. Only required services/protocols should be allowed. For example, if ftp is not required for a particular TCP/IP stack, it should be disabled in the relevant portconf file. If a protocol such as ftp is required, it needs to be used in a secure manner (i.e. encrypted session) if sensitive data is transmitted over the link, or if a userid with access to cardholder data is used for transmission. This is because passwords on an HP NonStop server are transmitted in the clear by default.

If different services are required in different TCP/IP stacks, the relevant listener processes should be started using different portconf files.

The **XYGATE Security Compliance Wizard (XSW)** can assist by providing a baseline of which TCP/IP ports should be open and which processes should be running on the system. If any changes occur to the baseline from one XSW collection to the next, alerts can be raised. This provides a framework for continually tracking authorized processes across the HP NonStop servers and minimizes the amount of time and effort required to reliably monitor these components.

SYSTEM SECURITY PARAMETERS

A part of requirement 2 is to configure system security parameters. This requirement effectively refers to the configuration of all security related settings across the system and would include the following:

- Safeguard globals.
- Safeguard ACL protection for all critical files such as:
  - system files
  - files in global pmsearchlists
  - tacllocl
  - privileged userid/alias taclcstm files
  - application files (object code, data, configuration, log files etc.)
- User/alias configuration
- Privileged users configured on the system
- XYGATE configuration
- Third party security software configuration
- Owners of files and Safeguard records
- Pathway/Application configuration
- Spooler
- Licensed and Progid'ed files.
- OSS security for relevant files/folders (profile files, inetd.conf etc.)

To assist in choosing which values should be selected for various system settings, it is recommended that the Best Practice recommendations in the *HP NonStop Server Security*[5] and *Securing HP NonStop Servers in an Open Systems World*[6] are consulted. This will ensure that no items are overlooked and that a conscious decision has been made for all values rather than just accepting default values.

The **XYGATE Security Compliance Wizard (XSW)** can assist in this task as it has all of the Best Practices recommended in the two books pre-configured in the software. This means that it can check for compliance of all HP NonStop nodes against the more than 2500 Best Practices automatically and very quickly. Best Practice values can be customized to reflect settings used on the systems in cases where an organization chooses to run different values than those recommended to meet their specific requirements. By configuring XSW to run at regular intervals (for example, nightly), the systems can be monitored for continual compliance.

Unrequired features, processes, devices, printers, programs etc. should be disabled. For example:

- OSS subsystem if not running OSS
- iTP webserver
- Compilers should be removed
- Non-required programs such as adduser, deluser, rpasswrd, diver, tandump, inspect, einspect programs should be removed or disabled, unless there is a specific documented and justifiable reason why these programs should exist on a production or DR system.
- Old $system.sys*nn* subvolumes should be disabled so that users cannot run old versions of programs.

SESSION ENCRYPTION

On an HP NonStop server, userid and password information is transmitted in the clear (unencrypted) by default. To satisfy requirement 2.3, session encryption must be used. All access by a privileged userid/alias - for example, access by super user group, security administrator, XYGATE owner userid or application owner - must be via an encrypted session.

Session types requiring encryption include telnet (TACL, osh), ftp, ixf, rsc sessions or any other type of session for a privileged userid/alias.

The operating system for new NS-series and new NB-series systems now ships with session encryption software included.

XYGATE Host Encryption (XHE) can be used to SSL encrypt card holder data during transmission over open/public networks protocols such as FTP, HTTP, TELNET, RSC, and ODBC/JDBC. XHE supports a number of cipher suites. It is necessary to ensure that only PCI DSS compliant cipher suites are used.

Whichever encryption method is used, it is imperative to ensure that only cipher suites satisfying PCI DSS are enabled for user sessions. These must come under the category of "Strong Cryptography" as defined by PCI DSS.

[5] HP NonStop Server Security- A Practical Handbook, by XYPRO Technology Corporation (ISBN: 1-55558-314-8)
[6] Securing HP NonStop Servers in an Open Systems World, by XYPRO Technology Corporation (ISBN: 1-55558-344-X)

THE REQUIREMENT

Req. No	PCI DSS Requirement	Testing Procedure	Remark
2.1	*Always change vendor-supplied defaults before installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.*	*Choose a sample of system components, critical servers, and wireless access points, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor supplied accounts/passwords.)*	*For this requirement, a QSA will typically:* • *Ask to witness a session by a user logging on to SUPER.SUPER without entering a password, or perform some similar test to demonstrate that a password has been set. The logon attempt should fail if no password has been entered.* • *Ask for verification that NULL.NULL userid is disabled or deleted.* *For information on defaults that should be changed, see Change Default Settings and Default System Console Settings.*
2.1.1	***For wireless environments** connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.*	*Verify the following regarding vendor default settings for wireless environments and ensure that all* *wireless networks implement strong encryption mechanisms (for example, AES):* • *Encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions* • *Default SNMP community strings on wireless devices were changed* • *Default passwords/passphrases on access points were changed* • *Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2)Other security-related wireless vendor defaults, if applicable*	*Not applicable specifically to the HP NonStop server*
2.2 **2.2.a**	*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*	*Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry accepted hardening standards—for example, SysAdmin Audit Network Security (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).*	*For this requirement, a QSA will typically:* • *Need to verify that a System Configuration Standards document exists and that there is content in the document.* *For details of contents to include in this document, see System Configuration Standards.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
2.2.b	*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*	*Verify that system configuration standards include each item below (at 2.2.1 – 2.2.4).*	*For this requirement, a QSA will typically:* • *Review the documentation to ensure that the required content is included* • *Examine system settings to ensure that they match the document.*
2.2.c	*Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*	*Verify that system configuration standards are applied when new systems are configured.*	*For this requirement, a QSA will typically:* • *For a new system want to see that the system was built as per the System Configuration Standard document. Examples of such evidence could be:* • *A signed off document indicating that the build has been completed as specified.* • *Safeguard or other subsystem audit records or logs that show when and how system configuration settings have been applied. The dates found in the logs should correspond with when the system was delivered, built and went "live".*
2.2.1	*Implement only one primary function per server.*	*For a sample of system components, verify that only one primary function is implemented per server. For example, web servers, database servers, and DNS should be implemented on separate servers.*	*For this requirement, a QSA will typically ask for the following evidence from the sample node(s):* • *A list of all running processes to be able to define exactly what application functions are running on the system. If, for example, a web service is running, a QSA may ask for justification as to why this is the case if the system is not specifically running as a web server.* • *A list of all application related subvolumes and OSS directories* • *Safeguard configuration that applies to all application objects* • *Security vectors or ACLs for OSS related objects* • *Details of relevant userids with access to each application environment* *As it is a requirement that only one primary function is implemented per server, if this is not the case and even if the application environments are suitably segregated, the QSA may ask the organization to apply for a Compensating Control for this item.* *See Single Function Server for more information on this requirement.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
2.2.2	*Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).*	*For a sample of system components, inspect enabled system services, daemons, and protocols. Verify that unnecessary or insecure services or protocols are not enabled, or are justified and documented as to appropriate use of the service. For example, FTP is not used, or is encrypted via SSH or other technology.*	*For this requirement, a QSA will typically:* • *Open ports for all TCP/IP processes using SCF (state of LISTEN or ESTAB)* • *PORTCONF and SERVICES files in the Guardian environment and the inetd.conf file in the OSS environment. By default, the PORTCONF file includes entries for FTP, FINGER, ECHO. Typically echo and finger are not required and should be removed. FTP should only be enabled on IP stacks where there is an authorized need. Different portconf files should be used for different listener processes if required so as to achieve this. These files should be strongly secured and audited for any changes where possible.* • *The complete list of all processes running on the system to verify that only required processes are running on the system. All required processes should be documented and have the process name specified (where applicable), the function of the process, the userid that the process should be running as, the program file that is being run and the number of instances of the process.* *See Services and Protocols for more information on this requirement.*
2.2.3 **2.2.3.a**	*Configure system security parameters to prevent misuse.*	*Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components.*	*For this requirement, a QSA will typically:* • *Interview the System Manager of the relevant NonStop server to determine if they understand the security setup of the system. This will include Safeguard, Guardian and OSS security configuration where applicable.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
2.2.3.b	*Configure system security parameters to prevent misuse.*	*Verify that common security parameter settings are included in the system configuration standards.*	*For this requirement, a QSA will typically view that all common security parameters are included in the organization's documentation. This will include items such as:* • *Safeguard globals* • *Security of system subvolumes and old system subvolumes* • *OSS environment security settings where applicable. If OSS is not running on the system, this should be stated.* • *The security relevant commands and utilities in Guardian, Safeguard, and OSS, which user accounts have the privileges to execute them, what the commands do, and so on. Where possible (for example, for "what the commands do") it is acceptable to reference out to relevant HP documents such as the Safeguard Reference Manual (HP NonStop Technical Library). Likewise for XYGATE or other vendor software.*
2.2.3.c	*Configure system security parameters to prevent misuse.*	*For a sample of system components, verify that common security parameters are set appropriately.*	*For this requirement, a QSA will typically:* • *Analyze all of the relevant configuration settings on the system* • *Verify that the configuration matches the settings that are documented as per section 2.2.3.b* • *Ensure that all configured and documented settings are justified and follow industry best practices.* *As a part of this, a QSA will typically require a list of all subvolumes, OSS directories, processes and devices on the system(s). For key subvolumes/directories the list will need to include details of all files. The subvolumes/directories listed should include at least the following:* • *System subvolumes ($system.system, $system.sysnn, relevant $system.z* type subvolumes)* • *Startup/Shutdown subvolumes* • *Application subvolumes (Pathway configuration, logs, programs, libraries, and so on)* • *Database Subvolumes* • *Subvolumes on #PMSEARCHLIST* *See System Security Parameters for suggestions on which parameters to include.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
2.2.4	*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*	*For a sample of system components, verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed. Verify enabled functions are documented and support secure configuration, and that only documented functionality is present on the sampled machines.*	*For this requirement, a QSA will typically:* • *Check that all existing programs, subvolumes, processes and devices are documented as per section **2.2.b*** • *Check that all configuration matches the documentation as per section **2.2.a**.*
2.3	*Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.*	*For a sample of system components, verify that non-console administrative access is encrypted by:* • *Observing an administrator log on to each system to verify that a strong encryption method is invoked before the administrator's password is requested;* • *Reviewing services and parameter files on systems to determine that Telnet and other remote log-in commands are not available for use internally; and* • *Verifying that administrator access to the web-based management interfaces is encrypted with strong cryptography.*	*For this requirement, a QSA will typically want to see:* • *Evidence of session encryption by witnessing a user logon sequence.* • *A network trace of a user session using a tool such as Wireshark.* • *Evidence of what cipher suites are being used for the encryption. This will be in the configuration of the session encryption product. The available cipher suites must be documented as per **2.2.a** and **2.2.b**.* *See Session Encryption for more information.*
2.4	*Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in the PCI DSS Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.*	*Perform testing procedures **A.1.1** through **A.1.4** detailed in PCI DSS Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities' (merchants and service providers) hosted environment and data.*	*If the HP NonStop server is being used in a host sharing environment for multiple clients, the system must be compliant with all requirements in Appendix A of the PCI DSS.*

REQUIREMENT 3: PROTECT STORED CARDHOLDER DATA

REQUIREMENT INTRODUCTION

The introduction for requirement 3 of PCI DSS states:

> *Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.*

REQUIREMENT DESCRIPTION

This requirement relates to ensuring that cardholder data is not stored in a readable form. How to best approach this requirement is often dependant on the nature of the card application and how it processes, stores or transmits data. If the organization is using a software product such as BASE24 or CONNEX, it is recommended that the software vendor is contacted to determine if you are running the latest version of the software. It is possible that some of the issues regarding storage or protection of data may be addressed in a more recent version of the product.

For customized or in-house applications, it may be necessary to modify the application in order to make stored cardholder data unreadable.

See the *PCI Data Storage Do's and Don'ts* document for more information on PCI data storage (https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf).

PROTECTION OF CARDHOLDER DATA

Some of the card processing applications used in the financial industry do not include protection of cardholder data. It is recommended that you consult with your application vendor to determine the current status of this, as circumstances in the software industry constantly change. Even if these applications are updated to protect cardholder data in accordance with PCI DSS, most organizations have a unique processing environment and have typically customized the application to suit their individual business needs. This may mean that even if an "off the shelf" application has been enhanced to provide protection for cardholder data, the "home grown" parts of the application may still contain unprotected data. The onus is on the organization to determine all places where cardholder data is stored, processed or transmitted and ensure that protection is provided in accordance with this requirement.

XYGATE Encryption Library (XEL) is an encryption library that can be used to encryption-enable applications such as BASE24, CONNEX or in-house developed applications, databases and communications using FIPS 140-2 validated encryption. Code modification is required to the card processing application to call the relevant XEL functions for loading encryption keys, performing encryption/ decryption operations and so on. XEL is capable of encryption enabling any application on the HP NonStop server to help satisfy this requirement. XEL supports a large number of encryption algorithms. If using XEL, it is necessary to ensure that the encryption algorithms used in the application are those that satisfy the PCI DSS requirements for strong encryption.

XYGATE Key Manager (XKM) provides a software based encryption key management solution. XEL contains library functions that interface with XKM.

If a company does not believe that it is possible to re-develop their application due to legitimate technical or documented business constraints, it may be possible to use **XYGATE Object Security (XOS)** as a compensating control to protect the PAN. XOS can be used to protect files containing the PAN by restricting access to allow only the application owner userid to have access, if the access attempt is made by specified authorized application processes. This would restrict, for example, any user logged on to an interactive session as the application userid from being able to read the PAN data using non-specified programs/processes such as FUP or SQLCI. A user should not, for example, be able to 'FUP COPY' the contents of a file when logged on as SUPER.SUPER or the application userid and be able to read the PAN.

Note that to deny SUPER.SUPER read access to objects, the system must be configured with SUPER.SUPER deniable.

It should be noted that a QSA may view a compensating control as a temporary measure. What may be acceptable for an assessment one year may not be acceptable the following year if the QSA expects the organization to be moving forward to full compliance in the longer term. This will depend on the reason for and nature of the compensating control and the relevant QSA who is performing the PCI DSS assessment. Whether any measure of protection other than making the PAN unreadable is acceptable to a QSA will likely also depend on the nature of the application. For example, if it is possible from within the application to dump out a list of credit card details en masse, it is likely to be unacceptable for the PAN to remain readable. Ultimately, it is the relevant acquirer of the card scheme that needs to be satisfied that the compensating control is a suitable measure for protecting cardholder information.

BACKUP DATA

If PAN data is not rendered unreadable in the database, consideration needs to be given to system/application backups and also to TMF dumps. Storage of cardholder data in any of these forms needs to be protected.

DISK ENCRYPTION

For disk encryption to be an acceptable method used to satisfy PCI DSS protection of cardholder data there needs to be a method of authentication used, other than that used by the operating system. That is, when a user/program requires access to the encrypted volume, they should be authenticated by a mechanism other than the Guardian USERID file before gaining access.

In cases where disk encryption is used, the method of encryption and access must be fully documented including details of the cipher suites used and the authentication mechanism.

HP NonStop volume level encryption, which is available from HP for all NB series machines and NS series machines that support storage CLIMs, will not satisfy this requirement, as authentication is performed at the operating system level. Once the encrypted volume is mounted it is accessible in the clear to all users who have authenticated to the system. While not satisfying this particular PCI DSS requirement, volume level encryption is still beneficial as it ensures that no data can be read from the disk once it has been physically removed from the system. HP NonStop volume level encryption also supports certain types of NonStop tape devices and so may be suitable for ensuring that backups and TMF dumps are encrypted on tape.

ENCRYPTION KEY CUSTODIANS

A part of this requirement is in regards to encryption key custodians. A good deal of consideration and planning is needed for this requirement. The fewest number of key custodians that satisfies the requirement for split knowledge must be used. Conversely the organization must make sure that there are

sufficient custodians, so that the minimum number is always available to perform key management operations if required. If for some reason the required number of key custodians cannot be obtained, potentially the database can no longer be decrypted and the data may be effectively lost. To ensure that this doesn't occur, a sufficient number of key custodians must be chosen to cater for possible absentees due to termination of employment, holidays, illness and so on. A better option may be for the organization to set up a procedure to guarantee that the passphrases or other credentials of the custodians are always obtainable under controlled circumstances. This could be achieved, for example, by setting up two separate departments as the custodians, using split passphrases so that no individual knows the entire passphrase, and storing the components of the passphrase for each custodian department in separate safes, each requiring two people from the relevant department to gain access. Any such procedure needs to be well documented and would need to be approved by the assessing QSA as being satisfactory.

XYGATE Key Manager (XKM) can be fully configured to set the total number of custodians and the number of those custodians who need to be present to perform key management functions, such as starting or stopping the key server, changing master keys and so on.

ENCRYPTION KEYS

A part of this requirement surrounds the generation, storage and management of encryption keys. It is necessary to ensure that encryption keys cannot be obtained in an unauthorized manner and used to decrypt cardholder data.

Encryption key generation must meet the definition of strong cryptography as defined in the PCI DSS Glossary https://www.pcisecuritystandards.org/security_standards/glossary.shtml.

The components required for strong cryptographic storage are also well described on the OWASP web site (http://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet).

XYGATE Key Manager (XKM) stores data encryption keys in an encrypted database on the HP NonStop server. The XKM key database is encrypted using a Local Master Key (also known as a Key Encryption Key or KEK) which is a randomly generated key. The LMK is also stored on disk, only in an encrypted format. It can only be decrypted by the XKM application when a designated number of custodians, who must first authenticate with their individual Guardian userid and password, enter their individual XKM custodian passphrases. The decrypted LMK is stored only in volatile memory.

XKM provides a mechanism for archiving old or suspected compromised encryption keys. This means that they are available if required to decrypt "old" data, for example from a backup tape, but are not available for daily use.

XKM requires split knowledge and dual control to perform any key-management operations.

XYGATE Encryption Library (XEL) provides a mechanism for using strong cryptographic algorithms including AES, RSA public key cryptography and SHA-512 for hashing. The implementation of the encryption algorithms used in XEL is FIPS 140-2 validated.

THE REQUIREMENT

Req. No	*PCI DSS Requirement*	*Testing Procedure*	*Remark*
3.1	*Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.*	*Obtain and examine the company policies and procedures for data retention and disposal, and perform the following:* • *Verify that policies and procedures include legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons)* • *Verify that policies and procedures include provisions for disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data* • *Verify that policies and procedures include coverage for all storage of cardholder data* • *Verify that policies and procedures include a programmatic (automatic) process to remove, at least on a quarterly basis, stored cardholder data that exceeds business retention requirements, or, alternatively, requirements for a review, conducted at least on a quarterly basis, to verify that stored cardholder data does not exceed business retention requirements.*	*This requirement is not specific just to the HP NonStop server and should be handled as part of the corporate data retention policy and procedure.* *For this requirement, a QSA will typically:* • *Review the documentation to ensure that relevant details on data retention are included as specified in the requirement.*
3.2	*Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:*	*If sensitive authentication data is received and deleted, obtain and review the processes for deleting the data to verify that the data is unrecoverable. For each item of sensitive authentication data below, perform the following steps:*	*This requirement and sub-requirements are relevant to the card processing application running on the HP NonStop server such as BASE24, CONNEX, in-house developed application and so on.* *For this requirement, a QSA would typically:* • *Review the content of a sample of the types of files listed in Requirement 3.2.1 to 3.2.3 to ensure that sensitive authentication data is not stored. This will likely include the cardholder database, application logfiles and application audit files.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
3.2.1	*Do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.* *Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* • *The cardholder's name,* • *Primary account number (PAN),* • *Expiration date, and* • *Service code* *To minimize risk, store only these data elements as needed for business.*	*For a sample of system components, examine the following and verify that the full contents of any track from the magnetic stripe on the back of card are not stored under any circumstance:* • *Incoming transaction data* • *All logs (for example, transaction, history, debugging, error)* • *History files* • *Trace files* • *Several database schemas* • *Database contents.*	*This applies to **card present transactions only** and is typically relevant to the card processing application running on the HP NonStop server rather than the HP NonStop server itself, for example BASE24, CONNEX, in-house developed card processing application and so on.* *For this requirement, a QSA would typically:* • *Review the content of a sample of the types of files referenced in the requirement procedure to ensure that sensitive authentication data is not stored.*
3.2.2	*Do not store the card verification code or value (three digit or four-digit number printed on the front or back of a payment card) used to verify card-notpresent transactions.*	*For a sample of system components, verify that the three-digit or four-digit card-verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance:* • *Incoming transaction data* • *All logs (for example, transaction, history, debugging, error)* • *History files* • *Trace files* • *Several database schemas* • *Database contents.*	*This applies to **card <u>not</u> present transactions only** and is typically relevant to the card processing application running on the HP NonStop server rather than the HP NonStop server itself, for example BASE24, CONNEX, in-house developed card processing application and so on.* *For this requirement, a QSA would typically:* • *Review the content of a sample of the types of files referenced in the requirement procedure to ensure that sensitive authentication data is not stored.*
3.2.3	*Do not store the personal identification number (PIN) or the encrypted PIN block.*	*For a sample of system components, examine the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance:* • *Incoming transaction data* *All logs (for example, transaction, history, debugging, error)* • *History files* • *Trace files* • *Several database schemas* • *Database contents.*	*This applies to **card present transactions only** and is typically relevant to the card processing application running on the HP NonStop server rather than the HP NonStop server itself, for example BASE24, CONNEX, in-house developed card processing application and so on.* *For this requirement, a QSA would typically:* • *Review the content of a sample of the above types of files to ensure that sensitive authentication data is not stored.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
3.3	*Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). Notes:* • *This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN.* • *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.*	*Obtain and examine written policies and examine displays of PAN (for example, on screen, on paper receipts) to verify that primary account numbers (PANs) are masked when displaying cardholder data, except for those with a legitimate business need to see full PAN.*	*This requirement does not apply specifically to the HP NonStop server but is relevant to users who need to view PAN information as a part of their documented job role.* *For this requirement, a QSA would typically:* • *Examine the documented job description and confirm that only authorized personnel can view the full PAN.*
3.4 **3.4.a**	*Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches:* • *One-way hashes based on strong cryptography* • *Truncation* • *Index tokens and pads (pads must be securely stored)* • *Strong cryptography with associated key-management processes and procedures* *The MINIMUM account information that must be rendered unreadable is the PAN.* *Notes:* • *If for some reason, a company is unable render the PAN unreadable, refer to Appendix B: Compensating Controls.* • *"Strong cryptography" is defined in the PCI DSS Glossary of Terms, Abbreviations, and Acronyms.*	*Obtain and examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that the PAN is rendered unreadable using one of the following methods:* • *One-way hashes based on strong cryptography* • *Truncation* • *Index tokens and pads, with the pads being securely stored* • *Strong cryptography, with associated key management processes and procedures*	*For this requirement, a QSA would typically:* • *Review documentation describing the method of PAN protection used.* • *Verify that the type of encryption method and the key length are satisfactory, if encryption is used.* • *Check system settings/application source code/scripts/processes to see if PAN protection has been implemented as per documentation.* *See Protection of Cardholder Data for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
3.4.b	*Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches:* • *One-way hashes based on strong cryptography* • *Truncation* • *Index tokens and pads (pads must be securely stored)* • *Strong cryptography with associated key-management processes and procedures* *The MINIMUM account information that must be rendered unreadable is the PAN.* *Notes:* • *If for some reason, a company is unable render the PAN unreadable, refer to Appendix B: Compensating Controls.* • *"Strong cryptography" is defined in the PCI DSS Glossary of Terms, Abbreviations, and Acronyms.*	*Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).*	*This requirement refers to files or tables where the PAN is stored. For this requirement to be satisfied, the PAN must be stored in these locations in an unreadable form.* *For this requirement, a QSA will typically:* • *Examine the contents of a sample of tables or files storing the PAN to confirm that the PAN is not readable.* *If XOS or similar mechanism is used as a compensating control for Requirement 3.4.a, a QSA would likely need a demonstration of attempts to access the PAN using programs such as FUP or SQLCI when logged on as the application owner userid or "owner" of the data or SUPER.SUPER. Such attempts to access the data by means other than through the application itself should fail with a security error (error 48).*
3.4.c	*Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches:* • *One-way hashes based on strong cryptography* • *Truncation* • *Index tokens and pads (pads must be securely stored)* • *Strong cryptography with associated key-management processes and procedures* *The MINIMUM account information that must be rendered unreadable is the PAN.* *Notes:* • *If for some reason, a company is unable render the PAN unreadable, refer to Appendix B: Compensating Controls.* • *"Strong cryptography" is defined in the PCI DSS Glossary of Terms, Abbreviations, and Acronyms.*	*Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable.*	*For this requirement, a QSA will typically:* • *Sample a number of removable media to ensure that the PAN is stored unreadable using one of the methods listed above.* *See Backup Data for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
3.4.d	*Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches:* • *One-way hashes based on strong cryptography* • *Truncation* • *Index tokens and pads (pads must be securely stored)* • *Strong cryptography with associated key-management processes and procedures* *The MINIMUM account information that must be rendered unreadable is the PAN.* *Notes:* • *If for some reason, a company is unable render the PAN unreadable, refer to Appendix B: Compensating Controls.* • *"Strong cryptography" is defined in the PCI DSS Glossary of Terms, Abbreviations, and Acronyms.*	*Examine a sample of audit logs to confirm that the PAN is sanitized or removed from the logs.*	*For this requirement, a QSA will typically:* • *Review the content of a sample of audit logs holding the PAN to confirm that PAN is not readable.*
3.4.1 **3.4.1.a**	*If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.*	*If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local user account databases).*	*For this requirement, a QSA will typically:* • *Review the relevant system settings to ensure that appropriate logical access to the disk has been implemented* • *Verify that the method used and associated authentication has been fully documented.* *See Disk Encryption for further information.*
3.4.1.b	*If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.*	*Verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).*	*This requirement is only relevant if disk encryption is the method used for protecting the PAN.* *For this requirement, a QSA will typically:* • *Review documentation describing how the cryptographic keys are stored and managed.* • *Review system settings and processes to ensure that cryptographic keys are stored and managed as described in the documentation.* *See Disk Encryption for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
3.4.1.c	*If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.*	*Verify that cardholder data on removable media is encrypted wherever stored.* *Note: Disk encryption often cannot encrypt removable media, so data stored on this media will need to be encrypted separately.*	*This requirement is only relevant if disk encryption is the method used for protecting the PAN.* *For this requirement, a QSA will typically:* • *Review the content of a sample of removable media holding PANs to confirm that the PAN is not readable.* • *Review documentation describing how data is protected on removable media.* *See Disk Encryption for further information.*
3.5	*Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse:*	*Verify processes to protect keys used for encryption of cardholder data against disclosure and misuse by performing the following:*	
3.5.1	*Restrict access to cryptographic keys to the fewest number of custodians necessary.*	*Examine user access lists to verify that access to keys is restricted to very few custodians.*	*For this requirement, a QSA will typically require:* • *A key management document detailing the list of key custodians and the exact role of the custodians.* • *A description in the documentation as to how the data encryption key is constructed or generated using the inputs from the key custodians* • *System settings, source code or scripts confirming that the construction or generation of the PAN encryption key is consistent with the documentation.* *See Encryption Key Custodians for further information.*
3.5.2	*Store cryptographic keys securely in the fewest possible locations and forms.*	*Examine system configuration files to verify that keys are stored in encrypted format and that key encrypting keys are stored separately from data-encrypting keys.*	*For this requirement, a QSA will typically:* • *Examine system settings/source code/scripts to confirm that the PAN encryption key is stored in an encrypted form using a KEK (key encryption key).* • *Check that the KEK is only stored in a protected form, for example only in volatile memory and constructed as per requirement 3.6.6, that is dual control and split knowledge.* • *Check that the KEK is not stored with the encrypted PAN encryption key.* *See Encryption Keys for further information.*
3.6 **3.6.a**	*Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:*	*Verify the existence of key-management procedures for keys used for encryption of cardholder data.* *Note: Numerous industry standards for key management procedures for keys management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*	*For this requirement, a QSA will typically:* • *Review documents that describe all key management processes and procedures.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
3.6.b	*Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:*	*For service providers only: If the service provider shares keys with their customers for transmission of cardholder data, verify that the service provider provides documentation to customers that includes guidance on how to securely store and change customer's keys (used to transmit data between customer and service provider).*	*This requirement refers only to service providers in situations where a fixed secret key is used for encrypting the PAN for transmission.* *For this requirement, a QSA will typically:* • *Review the documentation that describes how the key is securely stored and changed.* • *Applies to requirement 3.6.a through 3.6.c*
3.6.c	*Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:*	*Examine the key-management procedures and perform the following*	
3.6.1	*Generation of strong cryptographic keys.*	*Verify that key-management procedures are implemented to require the generation of strong keys.*	*For this requirement, a QSA will typically:* • *Review the document that describes the procedure under this requirement.* • *Observe the process/state of the system to confirm that the procedure is implemented as documented.* • *Verify that a random number generator has been used to create the keys/key phrases/key components.*
3.6.2	*Secure cryptographic key distribution.*	*Verify that key-management procedures are implemented to require secure key distribution.*	*For this requirement, a QSA will typically:* • *Review the document that describes the procedure under this requirement, to ensure that a secure key distribution method is used. Note that this will apply to the PAN encryption key, Key Encryption Key and key component/phrases.* • *Ask for a mock up of the key distribution process to see that the procedure is implemented as documented.*
3.6.3	*Secure cryptographic storage.*	*Verify that key-management procedures are implemented to require secure key storage.*	*For this requirement, a QSA will typically:* • *Review the document that describes the procedure under this requirement, to ensure that a secure key storage method is used. Note that this will apply to the PAN encryption key, Key Encryption Key and key component/phrases.* • *Observe system settings/process to ensure that keys are stored in a secure manner as described in the documentation.*

Req. No	***PCI DSS Requirement***	***Testing Procedure***	***Remark***
3.6.4	*Periodic cryptographic key changes* • *As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically* • *At least annually.*	*Verify that key-management procedures are implemented to require periodic key changes at least annually.*	*For this requirement, a QSA will typically:* • *Review the document that describes the procedure under this requirement, to ensure cryptographic keys are changed at least annually. Note that this will apply to the PAN encryption key, Key Encryption Key and key component/phrases.* • *Witness the change control documentation confirming that the keys have been changed within the past 12 months.*
3.6.5 ***3.6.5.a***	*Retirement or replacement of old or suspected compromised cryptographic keys.*	*Verify that key-management procedures are implemented to require the retirement of old keys (for example: archiving, destruction, and revocation as applicable).*	*For this requirement, a QSA will typically:* • *Review the document that describes the procedure under this requirement whereby old cryptographic keys are retired/replaced. Note that this will apply to the PAN encryption key, Key Encryption Key and key component/phrases.*
3.6.5.b	*Retirement or replacement of old or suspected compromised cryptographic keys.*	*Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys.*	*For this requirement, a QSA will typically:* • *Review the document that describes the procedure under this requirement whereby suspected compromised cryptographic keys are retired/replaced. Note that this will apply to the PAN encryption key, Key Encryption Key and key component/phrases.*
3.6.6	*Split knowledge and establishment of dual control of cryptographic keys.*	*Verify that key-management procedures are implemented to require split knowledge and dual control of keys (for example, requiring two or three people, each knowing only their own part of the key, to reconstruct the whole key).*	*For this requirement, a QSA will typically:* • *Review the document that describes the procedure under this requirement to ensure that dual control and split knowledge has been established for cryptographic keys. Note that this will apply to the PAN encryption key, Key Encryption Key and key component/phrases.* • *Ask for a mock up of the key injection process to see that the procedure is implemented as documented.*

Req. No	***PCI DSS Requirement***	***Testing Procedure***	***Remark***
3.6.7	*Prevention of unauthorized substitution of cryptographic keys.*	*Verify that key-management procedures are implemented to require the prevention of unauthorized substitution of keys.*	*For this requirement, a QSA will typically:* • *Review the document that describes the procedure under this requirement to ensure that there can be no unauthorized substitution of cryptographic keys. Note that this will apply to the PAN encryption key, Key Encryption Key and key component/phrases.* • *Review system settings/process that prevents unauthorized substitution of keys such as whether each key substitution can only be done under dual control of the key custodians.* • *Check that key custodians are successfully authenticated before being able to perform any key substitution operations.* • *Check that the key components/phrases held by key custodians have not been changed by an unauthorized person. For example, checking the KCV (Key Check Value) if one exists.*
3.6.8	*Requirement for cryptographic key custodians to sign a form stating that they understand and accept their key custodian responsibilities.*	*Verify that key-management procedures are implemented to require key custodians to sign a form specifying that they understand and accept their key custodian responsibilities.*	*For this requirement, a QSA will typically:* • *Review the document that describes the procedure under this requirement which requires key custodians to sign a form stating they understand their responsibilities as a key custodian.* • *Examine a sample of forms signed by key custodians to confirm that the procedure is being followed as documented.*

REQUIREMENT 4: ENCRYPT TRANSMISSION OF CARDHOLDER DATA ACROSS OPEN, PUBLIC NETWORKS

REQUIREMENT INTRODUCTION

The introduction for requirement 4 of PCI DSS states:

> *Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.*

REQUIREMENT DESCRIPTION

This requirement specifies the need for using session encryption to protect sensitive information. Encryption must be used where cardholder data is transmitted over a public network. It should also be noted that if an organization commissions private communications lines from a telecommunications company, it may be possible that the telecommunications company who owns the lines has the ability to view any unencrypted traffic.

The requirement covers not only sessions transmitting cardholder data, but also those that send any information that may help provide an unauthorized user with access to the system. User sessions such as TACL, osh, ftp and so on, send userid and password information in the clear. To protect this information from being obtained by a network trace or sniffer utility, some form of session encryption is required.

See the section on Session Encryption detailed in Requirement 2.

THE REQUIREMENT

Req. No	***PCI DSS Requirement***	***Testing Procedure***	***Remark***
4.1 ***4.1.a***	*Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.* *Examples of open, public networks that are in scope of the PCI DSS are:* • *The internet,* • *Wireless technologies,* • *Global System for Mobile communications (GSM), and* • *General Packet Radio Service (GPRS).*	*Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks* • *Verify that strong encryption is used during data transmission* • *For SSL implementations:* - *Verify that the server supports the latest patched versions.* - *Verify that HTTPS appears as a part of the browser Universal Record Locator (URL).* - *Verify that no cardholder data is required when HTTPS does not appear in the URL.* • *Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit.* • *Verify that only trusted SSL/TLS keys/certificates are accepted.* • *Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)*	*For this requirement, a QSA will typically:* • *Review the document that describes how cardholder data is protected while being transmitted over an open or public network.* *Interview relevant personnel to:* • *Get the list of publicly facing URLs used to connect to the cardholder data environment.* • *Get the list of URLs of external organizations to which cardholder data is sent.* • *Understand what protection mechanism is used to protect cardholder data during transmission.* *For SSL implementations the QSA will typically:* • *Scan the relevant ports to see which cipher suites are enabled.* • *View the SSL configuration to see which cipher suites are enabled.* • *Perform test transactions and capture traffic using tools such as Wireshark to ensure that SSL encryption is used for transmitting cardholder data.* • *Ensure that the SSL certificates have been issued by a trusted Certification Authority (CA).* *For other encryption technologies, the QSA will typically:* • *Examine the relevant configuration to see which cipher suites are enabled.* • *Perform test transactions and capture traffic with tools such as Wireshark to ensure that encryption is used for transmitting cardholder data.* *See Session Encryption for further information.*

Req. No	***PCI DSS Requirement***	***Testing Procedure***	***Remark***
4.1.1	*Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.* • *For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.* • *For current wireless implementations, it is prohibited to use WEP after June 30, 2010.*	*For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.*	*This requirement is generally not applicable to the HP NonStop server.*
4.2 ***4.2.a***	*Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).*	*Verify that strong cryptography is used whenever cardholder data is sent via end-user messaging technologies.*	*This requirement is generally not applicable to the HP NonStop server.*
4.2.b	*Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).*	*Verify the existence of a policy stating that unencrypted PANs are not to be sent via end-user messaging technologies.*	*This requirement is generally not applicable to the HP NonStop server.*

REQUIREMENT 5: USE AND REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS

REQUIREMENT INTRODUCTION

The introduction for requirement 5 of PCI DSS states:

> *Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business approved activities including employees' e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.*

REQUIREMENT DESCRIPTION

Typically, the following operating systems are not commonly affected by malicious software: mainframes, and certain Unix servers (such as AIX, Solaris, and HP-Unix). However, industry trends for malicious software can change quickly and each organization must comply with Requirement 6.2 to identify and address new security vulnerabilities and update their configuration standards and processes accordingly[7].

HP NonStop servers are not systems that are commonly affected by malware so this section is not applicable when strictly applied to HP NonStop servers. However, HP NonStop servers are regularly accessed by Windows workstations, including the system console, which are vulnerable to such attacks. Malicious programs such as software based key loggers, if installed on the system console, could potentially provide privileged userid and password information to unauthorized users. It is imperative that this is guarded against.

Any Windows based systems accessing an HP NonStop server that stores, processes or transmits cardholder data are subject to requirement 5.

SECURING THE SYSTEM CONSOLE

For HP's recommendations on how the system console should be protected, see the *HP NonStop Security – NSC Security Program*[8] webpage on HP's website. This document details anti-virus/anti-malware software that is supported for the system console and how it should best be secured.

The recommendations below and any comments in this section apply to the system console and any other Windows based consoles connected to the HP NonStop server, such as those used for system monitoring. Other Windows based machines are likely to be subject to this requirement, but as this document focuses specifically on the HP NonStop server environment, they are not in scope.

For the system console automatic updates of software may not be possible as it is quite likely to be connected neither to the internet nor to a Windows Domain. In this case, anti-virus/anti-malware software and definitions will need to be updated manually. The process for updating the anti-virus/anti-malware software and definitions should be documented.

Automatic virus scans should be configured for all Windows workstations that provide access to the HP NonStop server.

---

[7] From *Navigating PCI DSS:Understanding the Intent of the Requirements* (https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf)

[8] HP NonStop Security – NSC Security Program (http://www.hp.com/go/nonstop/security/NSCSecurity)

THE REQUIREMENT

Req. No	PCI DSS Requirement	Testing Procedure	Remark
5.1	*Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).*	*For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.*	*For this requirement, a QSA will typically:* • *Examine the system console to confirm that appropriate anti-virus/anti-malware software is installed.* *See Securing the System Console for further information.*
5.1.1	*Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.*	*For a sample of system components, verify that all anti-virus programs detect, remove, and protect against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits).*	*For this requirement, a QSA will typically:* • *Examine the installed software to verify that it can perform all of the functions specified in the requirement.*
5.2	*Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.*	*Verify that all anti-virus software is current, actively running, and capable of generating logs by performing the following:*	*For this requirement, a QSA will typically:* • *Examine the installed software and associated configuration to ensure that anti-virus/anti-malware software is current, actively running and capable of generating logs.* • *Applies to requirement 5.2.a through 5.2.d*
5.2.a	*Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.*	*Obtain and examine the policy and verify that it requires updating of anti-virus software and definitions.*	*For this requirement, a QSA will typically:* • *Review the document that describes the policy for updating of anti-virus/anti-malware software and virus definitions.* • *Observe the process/state of the system console to confirm that the procedure is implemented as documented. This would include checking the logs showing that anti-virus software has been updated.*
5.2.b	*Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.*	*Verify that the master installation of the software is enabled for automatic updates and periodic scans.*	*For this requirement, a QSA will typically:* • *Examine the configuration of the anti-virus/anti-malware software to ensure it is configured as per the requirement.* • *Examine the software logs to ensure that updates have occurred as per the procedure.* • *Examine the software logs to ensure that scans have occurred as required and as documented.*

Req. No	***PCI DSS Requirement***	***Testing Procedure***	***Remark***
5.2.c	*Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.*	*For a sample of system components including all operating system types commonly affected by malicious software, verify that automatic updates and periodic scans are enabled.*	*For this requirement, a QSA will typically:* • *Examine the software logs to ensure that updates have occurred as per the procedure.* • *Examine the software logs to ensure that scans have occurred as required and as documented.*
5.2.d	*Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.*	*For a sample of system components, verify that antivirus software log generation is enabled and that such logs are retained in accordance with PCI DSS Requirement 10.7*	*For this requirement, a QSA will typically:* • *Review the documentation to ensure that it describes the process and procedures regarding log generation and retention for anti-virus/anti-malware software.* • *Examine evidence that the logs are generated and retained as specified in the documentation.*

REQUIREMENT 6: DEVELOP AND MAINTAIN SECURE SYSTEMS AND APPLICATIONS

REQUIREMENT INTRODUCTION

The introduction for requirement 6 of PCI DSS states:

> *Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.*
>
> *Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.*

REQUIREMENT DESCRIPTION

This requirement relates to ensuring that no software vulnerabilities exist and includes both system and application software. A large portion of the requirement focuses on establishing good coding, testing and application deployment practices.

SECURITY UPDATES TO SOFTWARE

Any security related SPRs that are identified as critical need to be implemented within one month of being released. This also applies to any third party security software that may be running on the system. Any critical patches released by the vendor should likewise be implemented within one month.

The organization must have a security policy that documents that all such security related patches will be applied within one month to the HP NonStop servers.

It should be a part of documented procedures to go through all SPR release notes and ensure that any SPRs related to security are applied.

To enroll in receiving HP ExpressNotice so as to be alerted to newly discovered security vulnerabilities for the HP Operating System and HP products, a user should register via the HP NonStop eService Portal which is located at https://onepoint.nonstop.compaq.com.

To register for new release notification and urgent notices for XYGATE software from XYPRO Technology, register on the XYPRO website at https://www.xypro.com/index.php?id=login and modify your user profile settings accordingly.

Contact other third party software vendors to determine their procedure for alerting of security vulnerabilities and notification of new software patches and releases.

If the organization has no process in place for analyzing security related patches to determine which ones should be applied to the system, then all patches need to be installed within one month of release.

XYGATE Security Compliance Wizard (XSW) can be used to assist in gathering information and reporting on what software is installed on the system.

ROLE BASED APPLICATION ACCESS CONTROL

In regards to software applications, role-based access control typically relates to users only being authorized to perform functions or have access to screens required to fulfill their documented role within the organization. This type of functionality needs to be included in the design of the application.

SEPARATION OF TEST AND DEVELOPMENT FROM PRODUCTION

Test and Development environments must be separate from Production and Disaster Recovery (DR) environments. Ideally this means that they should not be on the same physical system or on the same Expand network.

Strong controls must be in place to ensure that there is no mixing of environments. There must be no possible access to production environments from development or test userids whether they are on the same system (if for example the DR system is also a test system) or from separate physical development or test systems. Such measures that would assist in keeping environments separate include the following:

- No sharing of userids between the environments. That is, no development/test userids should be able to access a production or DR environment.
- Unique subvolumes for each environment with appropriate Safeguard protection in place to enforce access control and auditing.
- Unique directories for each OSS environment with strong access security applied.
- Real (production) cardholder data must not be used on the development/test systems for test or development purposes.
- Production/DR application userids should not exist on the Dev/Test systems.
- Privileged userids on the Dev/Test system, such as SUPER.SUPER, should not have privileged capabilities on the Production/DR system.
- No shared communication lines between Prod/DR and Test/Dev.

Documentation must describe the process used for ensuring that test data and accounts are never ported to the production environment.

Different roles, for example testing and production support may be performed across the production and development/test environments by the same person. The different roles must however be performed by separate userids/aliases with different passwords. Each role performed must be fully documented.

If userids or aliases are common across production and development/test systems (not recommended), the passwords for these userids/aliases must be different.

If test users do exist on the production system due to shared physical systems, for example DR and test, they must be completely segregated as described above.

CHANGE CONTROL

It needs to be shown that proper change control procedures are fully documented and are followed for the implementation of any changes to the system. Such change procedures should include impact analysis, testing, back-out procedures and management sign-off.

CODING WEB APPLICATIONS AGAINST KNOWN VULNERABILITIES

Coding of web based applications must address each vulnerability included in the OWASP Top 10 vulnerability list at the time that PCI DSS 1.2 was published (October 2008). At the time that this

document was published in September 2010, the OWASP Top 10 list had changed to the following vulnerabilities:

- A1: Injection
- A2: Cross-Site Scripting (XSS)
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross-Site Request Forgery (CSRF)
- A6: Security Misconfiguration
- A7: Insecure Cryptographic Storage
- A8: Failure to Restrict URL Access
- A9: Insufficient Transport Layer Protection
- A10: Unvalidated Redirects and Forwards

The vulnerabilities listed above that are not specified in Requirements 6.5.1 through 6.5.10 must also be addressed in a like manner. A QSA will be looking to see that all of these vulnerabilities have been addressed.

See the OWASP website (http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project) for full details of the OWASP Top 10 and descriptions of the various web application security risks.

THE REQUIREMENT

Req. No	PCI DSS Requirement	Testing Procedure	Remark
6.1 **6.1.a**	*Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.* *Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*	*For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed.*	*For this requirement, a QSA will typically examine the following:* • *SYSINFO to show current OS version* • *SYSTIMES to show when the system was last cold loaded* • *List of all installed SPRs and OS file versions* • *List of all latest releases of SPRs from HP* • *List of all installed third party software* • *List of all latest releases from third party software vendor* *See Security Updates to Software for further information.*
6.1.b	*Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.* *Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*	*Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.*	*The organization must have a security policy that documents that all security related critical SPRs as per **6.1.a** will be applied within one month to the HP NonStop servers.* *For this requirement, a QSA will typically:* • *Examine the documentation to confirm that the process for installing SPRs is included and is satisfactory.* *See Security Updates to Software for further information.*
6.2 **6.2.a**	*Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.*	*Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities.*	*For this requirement, a QSA will typically:* • *Interview relevant personnel to determine the method that they use for reviewing and applying security related patches and updating documentation.* *See Security Updates to Software for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
6.2.b	*Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.*	*Verify that processes to identify new security vulnerabilities include using outside sources for security vulnerability information and updating the system configuration standards reviewed in Requirement 2.2 as new vulnerability issues are found.*	*You will likely need to provide evidence of the method of receiving the information and applying relevant patches provided to the QSA as per **6.2.1**.* *For this requirement, a QSA will typically examine the following:* • *Documentation indicating the process for receiving and reviewing SPR and release documents from HP and third party software vendors respectively.* • *Evidence of received SPR Notifications and Hotstuffs* • *Evidence of a method used for analyzing release notices to determine if they need to be applied, such as a security incident register or spreadsheet detailing all released relevant SPRs, which ones need to be applied to the systems and when they were applied.* *See Security Updates to Software for further information.*
6.3 **6.3.a**	*Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout the software development life cycle. These processes must include the following:*	*Obtain and examine written software development processes to verify that the processes are based on industry standards, security is included throughout the life cycle, and software applications are developed in accordance with PCI DSS.*	*A document must exist that describes the software development methodology used. It must include all requirements specified in 6.3.1 through 6.6.* *For this requirement, a QSA will typically:* • *Review the document to ensure that it contains all of the required information.*
6.3.b	*Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout the software development life cycle. These processes must include the following:*	*From an examination of written software development processes, interviews of software developers, and examination of relevant data (network configuration documentation, production and test data, etc.), verify that:*	*For this requirement, a QSA will typically:* • *Review documentation for software development and testing to ensure that it incorporates all requirements from 6.3.1 through 6.6.* • *Review development/test environments and analyze test results to ensure that they are in accordance with the documentation.* • *Interview software developers and testers to ensure that they perform development and test tasks in accordance with the requirement and as documented.*

Req. No	***PCI DSS Requirement***	***Testing Procedure***	***Remark***
6.3.1	*Testing of all security patches, and system and software configuration changes before deployment, including but not limited to the following:*	*All changes (including patches) are tested before being deployed into production.*	*For this requirement, a QSA will typically:* • *Review documentation for software testing to ensure that it includes details of how changes are tested.* • *Review development/test environments and analyze test results to ensure that they are in accordance with the documentation.* • *Interview software developers and testers to ensure that they perform development and test tasks in accordance with the requirement and as documented.*
6.3.1.1	*Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.).*	*Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.).*	*For this requirement, a QSA will typically:* • *Review documentation for software development and testing to ensure that it includes details of how validation of input is coded and tested.* • *Review development/test environments and analyze test results to ensure that they are in accordance with the documentation.* • *Interview software developers and testers to ensure that they perform development and test tasks in accordance with the requirement and as documented.*
6.3.1.2	*Validation of proper error handling.*	*Validation of proper error handling.*	*For this requirement, a QSA will typically:* • *Review documentation for software development and testing to ensure that it includes details of how error handling is coded and tested.* • *Review development/test environments and analyze test results to ensure that they are in accordance with the documentation.* • *Interview software developers and testers to ensure that they perform development and test tasks in accordance with the requirement and as documented.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
6.3.1.3	*Validation of secure cryptographic storage.*	*Validation of secure cryptographic storage.*	*For this requirement, a QSA will typically:* • *Review documentation for software development and testing to ensure that it includes details of the secure cryptographic storage methods used and how they are tested.* • *Review development/test environments and analyze test results to ensure that they are in accordance with the documentation.* • *Interview software developers and testers to ensure that they perform development and test tasks in accordance with the requirement and as documented.*
6.3.1.4	*Validation of secure communications.*	*Validation of secure communications.*	*For this requirement, a QSA will typically:* • *Review documentation for software development and testing to ensure that it includes details of how secure communications methods are coded and tested.* • *Review development/test environments and analyze test results to ensure that they are in accordance with the documentation.* • *Interview software developers and testers to ensure that they perform development and test tasks in accordance with the requirement and as documented.*
6.3.1.5	*Validation of proper role-based access control (RBAC).*	*Validation of proper role-based access control (RBAC).*	*For this requirement, a QSA will typically:* • *Review documentation for software development and testing to ensure that it includes details of how role-based access control has been implemented and how it is tested.* • *Review development/test environments and analyze test results to ensure that they are in accordance with the documentation.* • *Interview software developers and testers to ensure that they perform development and test tasks in accordance with the requirement and as documented.* *See Role Based Application Access Control for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
6.3.2	*Separate development/test and production environments.*	*The development/test environments are separate from the production environment, with access control in place to enforce the separation.*	*For this requirement, a QSA will typically:* • *Examine configuration, interview relevant personnel, review documentation and check procedures, to ensure that satisfactory separation exists between production and dev/test environments.* *See Separation of Test and Development from Production for further information.*
6.3.3	*Separation of duties between development/test and production environments.*	*There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment.*	*For this requirement, a QSA will typically:* • *Request for a user to logon to a sample userid that exists on both systems and show by demonstration that the passwords are different.* *See Separation of Test and Development from Production for further information.*
6.3.4	*Production data (live PANs) are not used for testing or development.*	*Production data (live PANs) are not used for testing and development, or are sanitized before use.*	*For this requirement, a QSA will typically:* • *Interview relevant personnel to determine how test data is obtained or generated. They may also want to observe the generation process and examine test data.* • *Confirm that the process for obtaining or generating test data is fully documented.* *See Separation of Test and Development from Production for further information.*
6.3.5	*Removal of test data and accounts before production systems become active.*	*Test data and accounts are removed before a production system becomes active.*	*For this requirement, a QSA will typically:* • *Interview relevant personnel to determine the process for ensuring that test data and accounts are never ported to the production environment.* • *Review documentation to ensure that it describes the process used for ensuring that test data and accounts are never ported to the production environment.* • *Examine change control documents to ensure that test data and accounts are not ported from development/test environments.* • *Examine production data files or tables to ensure that there is no test data included (for example "Greg's Test Record") and a list of userids/aliases to ensure that there are no test users on the production system.* *See Separation of Test and Development from Production for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
6.3.6	*Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers.*	*Custom application accounts, user IDs and/or passwords are removed before system goes into production or is released to customers.*	*For this requirement, a QSA will typically:* • *Perform the same tests and require the same information as described for Requirement 6.3.5 above.*
6.3.7 **6.3.7.a**	*Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability* *Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle required by PCI DSS Requirement 6.3. Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*	*Obtain and review policies to confirm all custom application code changes for internal applications must be reviewed (either using manual or automated processes), as follows:* • *Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices.* • *Appropriate corrections are implemented prior to release.* • *Code review results are reviewed and approved by management prior to release.*	*A document must exist that describes the code review process and policies for internal applications as detailed in this requirement.* *For this requirement, a QSA will typically:* • *Review the relevant documentation* • *Ask for evidence that shows that the process has been followed as described.*
6.3.7.b	*Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability* *Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle required by PCI DSS Requirement 6.3. Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*	*Obtain and review policies to confirm all custom application code changes for web applications must be reviewed (either using manual or automated processes), as follows:* • *Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices.* • *Code reviews ensure code is developed according to secure coding guidelines such as the Open Web Security Project Guide (see PCI DSS Requirement 6.5).* • *Appropriate corrections are implemented prior to release.* • *Code review results are reviewed and approved by management prior to release.*	*A document must exist that describes the code review process and policies for web applications as detailed in this requirement.* *For this requirement, a QSA will typically:* • *Review the relevant documentation*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
6.3.7.c	*Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability* *Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle required by PCI DSS Requirement 6.3. Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*	*Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.7a and 6.3.7b above.*	*For this requirement, a QSA will typically:* • *Review the relevant documentation* • *Ask for evidence that shows that the process has been followed as described.*
6.4 **6.4.a**	*Follow change control procedures for all changes to system components. The procedures must include the following:*	*Obtain and examine company change-control procedures related to implementing security patches and software modifications, and verify that the procedures require items 6.4.1 – 6.4.4 below.*	
6.4.b	*Follow change control procedures for all changes to system components. The procedures must include the following:*	*For a sample of system components and recent change/security patches, trace those changes back to related change control documentation. For each change examined, perform the following:*	*For this requirement, a QSA will typically ask for you to step through the change control mechanism showing each step for the change being initiated, planned, reviewed, approved, scheduled, authorized, implemented and closed. If the organization is running a software package or automated tools that are used for tracking change management, the QSA will likely want to see you demonstrate a change's different stages within the software application.* *See Change Control for further information.*
6.4.1	*Documentation of impact.*	*Verify that documentation of customer impact is included in the change control documentation for each sampled change.*	*For this requirement, a QSA will typically:* • *Request to see a sample change control document with a description of the impact of the change.*
6.4.2	*Management sign-off by appropriate parties.*	*Verify that management sign-off by appropriate parties are present for each sampled change.*	*For this requirement, a QSA will typically:* • *Request to see a sample change control document with sign-off for the change to proceed.* *See evidence that the change has been completed as described in the change control documentation.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
6.4.3	*Testing of operational functionality.*	*Verify that operational functionality testing is performed for each sampled change.*	*For this requirement, a QSA will typically:* *Request to see a sample change control document that shows the testing that is to be performed for the change.*
6.4.4	*Back-out procedures.*	*Verify that back-out procedures are prepared for each sampled change.*	*For this requirement, a QSA will typically:* *Request to see a sample change control document that shows a description of the back-out procedures for the change.*
6.5 **6.5.a**	*Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in software development processes, to include the following* *Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current in the OWASP guide when PCI DSS v1.2 was published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.*	*Obtain and review software development processes for any web-based applications. Verify that processes require training in secure coding techniques for developers, and are based on guidance such as the OWASP guide (http://www.owasp.org).*	*For this requirement, a QSA will typically:* • *Request to see the document describing the software development processes for any web-based applications.* • *Ensure that the process requires training in secure coding techniques for developers, based on guidance such as the OWASP guide (http://www.owasp.org).* • *Request to see evidence that the process is followed. For example, records of staff training with dates.*
6.5.b	*Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in software development processes, to include the following:* *Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current in the OWASP guide when PCI DSS v1.2 was published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.*	*Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques.*	*For this requirement, a QSA will typically:* • *Interview a sample of developers to ensure that they have been trained in and understand secure coding techniques.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
6.5.c	*Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in software development processes, to include the following: Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current in the OWASP guide when PCI DSS v1.2 was published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.*	*Verify that processes are in place to ensure that web applications are not vulnerable to the following:*	*For Requirements 6.5.1 through 6.5.10, and for other vulnerabilities in the current OWASP Top 10, a QSA will typically perform the following:* • *Examine documentation that describes how to ensure that the vulnerability doesn't exist in the application. That is, how it has been addressed.* • *Interview software developers to see how they have ensured that the vulnerability doesn't exist in the application and to see if the responses correlate with the documentation.* • *Examine test results showing that the application has been tested against the vulnerability in this requirement and ensure that the test has been successful.* *See Coding Web Applications Against Known Vulnerabilities for further information.*
6.5.1	*Cross-site scripting (XSS).*	*Cross-site scripting (XSS) (Validate all parameters before inclusion.).*	*As per 6.5.c*
6.5.2	*Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.*	*Injection flaws, particularly SQL injection (Validate input to verify user data cannot modify meaning of commands and queries.).*	*As per 6.5.c*
6.5.3	*Malicious file execution.*	*Malicious file execution (Validate input to verify application does not accept filenames or files from users.).*	*As per 6.5.c*
6.5.4	*Insecure direct object references.*	*Insecure direct object references (Do not expose internal object references to users.).*	*As per 6.5.c*
6.5.5	*Cross-site request forgery (CSRF).*	*Cross-site request forgery (CSRF) (Do not reply on authorization credentials and tokens automatically submitted by browsers.).*	*As per 6.5.c*
6.5.6	*Information leakage and improper error handling.*	*Information leakage and improper error handling (Do not leak information via error messages or other means.).*	*As per 6.5.c*
6.5.7	*Broken authentication and session management.*	*Broken authentication and session management (Properly authenticate users and protect account credentials and session tokens.).*	*As per 6.5.c*
6.5.8	*Insecure cryptographic storage.*	*Insecure cryptographic storage (Prevent cryptographic flaws.).*	*As per 6.5.c*
6.5.9	*Insecure communications.*	*Insecure communications (Properly encrypt all authenticated and sensitive communications.).*	*As per 6.5.c*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
6.5.10	*Failure to restrict URL access.*	*Failure to restrict URL access (Consistently enforce access control in presentation layer and business logic for all URLs.).*	*As per 6.5.c*
6.6	*For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:* • *Review of documentation* • *Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes* • *Installing a web-application firewall in front of public-facing web applications.*	*For public-facing web applications, ensure that either one of the following methods are in place as follows:* • *Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows:* - *At least annually* - *After any changes* - *By an organization that specializes in application security* - *That all vulnerabilities are corrected* - *That the application is re-evaluated after the corrections* • *Verify that a web-application firewall is in place in front of public-facing web applications to detect and prevent web-based attacks.* *Note: "An organization that specializes in application security" can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.*	*A document must exist that describes how this requirement is met for publicly facing web-based applications.* *There is an information supplement from PCI SSC that clarifies how to meet this requirement. (https://www.pcisecuritystandards.org/security_standards/docs/information_supplement_6.6.pdf).*

REQUIREMENT 7: RESTRICT ACCESS TO CARDHOLDER DATA BY BUSINESS NEED TO KNOW

REQUIREMENT INTRODUCTION

The introduction for requirement 7 of PCI DSS states:

> *To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.*
>
> *"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.*

REQUIREMENT DESCRIPTION

There are a number of ways that non-privileged userids can gain privileged user abilities on an HP NonStop server if security is not configured correctly. By obtaining this level of privilege, a user may be able to access areas of the system that they are not authorized to access, potentially including sensitive cardholder data or applications.

The basis of this requirement is that users accessing the system should be provided only with the access privileges required to perform their specific (and documented) job role. This refers to both the use of privileged userids and also the access rights that are provided for users on the system.

In an HP NonStop server environment, a number of common tasks require SUPER group level access. This includes tasks that may fit regularly into a user's job role. For example, operations staff may be given the authority to bounce communications lines as a part of their authorized role. To perform this task in SCF, they would require super level access, yet if a SUPER userid is provided, this provides those staff with powers far in excess of just being able to bounce communications lines. Similarly if a progid version of SCF is provided for such users, they would be able to perform a wider range of activities than they may be authorized for. These factors must be considered when determining how to achieve compliance with this requirement.

In regards to accessing of files on the system, users should only be provided with the access that they require for their documented job role. Sensitive data should be restricted accordingly.

Note: If LDAP or Windows Active Directory is used for authenticating to the HP NonStop server, all of the requirements listed in Requirement 7 must be met on the authenticating server as well as the HP NonStop server.

ROLES AND RESPONSIBILITIES

There must be documentation describing the roles and responsibilities of the various users/groups that have access to the systems. The following should be included in the documentation:

- Identification of all departmental groups/userids that have access to the systems.
- For each user group, a brief description of their role as it relates to the HP NonStop servers.
- Tasks authorized for each group defined at a functional level. This should include:
  - Authorized day to day activities that can be performed from a user's personal userid/alias without any extra level of authority being required.
  - Authorized day to day activities that need to be performed from a userid/alias with elevated privileges such as, for example, SUPER.SUPER or application userids.
  - Activities that need to be performed periodically from a userid/alias with elevated privileges but that need to be authorized in accordance with the organization's change management procedures.
  - Activities that need to be performed from a userid/alias with elevated privileges in an emergency support situation.

USE OF PRIVILEGED USERIDS

The usage of privileged userids must be documented and must include a description of how and when these userids are used. Excessive privileges should not be provided to users without proper controls. In regards to an HP NonStop server, for example, system managers should not be provided with SUPER group privileges for their day to day operations, as this provides a greater level of access than will typically be required. Elevated privileges should only be made available on an as needs basis under a documented control mechanism.

Userids with elevated access privileges on the system (e.g. super users, XYGATE owner userid, application userids) need to be identified. For each of these userids the following should be detailed.

- Purpose for the userid and typical tasks that require use of the userid.
- Role groups who are authorized to access the userid under appropriate controls.
- Circumstances under which the userid will be made available to authorized users.
- Password ownership of the userid and password requirements. System level password controls applied to the userid.
- Procedure for obtaining the authority to access the userid and for obtaining passwords.
- Any system level logon controls applied to the userid (e.g. CMON or XYGATE User Authentication).

The various userids detailed in the Privileged Userids section should be included.

XYGATE Access Control (XAC) can be used to set up a role based security model so that users have the ability to perform all authorized actions, including those tasks normally requiring privileged userid access, from their own non-privileged personal userid. This means that users can be provided with exactly the level of privilege that they require for their job role, without being provided any greater privilege than they need. Any commands configured in XAC to provide this functionality should be fully documented.

USER ACCESS PRIVILEGES

User access privileges on the system must be documented. This should align with the roles as described above and should include details of the types of files/subvolumes that a user has access to on the system. The following types of files should be taken into account:

- Operating system objects
- Startup/Shutdown files for system and OS subsystems
- Configuration files for system and OS subsystems
- System and subsystem logfiles
- Security configuration
- Security audit logfiles
- Application object programs
- Application program source code/libraries/DDLs
- Application data subvolumes/directories
- Application reports
- Application configuration files
- Application startup/shutdown files
- Application logfiles

If a role based security tool such as **XYGATE Access Control (XAC)** is in use, any privileged commands provided to individuals should be fully documented.

ACCESS CONTROL SYSTEM

The NonStop platform comes with an access control system that provides the following functionality:

- Users must enter a userid and password to gain access to the system.
- Guardian, Safeguard and OSS provide controls that allow the restriction of access to files based on the userid attempting the access and the type of access operation being performed (read, write, execute, purge).

The HP *Security Management Guide*[9] describes that, while the Guardian tools provide basic authentication and authorization services, Safeguard features add auditing services and also extend the authentication and authorization capabilities. Safeguard features also allow segregating administration tasks. Safeguard's access control lists allow specifying access to a greater level of detail than Guardian security strings allow.

An automated mechanism should be used for restricting which users are allowed to logon to privileged userids. Neither Guardian nor Safeguard provides this level of access control.

XYGATE User Authentication (XUA) can be used to restrict the use of privileged userids to a set of authorized users. For example, it is possible to configure XUA so that only users in the SUPPORT.* user group have the ability to log on to SUPER.SUPER if they have the valid password. Other users would be denied access even if they had the password in their possession. Other controls in XUA for logon

[9] Security Management Guide (HP NonStop Technical Library)

restriction include rules based on requestor program (e.g. TACL, OSH, FTPSERV, specified application program etc.), IP address, terminal name, time of day and ancestor program.

XYGATE CMON (XCM) provides an alternate method of restricting the use of privileged userids. It can also enforce dual logon for authorized users so that each TACL session can be associated with a specific individual.

The following points should also be considered in regard to this requirement:

- If Safeguard is configured to let users login to OSS directly, then users would be able to login to the OSS environment without going through the Guardian shell. Otherwise, users have to login to the Guardian environment and then use the OSH command to login to the OSS environment.
- Access to OSS files is controlled by OSS file-permission bits and access control lists that are supported by the OSS file system.
- As a Command monitor process, $CMON controls user requests such as logons and running of commands. The process name $CMON should be protected by OBJECTTYPE PROCESS under Safeguard whether a $CMON process is running or not.

"NEED TO KNOW" ACCESS

A part of Requirement 7 refers to the implementation of security on the system that ensures that users do not have access to any component that they are not specifically authorized to access. For this to be achieved access needs to be denied by default.

An example of a "deny all" implementation in Safeguard is as follows:

Safeguard Globals:

- Safeguard configured with `SUPER.SUPER DENIABLE` (SYSGEN parameter)
- `DIRECTION-DISKFILE = FILENAME-FIRST`
- `COMBINATION-DISKFILE  = FIRST-ACL`
- `CHECK-VOLUME = ON`
- `CHECK-SUBVOLUME = ON`
- `CHECK-FILENAME = ON`

For each VOLUME:

- SUPER.SUPER or Application userid access only (depending on what is stored on the volume)
- Configured with no access to other userids.

For each SUBVOLUME:

- Required access configured for all relevant userids

DISKFILE Records:

- Only required where the security required for a file is different to the access provided by the Subvolume record.

OBJECTTYPE Records:

- Ensure that all objecttypes (including objectype objecttype) are secured so that only authorized users are able to add Safeguard records.

This ensures that if a Safeguard Subvolume record is not specifically defined, no access will be provided to users.

It would be possible to use other methods to achieve the above, such as Safeguard DISKFILE-PATTERNS or **XYGATE Object Security (XOS)**. XOS would provide the desired "deny all" result as above with significantly less access rules required than either the illustrated method or than would be

possible with Safeguard Diskfile Patterns. XOS also provides a “what if” test mechanism for testing the effects of configuration before implementing on the system, to ensure that the rules operate as desired.

“Deny all” default security should likewise be set in the OSS environment. OSS cannot currently be secured using Safeguard. OSS security needs to be set within the OSS environment itself at the file and directory level.

XYGATE Safeguard Manager (XSM) is a GUI based security module that simplifies security management within the OSS environment as well as within Safeguard, providing a graphical interface for both setting configuration and for examining what configuration is currently set. Reporting and exporting of configuration settings can be easily obtained. As setting up “deny all” security requires a significant effort in Safeguard, XSM can make the task a lot simpler and provide much greater visibility of existing configuration than is possible with Safecom.

THE REQUIREMENT

Req. No	PCI DSS Requirement	Testing Procedure	Remark
7.1	*Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:*	*Obtain and examine written policy for data control, and verify that the policy incorporates the following:*	*For this requirement, a QSA will typically:* • *Request to see the documentation to determine if all relevant items are included.* • *Applies to requirement 7.1.1. through 7.1.4* *See Roles and Responsibilities for further information.*
7.1.1	*Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities.*	*Confirm that access rights for privileged User IDs are restricted to least privileges necessary to perform job responsibilities.*	*For this requirement, a QSA will typically:* • *Request to see the documentation to determine if all relevant items are included.* *See Use of Privileged Userids for further information.*
7.1.2	*Assignment of privileges is based on individual personnel's job classification and function.*	*Confirm that privileges are assigned to individuals based on job classification and function (also called "role-based access control" or RBAC).*	*For this requirement, a QSA will typically:* • *Request to see the documentation to determine if all relevant items are included.* *See User Access Privileges for further information.*
7.1.3	*Requirement for an authorization form signed by management that specifies required privileges.*	*Confirm that an authorization form is required for all access, that it must specify required privileges, and that it must be signed by management.*	*For this requirement, a QSA will typically:* *Require a demonstration that displays that proper procedures are being followed in the process of providing access to the system. This may include a request to see a signed Access Request Form or equivalent to show that this is the case.*
7.1.4	*Implementation of an automated access control system.*	*Confirm that access controls are implemented via an automated access control system.*	*For this requirement, a QSA will typically:* • *Request to see a demonstration of the use of the automated access control system that is in place.* *See Access Control System for further information.*
7.2	*Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:*	*Examine system settings and vendor documentation to verify that an access control system is implemented as follows:*	*This requirement is comprised of Requirements 7.2.1 through 7.2.3.* *See Access Control System for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
7.2.1	*Coverage of all system components.*	*Confirm that access control systems are in place on all system components.*	*For this requirement, a QSA will typically:* • *Check whether or not Safeguard is running on the system* • *Check if any other access control mechanisms such as **XYGATE User Authentication (XUA)**, **XYGATE CMON (XCM)** or **XYGATE Object Security (XOS)** are running.* *See Access Control System for further information.*
7.2.2	*Assignment of privileges to individuals based on job classification and function.*	*Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.*	*For this requirement, a QSA will typically:* • *Examine the access configuration of the system.* • *Examine access authorization forms and privileges that are detailed in the forms for each user.* • *Ensure that access provided to a particular user on the system matches what is defined in the authorization form and documentation.* • *Examine security of all cardholder data - whether the files are readable or not by unauthorized users.* • *Examine user menu screens to ensure users can't "break" out and get back to a prompt if not authorized.* • *Verify whether there seems to be a good rationale as to why userids/aliases/groups and their corresponding access have been set up in the manner in which they have.* • *Check which userid(s) the system manager logs on to on a day to day basis.* • *Check what SUPER.SUPER is used for, how often, and if this use is as reflected in user access forms.* • *Check usage of aliases.* • *Check all types of access around files containing any sensitive cardholder data.* *See "Need to Know" Access for further information.*

Req. No	***PCI DSS Requirement***	***Testing Procedure***	***Remark***
7.2.3	*Default "deny-all" setting*	*Confirm that the access control systems have a default "deny-all" setting.* *Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*	*For this requirement, a QSA will typically:* *Examine security configuration settings, such as the following, to determine if this requirement has been satisfied:* • *All operating system files ($system.system, $system.sysnn, DSV subvols, ISV subvols)* • *System and OS subsystem startup/shutdown/configuration files* • *Security subsystem related files (including XYGATE or third party security software).* • *Pathway configuration. Note that by default when a new Pathway environment is created, it has a security setting of "N" meaning that any user on the network could add a server that will run any object (e.g. SCF or FUP) as the owner userid of the Pathway.* • *Netbatch security including security of all of the job "infiles".* • *Spooler configuration.* • *User default subvolume security. These should not be shared and should be secured so that only the owner can create or modify any files.* • *Subvolumes on common pmsearchlists.* • *Process security for $CMON.* • *Default security for users.*

REQUIREMENT 8: ASSIGN A UNIQUE ID TO EACH PERSON WITH COMPUTER ACCESS

REQUIREMENT INTRODUCTION

The introduction for requirement 8 of PCI DSS states:

> *Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.*

REQUIREMENT DESCRIPTION

Requirement 8 deals largely with the use and management of userids and passwords on the system. A main essence of the requirement is that every logon to the system must be directly traceable to a specific individual. If multiple personnel within the organization use the same userid, in the case of a potential security breach, it is not easy to determine which specific person has performed the relevant actions. By enforcing individual userids and non-sharing of passwords, user actions can be more easily determined.

The only exception permitted for shared logons under this requirement is for logon to shared userids that are not a security concern. For example, userids with no power or privilege such as those used only for monitoring, may be allowed.

A compensating control is required for the existence of any shared userids on the system. This includes standard HP NonStop server userids such as SUPER.SUPER.

All users of the system with userids or aliases providing access to cardholder data need to be familiar with corporate password procedures and policies.

Note: If LDAP or Windows Active Directory is used for authenticating to the HP NonStop server, all of the requirements listed in Requirement 8 must be met on the authenticating server as well as on the HP NonStop server.

ACCOUNTABILITY OF USER SESSIONS

On an HP NonStop server, some generic privileged userids will typically exist. These include userids such as SUPER.SUPER, SUPER.CE, application owner userids and so on. It is a specific aim of this requirement to ensure that all logons to the system must be tied to a specific individual. If generic/shared userids such as SUPER.SUPER exist, there must be some mechanism to ensure that all uses of such userids are traceable to a specific individual. There is no standard way through Safeguard of achieving this objective, so some other mechanism will need to be used. This mechanism must be documented and will form the basis of the compensating control. Use of aliases, TACL macros and procedures may assist in providing a compensating control for this mechanism, but considerations need to be taken for all user sessions on the system including osh, ftp, rsc, dsm/scm and so on, as well as TACL.

XYGATE User Authentication (XUA) has a number of features that can help satisfy this requirement in all system authentication scenarios:

- Enforce two-step logon to privileged userids ensuring that authorized users must logon to their own personal userid prior to logging on to a privileged userid, thus tracking exactly who has logged on to the privileged userid.

- Impersonate mechanism which allows authorized userids to authenticate to specified programs as a privileged userid by entering their own credentials (userid/alias and password) as the password for the privileged userid. This means that the password for the privileged userid does not need to be given out for activities that a user is authorized to perform on a day to day basis. The audit trail clearly shows which individual user has logged on to the privileged userid. This feature is especially useful for logon to GUI applications or applications requiring single logon such as FTP.

XUA can also restrict which userids are authorized to logon to other userids. For example, it would be possible to restrict logon to SUPER.SUPER to only members of the SUPPORT user group. This would mean that any other userid, for example, a member of the OPERATOR group, would not be able to logon as SUPER.SUPER even if they possessed the correct SUPER.SUPER password.

XUA also provides the capability for two factor authentication for the HP NonStop server. By using RSA SecurId® tokens, selected userids/aliases can be configured to authenticate against an RSA ACE/Server®.

XYGATE Access Control (XAC) can be configured so that each person with access to the system is able to perform all authorized tasks from their own individual non-privileged userid, This includes tasks that normally would require logging on to a shared privileged userid. With XAC, the use of shared privileged userids, or aliases of privileged userids, can be eliminated.

Note that application specific userids such as those required to logon to applications such as BASE24, CONNEX and so on are also subject to this requirement and will typically also be reviewed by a QSA for compliance.

Where shared userids are in place, a policy document must exist that defines which generic (or shared) userids exist on the system, what they are used for and what compensating control is in place. For example,"*SUPER.SUPER is a shared privileged userid that is only used for emergency support situations. Users must logon to their personal userid prior to logging on to SUPER.SUPER as enforced by XUA*".

PASSWORD ENCRYPTION

Userid and alias passwords must be encrypted both in storage and also in transmission.

Safeguard provides the facility to encrypt passwords in storage and this should be appropriately configured. The legacy encryption algorithm used in older versions of Guardian and Safeguard was DES. This setting is not appropriate as the DES encryption algorithm is no longer considered strong. Furthermore, it is only with the stronger algorithm of HMAC256 that passwords/passphrases longer than 8 characters are possible.

While passwords can be stored encrypted on an HP NonStop server using Safeguard, userid and password information is transmitted unencrypted as standard on an HP NonStop server. It is therefore essential to use an appropriate session encryption mechanism, as discussed in Requirement 2.

PASSWORD MANAGEMENT

Organizational procedures must be in place for verifying the identity of individuals before they have their password remotely reset by security or help desk personnel. For example, if an individual has forgotten their password or it has expired after returning from vacation, it may be necessary to have the password reset remotely by the help desk. On such occasions, the person resetting the password must have a procedure for validating the identity of the person requesting the password change and must be able to match the individual to their authorized userid. The procedure may be a manual procedure or it may be a part of a user password management program.

The **XYGATE Password Reset (XPR)** GUI (a component of **XYGATE Password Quality (XPQ)**) and **XYGATE Safeguard Manager (XSM)** GUI both contain a mechanism for storing personnel information about users on the system that can be used to verify the identity of an individual when resetting userid/alias passwords through either of these software modules.

PASSWORDS FOR NEW USERS

When userids or aliases are added to the system via Safecom, they should be added with their password expired, and with a Password-Expiry-Grace period set. This will force the individual to change their password when they first logon.

It is acceptable (in small organizations, for example) for a system administrator to add the user to the system via Safecom and for the individual to come over and change their password at the time by running the Password program. Blind Password must be enforced.

REVOKING OF USERIDS

Any user no longer employed by the organization should have their userid removed. This is important so that it is not possible for the ex-employee to gain access to the system, but also so that no existing employees are able to masquerade as that user by performing actions using the defunct userid.

XYGATE Safeguard Manager (XSM) and **XYGATE Security Compliance Wizard (XSW)** both provide a facility for reporting on “orphaned” Safeguard ACLs. This means that when a userid/alias is removed from the system, Safeguard configuration can be easily updated to remove corresponding access rules for that userid/alias.

PASSWORD EXPIRY

It is a part of Requirement 8 that a mechanism is in place to ensure that user passwords are changed every 90 days at a maximum. This requirement can typically be satisfied if userids/aliases are configured so that the sum of the values set for Password-Must-Change and Password-Expiry-Grace is less than 90 days in total. In such cases, a userid/alias will be frozen with a status of password-expired if they have not logged on for 90 days.

A compensating control is required for any userid or alias configured with a non-expiring password. For example, if the SUPER.SUPER password is non-expiring, a suitable compensating control may be the secure holding of the password by a group who do not have the ability to use the password to logon as SUPER.SUPER. The procedure or mechanism used to enforce this needs to be documented.

XYGATE Safeguard Manager (XSM) and **XYGATE Security Compliance Wizard (XSW)** both have a facility to list userids/aliases that have not logged on in the last 90 days or any other specified time period. They also can report on users with expired passwords, userid/alias password change settings, passwords not changed for a specified period and so on.

VENDOR OR THIRD PARTY USERIDS

Vendor userids such as those used by HP for remote support, or application software vendors where applicable, should be frozen when not in use. They should be thawed only as required and re-frozen when the relevant task has been completed.

When a service account is used (such as SUPER.CE), an authorized member of the organization needs to be present to witness the session of the engineer. If it is not possible or practical for somebody to be present in this capacity, there is a need to capture the session and review the logs to ensure no unauthorized actions were performed.

XYGATE Access Control (XAC) provides the ability to capture all user interactive sessions in conversational or block mode, Guardian or OSS and captures both the input and the output of commands. The associated reporting capability makes it possible to determine exactly what actions a user has performed during any given session.

XYGATE User Authentication (XUA) can restrict which userids can logon from which IP address, at what time of day and to which requestor (TACL, OSH, FTP and so on). This may assist in further refining use of vendor userids.

PASSWORD LENGTH AND COMPLEXITY

The longer and more complex a password, the more difficult it is for somebody to either guess or crack using brute force techniques. A part of Requirement 8 specifies that password must be a minimum of 7 characters long and complexity must be enforced, so that all users must be configured with passwords containing both numeric and alphabetic characters. As of G06.31, both of these requirements can be achieved using Safeguard.

It should be noted that the greater the length of a password/passphrase, the average time to crack using a brute force attack increases exponentially. Longer passphrases typically provide greater protection than a shorter password/passphrase configured with complexity.

XYGATE Password Quality (XPQ) provides the ability to set different password rules for different userids. It would be possible for example, to have individual users configured with the basic requirement above, and shared privileged userids with non-expiring passwords such as SUPER.SUPER set with a minimum password length of 20 characters containing numeric and alphabetic characters of mixed case.

INVALID ACCESS ATTEMPTS

Action must be taken to reduce the likelihood of anybody successfully logging on to the system by guessing the password of a valid userid or alias. Requirement 8 states that a userid or alias must be frozen if there are more than six consecutive invalid logon attempts. The mechanism within Safeguard for performing this action involves setting the values for AUTHENTICATE-MAXIMUM-ATTEMPTS to 6 and AUTHENTICATE-FAIL-FREEZE to ON. This however is **not recommended** on an HP NonStop server. The problem is that the Authenticate-Fail-Freeze parameter is a global setting. If it is set on, it is very easy for anybody to freeze out critical users such as SUPER.SUPER or SECURITY.ADMIN by continually attempting to logon with an incorrect password. If an organization loses SUPER.SUPER on the system, recovery is potentially a very difficult and time consuming procedure, perhaps requiring system down time or a complete rebuild of the system disk.

XYGATE User Authentication (XUA) can be configured with parameters such as Authenticate-Fail-Freeze set on a user by user basis. This means that it would be possible to have all users other than SUPER.SUPER configured to be frozen after 6 failed authentication attempts. SUPER.SUPER could be alternately configured so that the user session times out for 30 minutes after 6 failed logon attempts, but the userid itself remains thawed. If in combination with this, SUPER.SUPER were configured with an extremely long passphrase (**XYGATE Password Quality (XPQ)** could be configured so that SUPER.SUPER must have a long passphrase of 20 characters for example, whereas other userids and aliases have a minimum of 8 characters), this would significantly reduce the risk of a successful brute force password attack. This mechanism could possibly be used as a compensating control for this requirement.

XUA also provides a facility for authenticating users against Windows Active Directory (AD) or an LDAP server. By using this mechanism, the lock out facility as specified in this requirement could be provided by the authenticating server.

The requirement further states that a userid or alias must be locked (frozen) after the invalid logon attempts for a period of 30 minutes. Short of freezing the user permanently, with the associated problems as described above, this cannot be achieved by Safeguard. The Safeguard Global parameter AUTHENTICATE-FAIL-TIMEOUT freezes the user session, not the user account.

XYGATE User Authentication (XUA) and **XYGATE Password Quality (XPQ)** could be used as described above.

USER SESSION INACTIVITY TIMEOUT

If a user leaves their session inactive for 15 minutes, it is required that the session be automatically locked so that another user cannot perform actions on the system using that session. This requirement is to assist in ensuring that all user actions can be tied to a specific individual. It is possible to satisfy the requirement in general by using a Windows screensaver with a password set. At a shared console workstation however, if a generic userid with a shared password is being used for some reason, controls must be applied at the Guardian/OSS level.

If the system console screensaver password is shared, any TACL/OSS sessions must have autologoff or session locking after 15 minutes or less of session inactivity. As the console is often the workstation used by HP engineers to access the system, typically using a privileged userid, it is imperative that if the session is left logged on, that no other user will find it active and be able to enter commands.

Automatic termination of a TACL session after 15 minutes of session inactivity can be set in TACL using #SETCONFIGURATION. It can however be “fooled” if the user has entered a utility such as FUP or Viewpt. When the user exits the utility, the TACL session will still be alive and logged on. If for example, somebody has logged on to the system console as SUPER.SUPER, run Viewpt and forgotten to exit and logoff, when another user comes along to the console, they will find a logged on session running as SUPER.SUPER.

For osh sessions in the OSS environment, session timeout should be configured using the TMOUT env variable.

It is possible to use Telnet process timeout parameters to enforce session timeouts, but this may not exit the session in a clean manner and can also be “fooled” by users starting a Viewpt session, or equivalent, to keep the session alive.

XYGATE Access Control (XAC) can be configured either to password lock or to terminate a session after a period of session inactivity and is fully operable in both Guardian and OSS. If the user is in a conversational utility such as FUP, the session will timeout as soon as the configured inactivity time is reached. If the user is in a block mode application such as Viewpt, as soon as the user exits and returns to TACL, the session will terminate or lock based on configuration choices.

APPLICATION USERIDS

It is a part of Requirement 8 that application userids are not used by individuals for interactive logons to the system. This includes for purposes of managing the application, such as startup and shutdown. A mechanism such as Netbatch could potentially be used to assist in meeting this requirement.

XYGATE Access Control (XAC) can be configured to allow authorized users to start up or manage application processes from their own non-privileged userid, or from a designated support userid with dual logon control enforced by **XYGATE User Authentication (XUA)**.

THE REQUIREMENT

Req. No	PCI DSS Requirement	Testing Procedure	Remark
8.1	*Assign all users a unique ID before allowing them to access system components or cardholder data.*	*Verify that all users are assigned a unique ID for access to system components or cardholder data.*	*For this requirement a QSA will typically interview relevant personnel, check documentation (for example, company security policy) and examine system configuration settings such as the following:* • *List of userids/aliases.* • *Check configuration of userids/aliases to ensure they are active and are not expired or frozen.* • *Check configuration of application userids to ensure they are not shared and that all are current.* • *XUA configuration if implemented.* • *Users/aliases on the system should match the relevant documentation.* *See Accountability of User Sessions for more information.*
8.2	*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:* • *Password or passphrase* • *Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys).*	*To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder data environment, perform the following:* • *Obtain and examine documentation describing the authentication method(s) used.* • *For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s).*	*For this requirement, a QSA will typically:* • *Confirm that all users logging on to the system require a userid and a password* • *Verify that this fact has been documented.* • *Observe a sample user logon to the system to ensure that a password is entered at the prompt. If the user logs on and does not enter a password, the logon should fail.*
8.3	*Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.*	*To verify that two-factor authentication is implemented for all remote network access, observe an employee (for example, an administrator) connecting remotely to the network and verify that both a password and an additional authentication item (for example, smart card, token, PIN) are required.*	*This requirement is not generally applicable to the HP NonStop server and should be implemented at the network layer by the relevant personnel within the organization.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
8.4 **8.4.a**	*Render all passwords unreadable during transmission and storage on all system components using strong cryptography (defined in PCI DSS Glossary of Terms, Abbreviations, and Acronyms).*	*For a sample of system components, examine password files to verify that passwords are unreadable during transmission and storage.*	*For this requirement, a QSA will typically check the following:* • *In Safeguard, the PASSWORD-ALGORITHM = HMAC-256.* • *Examination of the USERID file to ensure that all passwords are encrypted.* • *That session encryption is being used for all user sessions to the HP NonStop server.* *See Password Encryption for further information.*
8.4.b	*Render all passwords unreadable during transmission and storage on all system components using strong cryptography (defined in PCI DSS Glossary of Terms, Abbreviations, and Acronyms).*	*For service providers only, observe password files to verify that customer passwords are encrypted.*	*This requirement refers to organizations that provide cardholder services to multiple customers. For example, organizations running a payment gateway type of environment. It is not generally applicable to the HP NonStop server environment unless the users of the service application also have access to the operating system. If they do, this requirement is covered under 8.4.a.*
8.5	*Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:*	*Review procedures and interview personnel to verify that procedures are implemented for user authentication and password management, by performing the following:*	
8.5.1.a	*Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.*	*Select a sample of user IDs, including both administrators and general users. Verify that each user is authorized to use the system according to company policy by performing the following:* • *Obtain and examine an authorization form for each ID.* • *Verify that the sampled user IDs are implemented in accordance with the authorization form (including with privileges as specified and all signatures obtained), by tracing information from the authorization form to the system.*	*For this requirement, a QSA will typically:* • *Match the user authorization forms with privileges assigned to users on the system. This is a subset of 7.2.2.*
8.5.2	*Verify user identity before performing password resets.*	*Examine password procedures and observe security personnel to verify that, if a user requests a password reset by phone, e-mail, web, or other non-face-to- face method, the user's identity is verified before the password is reset.*	*For this requirement, a QSA will typically:* • *Witness the procedure used for relevant personnel changing another user's password.* *See Password Management for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
8.5.3	*Set first-time passwords to a unique value for each user and change immediately after the first use.*	*Examine password procedures and observe security personnel to verify that first-time passwords for new users are set to a unique value for each user and changed after first use.*	*For this requirement, a QSA will typically:* • *Examine documentation to confirm that it is specified that when a user's password is initially set, it must be changed when the user first logs on.* • *Examine the mechanism used for enforcing password change at first logon.* *See Passwords for New Users for further information.*
8.5.4	*Immediately revoke access for any terminated users.*	*Select a sample of employees terminated in the past six months, and review current user access lists to verify that their IDs have been deactivated or removed.*	*For this requirement, a QSA will typically:* • *Examine a current set of all userids and aliases on the system.* • *Verify that all userids and aliases on the list belong to currently employed personnel.* *See Revoking of Userids for further information.*
8.5.5	*Remove/disable inactive user accounts at least every 90 days.*	*Verify that inactive accounts over 90 days old are either removed or disabled.*	*For this requirement, a QSA will typically:* • *Review that a procedure for removing inactive user accounts is documented as specified.* • *Request to see evidence that the procedure is followed as documented.* *See Password Expiry for further information.*
8.5.6	*Enable accounts used by vendors for remote maintenance only during the time period needed.*	*Verify that any accounts used by vendors to support and maintain system components are disabled, enabled only when needed by the vendor, and monitored while being used.*	*For this requirement, a QSA will typically:* • *Confirm that vendor service userids/aliases are frozen.* • *Verify that the procedures used for monitoring actions performed by these userids are adequate and are as documented.* *See Vendor or Third Party Userids for further information.*
8.5.7	*Communicate password procedures and policies to all users who have access to cardholder data.*	*Interview the users from a sample of user IDs, to verify that they are familiar with password procedures and policies.*	*For this requirement, a QSA will typically:* • *Interview a sample of users to confirm that they understand the procedures and policies associated with passwords.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
8.5.8 **8.5.8.a**	*Do not use group, shared, or generic accounts and passwords.*	*For a sample of system components, examine user ID lists to verify the following:* • *Generic user IDs and accounts are disabled or removed.* • *Shared user IDs for system administration activities and other critical functions do not exist.* • *Shared and generic user IDs are not used to administer any system components.*	*This requirement is essentially the same as Requirement 8.1. The remarks under that section apply directly to this section also.*
8.5.8.b	*Do not use group, shared, or generic accounts and passwords.*	*Examine password policies/procedures to verify that group and shared passwords are explicitly prohibited.*	*For this requirement, a QSA will typically:* • *Examine the documentation to ensure that shared userids and their use are documented.* • *Verify that a compensating control is in place for any shared userids.* *See Accountability of User Sessions for further information.*
8.5.8.c	*Do not use group, shared, or generic accounts and passwords.*	*Interview system administrators to verify that group and shared passwords are not distributed, even if requested.*	*For this requirement, a QSA will typically:* • *Interview the system administrator to ensure that no passwords are shared for generic userids.*
8.5.9	*Change user passwords at least every 90 days.*	*For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days.* *For service providers only, review internal processes and customer/user documentation to verify that customer passwords are required to change periodically and that customers are given guidance as to when, and under what circumstances, passwords must change.*	*For this requirement, a QSA will typically:* • *Examine Safeguard configuration to determine that user passwords are set to expire as per the requirement.* • *Ensure that a suitable compensating control is in place for userids with non-expiring passwords.* *See Password Expiry for further information.*
8.5.10	*Require a minimum password length of at least seven characters.*	*For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long.* *For service providers only, review internal processes and customer/user documentation to verify that customer passwords are required to meet minimum length requirements.*	*For this requirement, a QSA will typically* • *Confirm that the value set in Safeguard for PASSWORD-MINIMUM-LENGTH is at least 7.* *Note: If **XYGATE Password Quality (XPQ)** is in use, this must also be configured with a PASSWORD-MINIMUM-LENGTH of at least 7.* *See Password Length and Complexity for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
8.5.11	*Use passwords containing both numeric and alphabetic characters.*	*For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain both numeric and alphabetic characters.* *For service providers only, review internal processes and customer/user documentation to verify that customer passwords are required to contain both numeric and alphabetic characters.*	*For this requirement, a QSA will typically:* • *Check Safeguard configuration to ensure that password complexity is in use and that it satisfies the rules stated in the requirement.*
8.5.12	*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*	*For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords.* *For service providers only, review internal processes and customer/user documentation to verify that new customer passwords cannot be the same as the previous four passwords.*	*For this requirement, a QSA will typically:* • *Confirm that the value set in Safeguard for PASSWORD-HISTORY is at least 4.*
8.5.13	*Limit repeated access attempts by locking out the user ID after not more than six attempts.*	*For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that a user's account is locked out after not more than six invalid logon attempts.* *For service providers only, review internal processes and customer/user documentation to verify that customer accounts are temporarily locked-out after not more than six invalid access attempts.*	*For this requirement, a QSA will typically:* • *Examine the system configuration that enforces the locking out of users after the invalid password attempts.* • *Observe the mechanism in effect to ensure it corresponds with the documentation.*
8.5.14	*Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.*	*For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.*	*For this requirement, a QSA will typically:* • *Examine the system configuration that enforces the locking out of users after the invalid password attempts.* • *Observe the mechanism in effect to ensure it corresponds with the documentation.*
8.5.15	*If a session has been idle for more than 15 minutes, require the user to re-enter the password to reactivate the terminal.*	*For a sample of system components, obtain and inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less.*	*For this requirement, a QSA will typically:* • *Examine the system configuration enforcing the inactivity timeout of user sessions.* • *Observe the mechanism in effect to ensure it corresponds with the documentation.*

Req. No	***PCI DSS Requirement***	***Testing Procedure***	***Remark***
8.5.16 ***8.5.16.a***	*Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.*	*Review database and application configuration settings and verify that user authentication and access to databases includes the following:* • *All users are authenticated prior to access.* • *All user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures).* • *Direct access or queries to databases are restricted to database administrators.*	*For this requirement, a QSA will typically require the following:* • *A list of all database users. Users with access to the database will typically be matched with their user roles as defined in documentation to see if they should have access.* • *Confirmation that all database users are authenticated against the system before accessing the database.* • *Confirmation that all application access to the database contains appropriate authentication mechanisms. For this the QSA may want to analyze the application code to see the authentication mechanism used and access method to the database.* • *Confirmation that only userids with a DBA function are permitted direct access to the data files by SQLCI, Enable etc. Users with this type of access to the database will typically be matched with their user roles as defined in documentation.*
8.5.16.b	*Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.*	*Review database applications and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes).*	*For this requirement, a QSA will typically check that:* • *Application owner userids are frozen.* • *Application startup is setup so that nobody needs to logon to the application owner userid itself, but startup of the application processes is via some other mechanism such as by use of Pathway owner settings, progid processes or a tool such as XAC.* *This requirement also has a component regarding network/firewall access. For this, a QSA will typically:* • *Check which ports are open on the system (for example, by running nmap scan) and whether or not firewalls prevent unauthorized access to the system from within the network.* • *Check open ports to see if it is possible to access the system through the port using an application userid, without authenticating, to access cardholder data.*

REQUIREMENT 9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA

REQUIREMENT INTRODUCTION

The introduction for requirement 9 of PCI DSS states:

> *Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.*

REQUIREMENT DESCRIPTION

Requirement 9 predominantly deals with the physical security required for systems and for media containing cardholder data. HP NonStop servers are typically stored in an organization facility that may house other system or network components used by the organization. As such, policies and procedures surrounding the facility are often not specific to the HP NonStop server environment and are more likely to be a part of overall organization policies and procedures. While all requirements in this section must be met for an organization to be PCI DSS compliant, often it is the role of a different area of the organization to ensure that this is the case.

Areas that may apply specifically to the HP NonStop server have been detailed where relevant.

SYSTEM CONSOLE PHYSICAL SECURITY

The system console should be physically secured as well as logically secured, for example by being locked in a cabinet. If somebody is able, for example, to attach a keystroke logging hardware device, it is quite likely that it is just a matter of time before they will be able to capture SUPER.SUPER or other privileged userid's password information giving them unauthorized privileged powers on the HP NonStop server.

REMOVABLE MEDIA

A large part of this requirement refers to removable media that contains cardholder data. When considering what is required to satisfy this requirement, consideration should be given to tapes and other removable media containing not only database backups, but also backups of system or application trace files, saveabend files, CPU dumps, TMF dumps and so on.

CLEARONPURGE PARAMETER

The file attribute CLEARONPURGE should be set on any cardholder data files. When a database file/table is purged or dropped from a database with the CLEARONPURGE option set, the data on the disk space is overwritten with zeroes to physically destroy the data space.

CLEARONPURGE increases security for sensitive data or programs. It should be noted that the time for deletion of the file will be increased with this attribute set.

When disks are physically removed from the system, they need to be securely destroyed.

Obsolete tape media needs to be physically destroyed.

THE REQUIREMENT

Req. No	PCI DSS Requirement	Testing Procedure	Remark
9.1	*Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.*	*Verify the existence of physical security controls for each computer room, data centre, and other physical areas with systems in the cardholder data environment.* • *Verify that access is controlled with badge readers or other devices including authorized badges and lock and key.* • *Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use.*	*For this requirement, a QSA will typically observe that the appropriate security requirements are in place. This will normally involve a visit to the data centre and an examination of the security implemented for the datacenter itself, the HP NonStop server, the console, network connections and any other relevant components.* *See System Console Physical Security for further information.*
9.1.1	*Use video cameras or other access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.* *Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*	*Verify that video cameras or other access control mechanisms are in place to monitor the entry/exit points to sensitive areas. Video cameras or other mechanisms should be protected from tampering or disabling. Verify that video cameras or other mechanisms are monitored and that data from cameras or other mechanisms is stored for at least three months.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
9.1.2	*Restrict physical access to publicly accessible network jacks.*	*Verify by interviewing network administrators and by observation that network jacks are enabled only when needed by authorized employees. For example, conference rooms used to host visitors should not have network ports enabled with DHCP. Alternatively, verify that visitors are escorted at all times in areas with active network jacks.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
9.1.3	*Restrict physical access to wireless access points, gateways, and handheld devices.*	*Verify that physical access to wireless access points, gateways, and handheld devices is appropriately restricted.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
9.2 **9.2.a**	*Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible.* *For purposes of this requirement, "employee" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.*	*Review processes and procedures for assigning badges to employees, and visitors, and verify these processes include the following:* • *Granting new badges, changing access requirements, and revoking terminated employee and expired visitor badges* • *Limited access to badge system.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
9.2.b	*Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible.* *For purposes of this requirement, "employee" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.*	*Observe people within the facility to verify that it is easy to distinguish between employees and visitors.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
9.3	*Make sure all visitors are handled as follows:*	*Verify that employee/visitor controls are in place as follows:*	
9.3.1	*Authorized before entering areas where cardholder data is processed or maintained.*	*Observe visitors to verify the use of visitor ID badges. Attempt to gain access to the data center to verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
9.3.2	*Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employee.*	*Examine employee and visitor badges to verify that ID badges clearly distinguish employees from visitors/outsiders and that visitors badges expire.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
9.3.3	*Asked to surrender the physical token before leaving the facility or at the date of expiration.*	*Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
9.4 **9.4.a**	*Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the employee authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.*	*Verify that a visitor log is in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
9.4.b	*Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the employee authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.*	*Verify that the log contains the visitor's name, the firm represented, and the employee authorizing physical access, and is retained for at least three months.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
9.5	*Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.*	*Verify that the storage location is reviewed at least annually to determine that back-up media storage is secure.*	*A document must exist that describes the policies and procedures for storing backup media. This should include backup tapes, DVDs, CDs, TMF media and so on.* *For this requirement, a QSA will typically:* • *Examine evidence showing that the storage location is reviewed at least annually to ensure that the location is secure.* *See Removable Media for further information.*
9.6	*Physically secure all paper and electronic media that contain cardholder data.*	*Verify that procedures for protecting cardholder data include controls for physically securing paper and electronic media (including computers, removable electronic media, networking, and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes).*	*A document must exist that describes the policies and procedures for physically securing backup media. This should include backup tapes, DVDs, CDs, TMF media and so on.* *For this requirement, a QSA will typically:* • *Review the documentation to ensure that the procedure specified in the requirement is adequately documented.* *See Removable Media for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
9.7	*Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data, including the following:*	*Verify that a policy exists to control distribution of media containing cardholder data, and that the policy covers all distributed media including that distributed to individuals.*	*A document must exist that describes the policies and procedures for distribution of backup media. This should include backup tapes, DVDs, CDs, TMF media and so on.* *For this requirement, a QSA will typically:* • *Review the documentation to ensure that the procedure specified in the requirement is adequately documented.* • *Applies to requirement 9.7.1 through 9.7.2* *See Removable Media for further information.*
9.7.1	*Classify the media so it can be identified as confidential.*	*Verify that all media is classified so that it can be identified as "confidential."*	*A document must exist that describes the policies and procedures for classification of backup media. This should include backup tapes, DVDs, CDs, TMF media and so on.* *For this requirement, a QSA will typically:* • *Review the documentation to ensure that the procedure specified in the requirement is adequately documented.* *See Removable Media for further information.*
9.7.2	*Send the media by secured courier or other delivery method that can be accurately tracked.*	*Verify that all media sent outside the facility is logged and authorized by management and sent via secured courier or other delivery method that can be tracked.*	*For this requirement, a QSA will typically:* • *Examine documents showing the date and time that any media has been sent outside of the facility.* • *Ensure that all media movement entries have been authorized.* • *Examine courier documentation or other evidence proving that all media is sent via secured courier or other traceable delivery method.* *This should include movement of backup tapes, DVDs, CDs, TMF media and so on.* *See Removable Media for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
9.8	*Ensure management approves any and all media containing cardholder data that is moved from a secured area (especially when media is distributed to individuals).*	*Select a recent sample of several days of offsite tracking logs for all media containing cardholder data, and verify the presence in the logs of tracking details and proper management authorization.*	*A document must exist that describes the policies and procedures for transferring backup media to offsite storage locations. This should include not only backup tapes, DVDs, CDs and so on, but also TMF media.* *For this requirement, a QSA will typically:* • *Examine the documentation to ensure that this requirement is covered.* • *Examine a recent sample of several days of offsite tracking logs for all media containing cardholder data, and verify the presence in the logs of tracking details and proper management authorization* *See Removable Media for further information.*
9.9	*Maintain strict control over the storage and accessibility of media that contains cardholder data.*	*Obtain and examine the policy for controlling storage and maintenance of hardcopy and electronic media and verify that the policy requires periodic media inventories.*	*A document must exist that describes the storage and handling of backup media. This should include backup tapes, DVDs, CDs, TMF media and so on.* *For this requirement, a QSA will typically:* • *Examine the documentation to ensure that this requirement is covered.* *See Removable Media for further information.*
9.9.1	*Properly maintain inventory logs of all media and conduct media inventories at least annually.*	*Obtain and review the media inventory log to verify that periodic media inventories are performed at least annually.*	*A document must exist that describes the storage and handling of backup media. This should include backup tapes, DVDs, CDs, TMF media and so on.* *For this requirement, a QSA will typically:* • *Examine the documentation to ensure that this requirement is covered.* • *Review the media inventory log to verify that periodic media inventories are performed at least annually.* *See Removable Media for further information.*
9.10	*Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:*	*Obtain and examine the periodic media destruction policy and verify that it covers all media containing cardholder data and confirm the following:*	*A document must exist that describes the secure destruction of any media that contains cardholder data. This should include backup tapes, DVDs, CDs, TMF media, etc.* *For this requirement, a QSA will typically:* • *Examine the documentation to ensure that this requirement is covered.* • *Applies to requirement 9.10.1 through 9.10.2* *See Removable Media for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
9.10.1 **9.10.1.a**	*Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.*	*Verify that hard-copy materials are cross-cut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
9.10.1.b	*Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.*	*Examine storage containers used for information to be destroyed to verify that the containers are secured. For example, verify that a "to-be-shredded" container has a lock preventing access to its contents.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
9.10.2	*Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.*	*Verify that cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).*	*For this requirement, a QSA will typically request to see the following:* • *Evidence that the CLEARONPURGE attribute is set or used as part of purge operations.* • *Evidence of secure destruction of disks such as media movement documents, logs etc.* • *Evidence of secure destruction of obsolete/faulty backup media (including TMF media), faulty/obsolete hard disk that may contain any cardholder data.* • *A document that describes the secure destruction of any media that contains cardholder data. This should include physical disks, backup tapes, TMF media, DVDs, CDs and so on.* *See Clearonpurge Parameter for further information.*

REQUIREMENT 10: TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA

REQUIREMENT INTRODUCTION

The introduction for requirement 10 of PCI DSS states:

> *Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.*

REQUIREMENT DESCRIPTION

Requirement 10 deals with the necessity to maintain audit logs used to track actions and user activity performed on the system. It also covers what the logs must contain and how the logs should be protected to ensure that they are not tampered with in any way.

It is of limited value if logs are captured but never reviewed, so this requirement deals not only with the capturing of logs but also which type of system events need to be reviewed on a regular basis.

NOTE: This requirement does not necessarily cover all types of audit logs and audit events that need to be captured. Most system administrator and DBA access will likely be covered by audit logs referred to in this section. All of the different log types referred to in the section Security Audit Logs should be taken into consideration.

A QSA will be able to assist in determining what type of events need to be captured if there are any additional to those described here due to the varied nature of environments.

ACCESS TO SYSTEM COMPONENTS

It is a part of this requirement to be able to determine what actions a user has performed while accessing the system. This is particularly important for users with elevated system or application privileges. Mechanisms must be in place to ensure that all access to the system can be associated with a specific individual and that these actions can be captured and reported upon.

Safeguard has the ability to capture user access to system objects such as files or devices, but does not have the ability to record exactly what actions a user has performed during a session. For example, if a user were to perform an action within SCF such as modifying the attributes of an object, Safeguard could be configured to provide information detailing that the user had executed the SCF program, but could not tell what the user did once they were inside of SCF.

XYGATE Access Control (XAC) provides the ability to capture all user interactive sessions in conversational or block mode, Guardian or OSS and captures both the input and the output of commands. With XAC it is possible to determine exactly what actions a user has performed during any given session.

If generic userids are in use, a mechanism must be in place to ensure that all user sessions are accountable to a specific individual.

XYGATE User Authentication (XUA) can enforce two step logon so that users must logon to their own individual userid prior to logon to a shared userid such as SUPER.SUPER. The audit trails will then capture exactly which individual userid has logged on to the shared userid.

The XUA Impersonate mechanism provides a facility for tracking exactly which individual has logged on to a GUI based screen such as DSM/SCM using a shared generic userid such as SUPER.SUPER.

INDIVIDUAL ACCESS TO CARDHOLDER DATA

All individual access to cardholder data must be recorded. This would typically be access occurring outside of the application, for example, copying the contents of a file using FUP. For this requirement to be satisfied, all Enscribe files and SQL/MP subvolumes containing cardholder data should be configured in Safeguard with appropriate audit settings. Where possible Safeguard protection of Enscribe files and SQL/MP should be configured at the subvolume level. Safeguard Diskfile records should be added for Enscribe files that have differing security requirements to that configured at the subvolume level. SQL/MP tables cannot be individually protected at the Safeguard diskfile level. All relevant subvolume and diskfile protection records should be configured so that:

- `AUDIT-ACCESS-PASS = ALL`
- `AUDIT-ACCESS-FAIL = ALL`

WARNING! Depending on the nature of the application environment, a setting of AUDIT-ACCESS-PASS = ALL may add significant processing overhead to the system. With this setting, Safeguard will write an audit log event (actually 2 or 3 records) every time the object in question is opened. Implementation of this setting should be fully tested for all relevant objects before being applied to a production environment to ensure that there is no significant impact to system or application performance.

Whereas Safeguard can only audit either all or zero access attempts to a Safeguard protected object, **XYGATE Object Security (XOS)** provides the ability to audit access attempts based on the requesting program. It is possible therefore to configure XOS so that access from authorized and known application objects is not captured, but access attempts from an interactive user session or any non-application process are fully captured. This may significantly reduce the amount of audit captured and reduce the processing overhead on the system.

SQL/MX tables cannot be protected by Safeguard. This means that if cardholder data is stored in SQL/MX tables, another mechanism must be used to audit access to the tables.

XYGATE Access Control (XAC) could be used to audit all user access to SQL/MX tables via interactive MXCI sessions. Likewise, XAC could be used to audit interactive SQLCI sessions for SQL/MP access, and FUP Enable, DBAccess and so on for access to Enscribe files.

RECORDING PRIVILEGED USER ACTIONS

A part of Requirement 10 is to capture all actions taken by any individual with administrative privileges. This would require capturing sessions for the SUPER.SUPER userid at a minimum. As described above, it is not possible for Safeguard to log all actions performed by users on the system.

XYGATE Access Control (XAC) provides the ability to capture all user interactive sessions in conversational or block mode, Guardian or OSS and captures both the input and the output of commands. From XAC it is possible to determine exactly what actions a user has performed during any given session.

ACCESS TO AUDIT TRAILS

Unauthorized access attempts to security audit logs may indicate an attempt to tamper with logs or of an attempt to see which activities have been recorded, so as to determine whether an action may be detected or not. Requirement 10 specifies that access attempts to security audit trails must be recorded and reported upon. Safeguard can be used to capture such access attempts. To configure Safeguard to

capture this information, set the relevant Safeguard records for the Safeguard Audit Pool subvolume, XYGATE audit subvolumes, other security software audit log subvolumes and application security related logfiles (for example BASE24 OMF data) so that:

- `AUDIT-ACCESS-PASS = ALL`
- `AUDIT-ACCESS-FAIL = ALL`

WARNING! A setting of AUDIT-ACCESS-PASS = ALL may add significant processing overhead to the system. With this setting, Safeguard will write an audit log event (actually 2 or 3 records) every time the object in question is opened. Implementation of this setting should be fully tested for all relevant objects before being applied to a production environment to ensure that there is no significant impact to system or application performance.

XYGATE Object Security (XOS) could be used so that auditing is not captured for legitimate specified program access to audit logs, for example the Safeguard processes (*$ZSnn*) writing to the Safeguard audit trail, but full audit is captured for any other access attempts to the log files. This may significantly reduce the amount of audit captured and reduce the processing overhead on the system.

FAILED LOGON ATTEMPTS

All failed logon attempts to the system by userids or aliases must be audited. To achieve this, configure Safeguard so that:

- `AUDIT-AUTHENTICATE-FAIL= ALL`

USERID MANAGEMENT ATTEMPTS

All creation, deletion and modification of userid or alias records must be audited. To achieve this, configure Safeguard so that:

- `SUBJECT-MANAGE-PASS= ALL`
- `SUBJECT-MANAGE-FAIL= ALL`

SECURITY MANAGEMENT EVENTS

If a user is able to manipulate the security subsystems or audit trails, they potentially could hide activities that have occurred on the system that would normally be captured by the security logs. If Safeguard were stopped, for example, not only would security of objects revert back to the Guardian level security, but system or object access attempts would not be logged. To ensure that such occurrences do not go undetected, Requirement 10 specifies that a number of critical events surrounding the security subsystems must be captured. Inherently, Safeguard and XYGATE satisfy the requirement by logging such events as follows:

- Starting and stopping of the Safeguard subsystem causes an event to be raised to the EMS subsystem and a record to be written to the Safeguard audit logs.
- Rollover or changing of Safeguard audit logs causes an event to be raised to the EMS subsystem and a record to be written to the Safeguard audit logs.
- Rollover of XYGATE audit logs raises an EMS event.

Initialization of audit logs and audit log rollover must be logged for any other security related audit logs.

SYSTEM LEVEL OBJECTS

Attempts to create and delete system level objects must be logged. For this requirement to be satisfied, all operating system subvolumes should be configured in Safeguard with appropriate audit settings

- `AUDIT-ACCESS-PASS = ALL`
- `AUDIT-ACCESS-FAIL = ALL`

WARNING! As described for requirement 10.2.1 above, a setting of `AUDIT-ACCESS-PASS = ALL` may add significant processing overhead to the system. With this setting, Safeguard will write an audit log event (actually 2 or 3 records) every time the object in question is opened. Implementation of this setting should be fully tested for relevant objects before being applied to a production environment to ensure that there is no significant impact to system or application performance.

XYGATE Object Security (XOS) provides the ability to audit access attempts based on the operation being performed (e.g. read, write, purge etc). This means that system objects, for example the TACL program, could be audited for Write, Purge or Create operations, but not for operations such as Execute.

SYNCHRONIZATION OF SYSTEM TIME

The system time is logged as part of system or security related events and typically also as part of application related events. It may be difficult to ascertain what has occurred on the system at an exact time if the system clocks across various system or network components are different. Requirement 10 states that all system clocks must be synchronized.

HP provides TIMESYNC software which enables the synchronization of the system clock on an HP NonStop server with a time source on the network.

Given the typical applications running on an HP NonStop server, it is not recommended for the HP NonStop server to be connected to a time source outside of the organization's corporate network. The network time should be obtained from a time source within the network.

ACCESS TO AUDIT LOGS

As the audit logs on the system provide the record of what has occurred on the system, it is imperative that they are protected and that access is monitored so as to detect any unauthorized access attempts. Such attempts may indicate a potential security breach.

A Safeguard subvolume record should be configured to protect the Safeguard audit pool from access to unauthorized persons. By default, SUPER.SUPER owns the Safeguard audit files and has full access. Other users that require access to the audit log files, such as security administrators who need to run security reports, should be configured with Read access to the Safeguard Audit Pool.

By default, XYGATE logs are owned by the user that the relevant XYGATE module runs under. This userid will need full access to the XYGATE audit trails to be able to create logs, write to the logs etc. As such, this userid should be treated as a privileged userid on the system. Access requirements for XYGATE audit logs should be analyzed and Safeguard ACLs put in place providing Read only access to relevant authorized users, such as security administrators, as for Safeguard.

As the access requirements for XYGATE audit trails are typically different to the access requirement to other files in the XYGATE module subvolumes, the audit trails should be configured to be in separate dedicated subvolumes. This is configured in the relevant *xx*CONF file for the module with an entry such as:

```
AUDIT $LOG00.XYGACLOG.AUDIT INVOKE DETAIL
```

No user other than SUPER.SUPER should have Write access to the Safeguard Audit Pool. No user other than the XYGATE owner userid should have Write access to the XYGATE Audit Trails. Relevant subvolumes should be controlled through the use of Safeguard subvolume records with appropriate ACL configuration. Likewise for any third party security software audit trails, relevant security related application audit trails, and so on.

STORAGE OF AUDIT LOGS

One method of decreasing the chances of audit logs being tampered with in any way is for them to be sent to a centralized audit log repository. This is typically a device or system on the network whose sole purpose is to collect security logs for storage and for running of reports and raising alerts. Safeguard does not have the facility to write audit trail data to a centralized server.

XYGATE Merged Audit (XMA) can send audit trail data in real time from Safeguard, XYGATE, EMS and BASE24 to a centralized server , for example HP CLW or RSA enVision®, in syslog message format .

If relevant audit trail data is stored locally on the HP NonStop server and nowhere else, there needs to be some kind of File Integrity Monitoring (FIM) in place that can monitor whether any changes have occurred to existing log data. This is not easily achievable in the NonStop world.

XYGATE Object Security (XOS) provides the ability to secure and audit access attempts based on the requesting program and also the operation performed. This means that XOS could be used, for example, to raise an audit event if any attempt is made to write to the Safeguard audit trail file by any program other than Safeguard itself. It can also provide the security to not allow any program other than Safeguard itself to write to the Safeguard audit trail. That would prevent any user logged on as SUPER.SUPER, for example, from being able to write to the logs using some other program.

XYGATE Merged Audit (XMA) could be configured to alert on events from XOS such as an access attempt being made to write to the Safeguard audit trail by an unauthorized program. XMA can generate alerts in syslog, SNMP, SMTP mail, or EMS formats.

AUDIT LOG RETENTION

Security policy documentation must include details of audit log retention. The time period specified must be a minimum of 12 months.

The audit trails to be kept should include those from Safeguard, XYGATE, application related security logs (e.g. BASE24 OMF logs) and any third party security logs.

It is advisable that security audit trails are monitored to ensure that they are not rolling over too quickly causing events to be overwritten prematurely. If Safeguard is sized incorrectly or if something goes wrong and unexpected events flood the Safeguard logs, it is possible that audit data could be lost. Likewise for audit logs from the other sources.

SECURITY REPORTS

The whole point of capturing the events that occur on the system is so that reports can be run to determine what has happened and when. Requirement 10 specifies how often particular security events need to be reviewed.

Safeguard does not come with a useful reporting tool, just the Safeguard Audit Reduction Tool (SAFEART) which is in essence a tool for dumping complete audit records and is not very user friendly.

XYGATE Safeguard Reports (XSR) can be used to report on events captured by Safeguard and stored in the Safeguard audit trail.

XYGATE Merged Audit (XMA) can be used to report on Safeguard events but also on events from XYGATE modules, selected EMS events and BASE24 OMF logs. XMA also has the ability to raise alerts from these subsystems in syslog, SNMP, SMTP (i.e. email), EMS formats.

All XYGATE modules come bundled with a GUI based reporting facility, **XYGATE Report Manager (XRM)**.

THE REQUIREMENT

Req. No	PCI DSS Requirement	Testing Procedure	Remark
10.1	*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*	*Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.*	*For this requirement, a QSA will typically analyze the exact mechanism used for tracking user system activities and will typically want evidence of the following:* • *That Safeguard is running and fully operable.* • *That appropriate Safeguard audit settings are configured. That is, Safeguard globals or individual userids/aliases are set as follows* ○ *AUDIT-AUTHENTICATE-PASS = ALL* • *That appropriate auditing is turned on for XYGATE and any third party security tools.* • *That application level security auditing is configured and operable.* *See Access to System Components for further information.*
10.2	*Implement automated audit trails for all system components to reconstruct the following events:*	*Through interviews, examination of audit logs, and examination of audit log settings, perform the following:*	
10.2.1	*All individual accesses to cardholder data.*	*Verify all individual access to cardholder data is logged.*	*For this requirement, a QSA will typically require the following:* • *An interview to ask how the event is captured.* • *Evidence of the relevant configuration settings.* • *Evidence of the event being logged (e.g. sample log file).* *See Individual Access to Cardholder Data for further information.*
10.2.2	*All actions taken by any individual with root or administrative privileges.*	*Verify actions taken by any individual with root or administrative privileges is logged.*	*For this requirement, a QSA will typically require the following:* • *An interview to ask how the event is captured.* • *Evidence of the relevant configuration settings.* • *Evidence of the event being logged (e.g. sample log file).* *See Recording Privileged User Actions for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
10.2.3	*Access to all audit trails.*	*Verify access to all audit trails is logged.*	*For this requirement, a QSA will typically require the following:* • *An interview to ask how the event is captured.* • *Evidence of the relevant configuration settings.* • *Evidence of the event being logged (e.g. sample log file).* *See Access to Audit Trails for further information.*
10.2.4	*Invalid logical access attempts.*	*Verify invalid logical access attempts are logged.*	*For this requirement, a QSA will typically require the following:* • *An interview to ask how the event is captured.* • *Evidence of the relevant configuration settings.* • *Evidence of the event being logged (e.g. sample log file).* *See Failed Logon Attempts for further information.*
10.2.5	*Use of identification and authentication mechanisms.*	*Verify use of identification and authentication mechanisms is logged.*	*For this requirement, a QSA will typically require the following:* • *An interview to ask how the event is captured.* • *Evidence of the relevant configuration settings.* • *Evidence of the event being logged (e.g. sample log file).* *See Userid Management Attempts for further information.*
10.2.6	*Initialization of the audit logs.*	*Verify initialization of audit logs is logged.*	*For this requirement, a QSA will typically require the following:* • *An interview to ask how the event is captured.* • *Evidence of the relevant configuration settings.* • *Evidence of the event being logged (e.g. sample log file).* *See Security Management Events for further information.*
10.2.7	*Creation and deletion of system-level objects.*	*Verify creation and deletion of system level objects are logged.*	*For this requirement, a QSA will typically require the following:* • *An interview to ask how the event is captured.* • *Evidence of the relevant configuration settings.* • *Evidence of the event being logged (e.g. sample log file).* *See System level Objects for further information.*

Req. No	***PCI DSS Requirement***	***Testing Procedure***	***Remark***
10.3	*Record at least the following audit trail entries for all system components for each event:*	*Through interviews and observation, for each auditable event (from 10.2), perform the following:*	

Requirement 10.3 describes what information must be captured in all security related events. Safeguard and XYGATE audit satisfy this requirement.

Check that any other audit trails such as those listed in the section on Security Audit Logs also contain the required information.

A Safeguard logon (verifyuser) audit report generated using SAFEART is provided as a sample for requirements 10.3.1 through 10.3.6. In the example, the user KCTEST.GREG has logged on to KNIGHT.GREG.

For information on reading Safeguard audit trails using SAFEART and for a description of the various Safeguard audit record fields, see the *HP Safeguard Audit Services Manual* in the HP NonStop Technical Library. While the SAFEART tool is not recommended by the authors for day to day reporting due to the volume of information provided, it provides the complete Safeguard audit record so has been used here to provide examples.

Req. No	*PCI DSS Requirement*	*Testing Procedure*	*Remark*
10.3.1	*User identification.*	*Verify user identification is included in log entries.*	*For this requirement, a QSA will typically:* • *Examine evidence in the form of audit event logs or samples.*

The example below shows that the user who performed the logon operation was KCTEST.GREG with a user number of 86,201 on the \X system.

```
--------------------------------------------------------------------------------
Auditnumber           =FFFF02F1B299673301CF
TimeReported          =2010/08/02 01:12:24 TimeReceived        =2010/08/02 01:12:24
Operation             =VerifyUser          Outcome             =UserValid
ObjectType            =GuardianUser        Veracity            =Tr
OwnerUsername         =SECURITY.ADMIN      OwnerUsernumber     =253,001
OwnerIsRemote         =Remote
SubjectUserName       =KCTEST.GREG
SubjectUserNumber     =086,201             SubjectSystemName   =\X
SubjectCreatorName    =KCTEST.GREG         SubjectCreatorNumber =086,201
SubjectSystemNumber   =7
SubjectProcessName    =\X.$Y42Z
SubjectAuthlocName    =\X
SubjectTerminalName   =\X.$Y42Y.#IN
SubjectAuthlocNumber  =7
CreatorUserName       =SUPER.SUPER
CreatorUserNumber     =255,255             CreatorSystemName    =\X
CreatorCreatorName    =SUPER.SUPER         CreatorCreatorNumber =255,255
CreatorSystemNumber   =7
CreatorProcessName    =\X.$ZSMP
CreatorAuthlocName    =\X
CreatorTerminalName   =\X.$YMIOP.#CLCI
CreatorAuthlocNumber  =7
GuarduserUserName     =KNIGHT.GREG         GuarduserUserNumber  =107,082
UserAliasName         =
UserPrivLogonOper     =False
UserCreatorNumber     =000,000             UserCreatorName      =
UserCreatorIsAlias    =False               UserCreatorNodeNumber =0
UserCreationTime      =
--------------------------------------------------------------------------------
```

Req. No	PCI DSS Requirement	Testing Procedure	Remark
10.3.2	*Type of event.*	*Verify type of event is included in log entries.*	*For this requirement, a QSA will typically:* • *Examine evidence in the form of audit event logs or samples.*

The example below shows that the operation performed was a Verifyuser operation performed on a Guardian user, that is, a user logging on to the system. Note that there are several types of authentication procedures used for "logging on" to an HP NonStop server. These are logon, authenticate, verifyuser, privlogon.

```
--------------------------------------------------------------------------------
Auditnumber           =FFFF02F1B299673301CF
TimeReported          =2010/08/02 01:12:24 TimeReceived        =2010/08/02 01:12:24
Operation             =VerifyUser          Outcome             =UserValid
ObjectType            =GuardianUser        Veracity            =Tr
OwnerUsername         =SECURITY.ADMIN      OwnerUsernumber     =253,001
OwnerIsRemote         =Remote
SubjectUserName       =KCTEST.GREG
SubjectUserNumber     =086,201             SubjectSystemName   =\X
SubjectCreatorName    =KCTEST.GREG         SubjectCreatorNumber =086,201
SubjectSystemNumber   =7
SubjectProcessName    =\X.$Y42Z
SubjectAuthlocName    =\X
SubjectTerminalName   =\X.$Y42Y.#IN
SubjectAuthlocNumber  =7
CreatorUserName       =SUPER.SUPER
CreatorUserNumber     =255,255             CreatorSystemName    =\X
CreatorCreatorName    =SUPER.SUPER         CreatorCreatorNumber =255,255
CreatorSystemNumber   =7
CreatorProcessName    =\X.$ZSMP
CreatorAuthlocName    =\X
CreatorTerminalName   =\X.$YMIOP.#CLCI
CreatorAuthlocNumber  =7
GuarduserUserName     =KNIGHT.GREG         GuarduserUserNumber  =107,082
UserAliasName         =
UserPrivLogonOper     =False
UserCreatorNumber     =000,000             UserCreatorName      =
UserCreatorIsAlias    =False               UserCreatorNodeNumber =0
UserCreationTime      =
--------------------------------------------------------------------------------
```

Req. No	PCI DSS Requirement	Testing Procedure	Remark
10.3.3	*Date and time.*	*Verify date and time stamp is included in log entries.*	*For this requirement, a QSA will typically:* • *Examine evidence in the form of audit event logs or samples.*

The example below shows the time that the logon event was generated and the time that it was written to the log.

```
--------------------------------------------------------------------------------
Auditnumber           =FFFF02F1B299673301CF
TimeReported          =2010/08/02 01:12:24 TimeReceived        =2010/08/02 01:12:24
Operation             =VerifyUser          Outcome             =UserValid
ObjectType            =GuardianUser        Veracity            =Tr
OwnerUsername         =SECURITY.ADMIN      OwnerUsernumber     =253,001
OwnerIsRemote         =Remote
SubjectUserName       =KCTEST.GREG
SubjectUserNumber     =086,201             SubjectSystemName   =\X
SubjectCreatorName    =KCTEST.GREG         SubjectCreatorNumber =086,201
SubjectSystemNumber   =7
SubjectProcessName    =\X.$Y42Z
SubjectAuthlocName    =\X
SubjectTerminalName   =\X.$Y42Y.#IN
SubjectAuthlocNumber  =7
CreatorUserName       =SUPER.SUPER
CreatorUserNumber     =255,255             CreatorSystemName    =\X
CreatorCreatorName    =SUPER.SUPER         CreatorCreatorNumber =255,255
CreatorSystemNumber   =7
CreatorProcessName    =\X.$ZSMP
CreatorAuthlocName    =\X
CreatorTerminalName   =\X.$YMIOP.#CLCI
CreatorAuthlocNumber  =7
GuarduserUserName     =KNIGHT.GREG         GuarduserUserNumber  =107,082
UserAliasName         =
UserPrivLogonOper     =False
UserCreatorNumber     =000,000             UserCreatorName      =
UserCreatorIsAlias    =False               UserCreatorNodeNumber =0
UserCreationTime      =
--------------------------------------------------------------------------------
```

Req. No	PCI DSS Requirement	Testing Procedure	Remark
10.3.4	*Success or failure indication.*	*Verify success or failure indication is included in log entries.*	*For this requirement, a QSA will typically:* • *Examine evidence in the form of audit event logs or samples.*

The example below shows that the outcome of the operation was “UserValid”. This is described in the HP *Safeguard Audit Services Manual* as “the user was successfully authenticated”.

```
--------------------------------------------------------------------------------
Auditnumber           =FFFF02F1B299673301CF
TimeReported          =2010/08/02 01:12:24 TimeReceived        =2010/08/02 01:12:24
Operation             =VerifyUser          Outcome             =UserValid
ObjectType            =GuardianUser        Veracity            =Tr
OwnerUsername         =SECURITY.ADMIN      OwnerUsernumber     =253,001
OwnerIsRemote         =Remote
SubjectUserName       =KCTEST.GREG
SubjectUserNumber     =086,201             SubjectSystemName   =\X
SubjectCreatorName    =KCTEST.GREG         SubjectCreatorNumber =086,201
SubjectSystemNumber   =7
SubjectProcessName    =\X.$Y42Z
SubjectAuthlocName    =\X
SubjectTerminalName   =\X.$Y42Y.#IN
SubjectAuthlocNumber  =7
CreatorUserName       =SUPER.SUPER
CreatorUserNumber     =255,255             CreatorSystemName    =\X
CreatorCreatorName    =SUPER.SUPER         CreatorCreatorNumber =255,255
CreatorSystemNumber   =7
CreatorProcessName    =\X.$ZSMP
CreatorAuthlocName    =\X
CreatorTerminalName   =\X.$YMIOP.#CLCI
CreatorAuthlocNumber  =7
GuarduserUserName     =KNIGHT.GREG         GuarduserUserNumber  =107,082
UserAliasName         =
UserPrivLogonOper     =False
UserCreatorNumber     =000,000             UserCreatorName      =
UserCreatorIsAlias    =False               UserCreatorNodeNumber =0
UserCreationTime      =
--------------------------------------------------------------------------------
```

Req. No	PCI DSS Requirement	Testing Procedure	Remark
10.3.5	*Origination of event.*	*Verify origination of event is included in log entries.*	*For this requirement, a QSA will typically:* • *Examine evidence in the form of audit event logs or samples.*

The example below shows that the logon event originated from the process named $Y42Z on the \X system, and was performed from a terminal named $Y42Y.#IN on the \X system.

```
-------------------------------------------------------------------------------
Auditnumber           =FFFF02F1B299673301CF
TimeReported          =2010/08/02 01:12:24 TimeReceived        =2010/08/02 01:12:24
Operation             =VerifyUser          Outcome             =UserValid
ObjectType            =GuardianUser        Veracity            =Tr
OwnerUsername         =SECURITY.ADMIN      OwnerUsernumber     =253,001
OwnerIsRemote         =Remote
SubjectUserName       =KCTEST.GREG
SubjectUserNumber     =086,201             SubjectSystemName   =\X
SubjectCreatorName    =KCTEST.GREG         SubjectCreatorNumber =086,201
SubjectSystemNumber   =7
SubjectProcessName    =\X.$Y42Z
SubjectAuthlocName    =\X
SubjectTerminalName   =\X.$Y42Y.#IN
SubjectAuthlocNumber  =7
CreatorUserName       =SUPER.SUPER
CreatorUserNumber     =255,255             CreatorSystemName    =\X
CreatorCreatorName    =SUPER.SUPER         CreatorCreatorNumber =255,255
CreatorSystemNumber   =7
CreatorProcessName    =\X.$ZSMP
CreatorAuthlocName    =\X
CreatorTerminalName   =\X.$YMIOP.#CLCI
CreatorAuthlocNumber  =7
GuarduserUserName     =KNIGHT.GREG         GuarduserUserNumber  =107,082
UserAliasName         =
UserPrivLogonOper     =False
UserCreatorNumber     =000,000             UserCreatorName      =
UserCreatorIsAlias    =False               UserCreatorNodeNumber =0
UserCreationTime      =
-------------------------------------------------------------------------------
```

Req. No	PCI DSS Requirement	Testing Procedure	Remark
10.3.6	*Identity or name of affected data, system component, or resource.*	*Verify identity or name of affected data, system component, or resources is included in log entries.*	*For this requirement, a QSA will typically:* • *Examine evidence in the form of audit event logs or samples.*

The example below shows that the logon attempt was made to the userid KNIGHT.GREG which has a user number of 107,82.

```
--------------------------------------------------------------------------------
Auditnumber           =FFFF02F1B299673301CF
TimeReported          =2010/08/02 01:12:24 TimeReceived        =2010/08/02 01:12:24
Operation             =VerifyUser          Outcome             =UserValid
ObjectType            =GuardianUser        Veracity            =Tr
OwnerUsername         =SECURITY.ADMIN      OwnerUsernumber     =253,001
OwnerIsRemote         =Remote
SubjectUserName       =KCTEST.GREG
SubjectUserNumber     =086,201             SubjectSystemName   =\X
SubjectCreatorName    =KCTEST.GREG         SubjectCreatorNumber =086,201
SubjectSystemNumber   =7
SubjectProcessName    =\X.$Y42Z
SubjectAuthlocName    =\X
SubjectTerminalName   =\X.$Y42Y.#IN
SubjectAuthlocNumber  =7
CreatorUserName       =SUPER.SUPER
CreatorUserNumber     =255,255             CreatorSystemName    =\X
CreatorCreatorName    =SUPER.SUPER         CreatorCreatorNumber =255,255
CreatorSystemNumber   =7
CreatorProcessName    =\X.$ZSMP
CreatorAuthlocName    =\X
CreatorTerminalName   =\X.$YMIOP.#CLCI
CreatorAuthlocNumber  =7
GuarduserUserName     =KNIGHT.GREG         GuarduserUserNumber  =107,082
UserAliasName         =
UserPrivLogonOper     =False
UserCreatorNumber     =000,000             UserCreatorName      =
UserCreatorIsAlias    =False               UserCreatorNodeNumber =0
UserCreationTime      =
--------------------------------------------------------------------------------
```

Req. No	PCI DSS Requirement	Testing Procedure	Remark
10.4	*Synchronize all critical system clocks and times.*	*Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components. Verify the following is included in the process and implemented:*	*For this requirement, a QSA will typically want to see evidence that an automated time Synchronization mechanism such as TIMESYNC (from HP) is running on the system and that it is documented. They will likely want to see evidence of the configuration to confirm that it is set appropriately and that it is configured as described in the documentation. Typical configuration items that a QSA may look for are:* • *The TCP/IP process that the time synchronization process communicates through.* • *The name and IP address of the NTP time server used for time synchronization.* *The QSA will also likely want to see evidence of a successful synchronization of the system time, for example, from an event log. This should indicate the time that the synchronization took place and the time difference before the reset.* *See Synchronization of System Time for further information.*
10.4.a	*Synchronize all critical system clocks and times.*	*Verify that a known, stable version of NTP (Network Time Protocol) or similar technology, kept current per PCI DSS Requirements 6.1 and 6.2, is used for time synchronization.*	*For this requirement, a QSA will typically want to ensure that the time synchronization software is current. This may involve:* • *In the case of TIMESYNC, checking VPROC of the time synchronization object and matching against the HP website (latest SPRs) to see that they match. The Non-Stop Software Product Maintenance List, which can be obtained from the HP website, will show the latest version of the TIMESYNC product.* • *Checking the documentation to ensure that it contains a section stating that the latest version of Timesync (or equivalent) must be used and kept up to date.* *See Synchronization of System Time for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
10.4.b	*Synchronize all critical system clocks and times.*	*Verify that internal servers are not all receiving time signals from external sources. [Two or three central time servers within the organization receive external time signals [directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT)], peer with each other to keep accurate time, and share the time with other internal servers.]*	*For this requirement, a QSA will typically:* • *Request to see a network diagram displaying connectivity of the HP NonStop servers to the time synchronization server* • *Verify that the network diagram details information such as server IP Addresses.* *See Synchronization of System Time for further information.*
10.4.c	*Synchronize all critical system clocks and times.*	*Verify that specific external hosts are designated from which the timeservers will accept NTP time updates (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers).* *See www.ntp.org for more information*	*This requirement applies only to systems receiving the time source from outside of the corporate network. Given the typical usage of HP NonStop servers within an organization, it is not recommended that HP NonStop servers receive the time source in this manner.* *See Synchronization of System Time for further information.*
10.5	*Secure audit trails so they cannot be altered.*	*Interview system administrator and examine permissions to verify that audit trails are secured so that they cannot be altered as follows:*	*For requirement 10.5.1 through 10.5.5, a QSA will typically:* • *Interview staff to verify that the security of the audit trails complies with the standard. For example, if a user claims that they cannot access the audit logs, the QSA may ask that user to logon and show that they receive a security error when attempting to access the logs.* • *Ask to see the policy document where access to the security audit trails is described.* • *Ask to see the corresponding system settings* *Note that this requirement will include XYGATE audit trails, any third party security software audit trails, relevant security related application audit trails (for example BASE24 OMF audit data) as well as Safeguard audit trails.* *See Access to audit logs for further information.*
10.5.1	*Limit viewing of audit trails to those with a job-related need.*	*Verify that only individuals who have a job-related need can view audit trail files.*	*For this requirement, a QSA will typically:* • *Examine Safeguard records that protect the relevant audit trail subvolumes to ensure that they are satisfactory.* *See Access to audit logs for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
10.5.2	*Protect audit trail files from unauthorized modifications.*	*Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.*	*For this requirement, a QSA will typically:* • *Interview relevant personnel to discover how audit trails are protected.* • *Examine Safeguard records that protect the relevant audit trail subvolumes to ensure that they are satisfactory.* *See Access to audit logs for further information.*
10.5.3	*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*	*Verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.*	*For this requirement, a QSA will typically:* • *Interview relevant personnel to discover the process for satisfying the requirement.* • *Examine the configuration to ensure that the mechanism has been implemented as stated.* • *Observe sample audit trail data being written to a centralized server.* *See Storage of Audit Logs for further information.*
10.5.4	*Write logs for external-facing technologies onto a log server on the internal LAN.*	*Verify that logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are offloaded or copied onto a secure centralized internal log server or media.*	*This requirement is only relevant if the HP NonStop server is running a web server from within the DMZ of the organizational network. This is not a typical role for an HP NonStop server and so this requirement is typically not applicable.* *In the rare cases where organizations do use the NonStop for this type of activity, a tool such as **XYGATE Merged Audit (XMA)** would be required to write audit trail data to a centralized logging system.* *See Storage of Audit Logs for further information.*
10.5.5	*Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*	*Verify the use of file-integrity monitoring or change-detection software for logs by examining system settings and monitored files and results from monitoring activities.*	*If audit trail data is stored locally on the system and not on a centralized logging repository.* *For this requirement, a QSA will typically:* • *Ask for a description of what mechanism is in use to ensure the integrity of the security audit trail.* • *Require a demonstration of the mechanism used to ensure the integrity of the security audit trail.* • *Examine evidence of the configuration settings used to fulfill this requirement.* *See Storage of Audit Logs for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
10.6 **10.6.a**	*Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).* *Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6*	*Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required.*	*This requirement is a procedural item indicating that a documented policy must exist for examining security logs daily for events. The document must specify the running of daily reports/raising of alerts as per events detailed in Requirements 10.2.1 through 10.2.7.* *For this requirement, a QSA will typically:* • *Request to see the relevant document describing the policy.* *See Security Reports for further information.*
10.6.b	*Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).* *Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6*	*Through observation and interviews, verify that regular log reviews are performed for all system components.*	*For this requirement, a QSA will typically:* • *Interview the person who reviews the reports and/or alerts described in the policy document referred to in Requirement 10.6.a and verify that these are received and reviewed.* • *Ask to see evidence of the reports or samples of the alerts.* *See Security Reports for further information.*
10.7.a	*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 back-up).*	*Obtain and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year.*	*For this requirement, a QSA will typically:* • *Examine the policy documentation to ensure that the document includes details of audit trail retention.* *See Audit Log Retention for further information.*
10.7.b	*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 back-up).*	*Verify that audit logs are available for at least one year and processes are in place to restore at least the last three months' logs for immediate analysis.*	*For this requirement, a QSA will typically:* • *Check the location of the security audit logs.* • *Check the configuration in regards to size of audit pool and maximum number of files to retain in the pool, where applicable.* • *Verify that logs for the past 12 months are available.* • *Verify that logs from the past 3 months can be restored within a couple of hours if they are not stored online. This may involve a request to talk through the procedure of restoring logs to a state where they can be viewed, or if necessary, a request to perform the restore and run a report to confirm that the logs are valid and readable.* *See Audit Log Retention for further information.*

REQUIREMENT 11: REGULARLY TEST SECURITY SYSTEMS AND PROCESSES.

REQUIREMENT INTRODUCTION

The introduction for requirement 11 of PCI DSS states:

> *Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.*

REQUIREMENT DESCRIPTION

It is imperative to ensure that what is running on the system is what should be running on the system. Requirement 11 deals with the need for monitoring and regular testing against vulnerabilities so as to ensure the integrity of the system and application.

FILE INTEGRITY MONITORING

Part of this requirement is to ensure that there are no unauthorized changes to critical files on the system. This means that such files need to be monitored for any change by use of a File Integrity Monitor. There is no standard HP tool that provides the function of file integrity monitoring.

XYGATE Security Compliance Wizard (XSW) provides a file integrity monitoring function that allows for the monitoring of entire subvolumes or individual files for change of any kind, including attributes of the file such as owner, security, progid, licensed as well as monitoring for changes to the contents of the file. If a monitored file is detected as being different from the baseline file in any way, XSW triggers an alert.

XYGATE Merged Audit (XMA) can be configured to alert on access attempts to modify Safeguard or **XYGATE Object Security (XOS)** protected and audited files. XOS has the added ability of being able to audit based on operation so that it would be possible to alert on a write attempt to a critical file, but not audit when, for example, a user executes or reads the file.

THE REQUIREMENT

Req. No	PCI DSS Requirement	Testing Procedure	Remark
11.1 **11.1.a**	*Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.*	*Verify that a wireless analyzer is used at least quarterly, or that a wireless IDS/IPS is implemented and configured to identify all wireless devices.*	*This requirement is generally not applicable to the HP NonStop server. Requirements related to wireless access points are typically the responsibility of networking personnel within the organization.*
11.1.b	*Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.*	*If a wireless IDS/IPS is implemented, verify the configuration will generate alerts to personnel.*	*This requirement is generally not applicable to the HP NonStop server. Requirements related to wireless access points are typically the responsibility of networking personnel within the organization.*
11.1.c	*Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.*	*Verify the organization's Incident Response Plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.*	*This requirement is generally not applicable to the HP NonStop server. Requirements related to wireless access points are typically the responsibility of networking personnel within the organization.*
11.2 **11.2.a**	*Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).* *Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal staff.*	*Inspect output from the most recent four quarters of internal network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder data environment occurs. Verify that the scan process includes rescans until passing results are obtained.* *Note: External scans conducted after network changes, and internal scans, may be performed by the company's qualified internal personnel or third parties.*	*HP NonStop servers must be included in any internal vulnerability scans.* *For this requirement, a QSA will typically:* • *Examine documentation that covers the requirement.* • *Interview security personnel to see how the requirement is met and to confirm that the methods used align with the documentation.* • *Examine dated scan results (clean scan results) to see that the scan has been performed at least every quarter.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
11.2.b	*Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).* *Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal staff.*	*Verify that external scanning is occurring on a quarterly basis in accordance with the PCI Security* *Scanning Procedures, by inspecting output from the four most recent quarters of external vulnerability scans to verify that:* • *Four quarterly scans occurred in the most recent 12-month period;* • *The results of each scan satisfy the PCI Security Scanning Procedures (for example, no urgent, critical, or high vulnerabilities);* • *The scans were completed by an Approved Scanning Vendor (ASV) qualified by PCI SSC.* *Note: It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.*	*An external network vulnerability scan is a scan of ports on public facing IP addresses and needs to be performed by an Approved Scanning Vendor (ASV). This scan will include access to any public facing IP interface (i.e. configured TCP/IP subnets) on the HP NonStop server.* *For this requirement, a QSA will typically:* • *Examine documentation that covers the requirement.* • *Interview security personnel to see how the requirement is met and to confirm that the methods used align with the documentation.* • *Examine dated scan results (clean scan results) to see that the scan has been performed at least every quarter.*
11.2.c	*Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).* *Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal staff.*	*Verify that internal and/or external scanning is performed after any significant change in the network, by inspecting scan results for the last year. Verify that the scan process includes rescans until passing results are obtained.*	*This requirement applies to both internal and external scans. As such it applies to ports on all TCP/IP subnets configured on the HP NonStop server.* *For this requirement, a QSA will typically:* • *Examine documentation that covers the requirement.* • *Interview security personnel to see how the requirement is met and to confirm that the methods used align with the documentation.* • *Examine dated scan results (clean scan results) to see that the scan has been performed at least every quarter.* • *Examine dated scan results (clean scan results) to see that the scan has been performed after any significant change in the network/operating system. e.g. after rolling out a new version of the OS, applying SPRs or adding new software.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
11.3 **11.3.a**	*Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:*	*Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment. Verify that noted vulnerabilities were corrected and testing repeated.*	*This requirement applies to both internal and external penetration testing. As such it applies to ports on all TCP/IP subnets configured on the HP NonStop server.* *For this requirement, a QSA will typically:* • *Examine documentation that covers the requirement.* • *Interview security personnel to see how the requirement is met and to confirm that the methods used align with the documentation.* • *Examine dated internal and external penetration test results (clean test results) to see that the test has been performed at least every year and after any significant change in the network/operating system. e.g. rolling out new version of the OS, installation of SPRs, adding new software.*
11.3.b	*Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:*	*Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).*	*This requirement applies to both internal and external penetration testing. As such it applies to ports on all TCP/IP subnets configured on the HP NonStop server.* *For this requirement, a QSA will typically:* • *Examine documentation that covers the requirement.* • *Interview security personnel to see how the requirement is met and to confirm that the methods used align with the documentation.* • *Confirm that testing was performed by a qualified internal resource (independent) or a qualified external 3rd party. The QSA will question the qualification of the tester if they feel it is required.*
11.3.1	*Network-layer penetration tests.*	*Verify that the penetration test includes network layer penetration tests. These tests should include components that support network functions as well as operating systems.*	*This requirement applies to both internal and external penetration testing. As such it applies to ports on all TCP/IP subnets configured on the HP NonStop server.* *For this requirement, a QSA will typically:* • *Examine documentation that covers the requirement.* • *Interview security personnel to see how the requirement is met and to confirm that the methods used align with the documentation.* • *Confirm that testing was performed in the network layer. This will include testing of operating system components.*

Req. No	*PCI DSS Requirement*	*Testing Procedure*	*Remark*
11.3.2	*Application-layer penetration tests.*	*Verify that the penetration test includes application-layer penetration tests. For web applications, the tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5.*	*This requirement applies to both internal and external penetration testing. As such it applies to ports on all TCP/IP subnets configured on the HP NonStop server.* *For this requirement, a QSA will typically:* • *Examine documentation that covers the requirement.* • *Interview security personnel to see how the requirement is met and to confirm that the methods used align with the documentation.* • *Confirm that testing was performed in the application layer.* • *Web applications must include OWASP Top 10 vulnerability testing.*
11.4 ***11.4.a***	*Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.*	*Verify the use of intrusion-detection systems and/or intrusion-prevention systems and that all traffic in the cardholder data environment is monitored.*	*This requirement is generally not applicable to the HP NonStop server. Requirements related to intrusion-detection or intrusion-prevention systems are typically the responsibility of networking personnel within the organization.*
11.4.b	*Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.*	*Confirm IDS and/or IPS are configured to alert personnel of suspected compromises.*	*This requirement is generally not applicable to the HP NonStop server. Requirements related to intrusion-detection or intrusion-prevention systems are typically the responsibility of networking personnel within the organization.* **HP NonStop server**
11.4.c	*Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.*	*Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.*	*This requirement is generally not applicable to the HP NonStop server. Requirements related to intrusion-detection or intrusion-prevention systems are typically the responsibility of networking personnel within the organization.*

Req. No	***PCI DSS Requirement***	***Testing Procedure***	***Remark***
11.5	*Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.* *Note: For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*	*Verify the use of file-integrity monitoring products within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities.* *Examples of files that should be monitored:* • *System executables* • *Application executables* • *Configuration and parameter files* • *Centrally stored, historical or archived, log and audit files.*	*For this requirement, a QSA will typically:* • *Examine configuration settings and the process used for file integrity monitoring.* *See File Integrity Monitoring for further information.*

REQUIREMENT 12: MAINTAIN A POLICY THAT ADDRESSES INFORMATION SECURITY FOR EMPLOYEES AND CONTRACTORS

REQUIREMENT INTRODUCTION

The introduction for requirement 12 of PCI DSS states:

> *A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of this requirement, "employees" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the company's site.*

REQUIREMENT DESCRIPTION

The requirements in this section are all in regards to documentation. In reality, this section is the ideal place to start the process of approaching PCI DSS compliance. As all aspects of configuration, policies and procedures contained in the other 11 requirements need to be documented, starting with this section may help provide an overview of what is required for the organization to comply with PCI DSS.

A large number of the requirements in this section will typically be related to the policies and procedures of the organization in general. Some may apply specifically to the HP NonStop server environment. This will vary from one organization to another depending on individual business practices and circumstances.

For all requirements listed in this section, a QSA will typically:

- Review the documentation and ensure that the required information is included
- Observe processes and procedures to ensure that they are followed as specified in the documentation.
- In some cases, a QSA will also interview relevant personnel to ascertain further information or to confirm that the processes and procedures are followed as documented.

All PCI DSS requirements for this section of the specification are listed for the sake of completeness. For requirements where there is more likely to be specific relevance to the HP NonStop server environment, notes and recommendations have been included.

THE REQUIREMENT

Req. No	PCI DSS Requirement	Testing Procedure	Remark
12.1	*Establish, publish, maintain, and disseminate a security policy that accomplishes the following:*	*Examine the information security policy and verify that the policy is published and disseminated to all relevant system users (including vendors, contractors, and business partners).*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.1.1	*Addresses all PCI DSS requirements.*	*Verify that the policy addresses all PCI DSS requirements.*	*This requirement is all encompassing, essentially saying that documentation must exist describing exactly how all of the requirements of PCI DSS are being met.* *For this requirement, a QSA will typically:* • *Examine the documentation, likely in conjunction with examining all of the specific requirements of PCI DSS.*
12.1.2	*Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.*	*Verify that the information security policy includes an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.1.3	*Includes a review at least once a year and updates when the environment changes.*	*Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.*	*For this requirement, a QSA will typically:* • *Review documentation to ensure that the document history shows that version updates have occurred in the past 12 months.* • *Examine documentation to ensure that it includes changes that have occurred in the previous 12 months.*
12.2 **12.2.a**	*Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).*	*Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.3	*Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:*	*Obtain and examine the policy for critical employee-facing technologies and perform the following:*	
12.3.1	*Explicit management approval*	*Verify that the usage policies require explicit management approval to use the technologies.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
12.3.2	*Authentication for use of the technology.*	*Verify that the usage policies require that all technology use be authenticated with user ID and password or other authentication item (for example, token).*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.3.3	*A list of all such devices and personnel with access.*	*Verify that the usage policies require a list of all devices and personnel authorized to use the devices.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.3.4	*Labeling of devices with owner, contact information, and purpose.*	*Verify that the usage policies require labeling of devices with owner, contact information, and purpose.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.3.5	*Acceptable uses of the technology.*	*Verify that the usage policies require acceptable uses for the technology.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.3.6	*Acceptable network locations for the technologies.*	*Verify that the usage policies require acceptable network locations for the technology.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.3.7	*List of company-approved products.*	*Verify that the usage policies require a list of company-approved products.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.3.8	*Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.*	*Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.*	*Automatic disconnect should be configured for the HP NonStop server as described under requirement 8.5.15. The mechanism used should be fully documented.*
12.3.9	*Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use.*	*Verify that the usage policies require activation of remote-access technologies used by vendors only when needed by vendors, with immediate deactivation after use.*	*This requirement is generally not applicable specifically to the HP NonStop server.*
12.3.10	*When accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media.*	*Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives, and removable electronic media when accessing such data via remote-access technologies.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.4	*Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.*	*Verify that information security policies clearly define information security responsibilities for both employees and contractors.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
12.5	*Assign to an individual or team the following information security management responsibilities:*	*Verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. Obtain and examine information security policies and procedures to verify that the following information security responsibilities are specifically and formally assigned:*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.5.1	*Establish, document, and distribute security policies and procedures.*	*Verify that responsibility for creating and distributing security policies and procedures is formally assigned.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.5.2	*Monitor and analyze security alerts and information, and distribute to appropriate personnel.*	*Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned.*	*The mechanism used and the processes for analyzing alerts/reports must be fully documented. The documentation must include:* • *The delivery mechanism of alerts/events* • *Personnel responsible for analyzing alerts/reports* *XYGATE Merged Audit (XMA) provides the ability to send alerts based on security events from Safeguard, XYGATE, EMS and BASE24. Reports on events from these subsystems can also be obtained via XMA.*
12.5.3	*Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.*	*Verify that responsibility for creating and distributing security incident response and escalation procedures is formally assigned.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.5.4	*Administer user accounts, including additions, deletions, and modifications.*	*Verify that responsibility for administering user account and authentication management is formally assigned.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.5.5	*Monitor and control all access to data.*	*Verify that responsibility for monitoring and controlling all access to data is formally assigned.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.6 **12.6.a**	*Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.*	*Verify the existence of a formal security awareness program for all employees.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.6.b	*Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.*	*Obtain and examine security awareness program procedures and documentation and perform the following:*	

Req. No	PCI DSS Requirement	Testing Procedure	Remark
12.6.1 **12.6.1.a**	*Educate employees upon hire and at least annually.*	*Verify that the security awareness program provides multiple methods of communicating awareness and educating employees (for example, posters, letters, memos, web based training, meetings, and promotions).*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.6.1.b	*Educate employees upon hire and at least annually.*	*Verify that employees attend awareness training upon hire and at least annually.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.6.2	*Require employees to acknowledge at least annually that they have read and understood the company's security policy and procedures.*	*Verify that the security awareness program requires employees to acknowledge (for example, in writing or electronically) at least annually that they have read and understand the company's information security policy.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.7	*Screen potential employees (see definition of "employee" at 9.2 above) prior to hire to minimize the risk of attacks from internal sources. For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*	*Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) on employees prior to hire who will have access to cardholder data or the cardholder data environment. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.8	*If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:*	*If the entity being assessed shares cardholder data with service providers (for example, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), through observation, review of policies and procedures, and review of supporting documentation, perform the following:*	
12.8.1	*Maintain a list of service providers.*	*Verify that a list of service providers is maintained.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.8.2	*Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.*	*Verify that the written agreement includes an acknowledgement by the service providers of their responsibility for securing cardholder data.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
12.8.3	*Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.*	*Verify that policies and procedures are documented and were followed including proper due diligence prior to engaging any service provider.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.8.4	*Maintain a program to monitor service providers' PCI DSS compliance status.*	*Verify that the entity assessed maintains a program to monitor its service providers' PCI DSS compliance status.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.9	*Implement an incident response plan. Be prepared to respond immediately to a system breach.*	*Obtain and examine the Incident Response Plan and related procedures and perform the following:*	
12.9.1	*Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:* • *Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum* • *Specific incident response procedures* • *Business recovery and continuity procedures* • *Data back-up processes* • *Analysis of legal requirements for reporting compromises* • *Coverage and responses of all critical system components* • *Reference or inclusion of incident response procedures from the payment brands.*	*Verify that the Incident Response Plan includes:* • *Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum* • *Specific incident response procedures* • *Business recovery and continuity procedures* • *Data back-up processes* • *Analysis of legal requirements for reporting compromises (for example, California Bill 1386 which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database)* • *Coverage and responses for all critical system components* • *Reference or inclusion of incident response procedures from the payment brands.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.9.2	*Test the plan at least annually.*	*Verify that the plan is tested at least annually.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.9.3	*Designate specific personnel to be available on a 24/7 basis to respond to alerts.*	*Verify through observation and review of policies, that there is 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*

Req. No	***PCI DSS Requirement***	***Testing Procedure***	***Remark***
12.9.4	*Provide appropriate training to staff with security breach response responsibilities.*	*Verify through observation and review of policies that staff with security breach responsibilities are periodically trained.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.9.5	*Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.*	*Verify through observation and review of processes that monitoring and responding to alerts from security systems including detection of unauthorized wireless access points are covered in the Incident Response Plan.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*
12.9.6	*Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.*	*Verify through observation and review of policies that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.*	*This requirement is not applicable specifically to the HP NonStop server and should be implemented by the relevant personnel within the organization.*

REQUIREMENT A.1: SHARED HOSTING PROVIDERS MUST PROTECT THE CARDHOLDER DATA ENVIRONMENT

REQUIREMENT INTRODUCTION

The introduction for requirement A.1 of PCI DSS states:

> *As referenced in Requirement 12.8, all service providers with access to cardholder data (including shared hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.4 states that shared hosting providers must protect each entity's hosted environment and data. Therefore, shared hosting providers must additionally comply with the requirements in the Appendix.*

REQUIREMENT DESCRIPTION

Requirement A.1 is only relevant if the HP NonStop server is being used in a host-sharing environment for multiple clients, as per Requirement 2.4. That means that applications (that process, transmit or store cardholder data) for different customers are running on the same system. The requirements in this section are aimed at ensuring that each application environment is kept entirely separate.

SEGREGATION OF ENVIRONMENTS

The application environments for different customers must be kept entirely segregated. This means that each environment should be running under its own distinct userid and should be configured with its own customer application specific subvolumes/directories and non-privileged userids/aliases. The following should be ensured at a minimum:

- No sharing of userids between the environments.
- Unique subvolumes for each environment with appropriate Safeguard protection in place to enforce access control and auditing.
- Unique directories for each OSS environment with strong access security applied.

RESOURCE ALLOCATION

One of the aims of this requirement is to ensure that no application environment negatively impacts on any other environment by using up all available resources. Certain protection is inherently provided by the operating system due to its architecture. For example, non-shared memory space for processes, mechanism for reducing priority of looping processes and so on.

XYGATE CMON (XCM) can assist with allocation of resources by allocating specific CPUs for certain activities, restricting priority assignments and so on. It also has an automated load balancing feature to help ensure that system resources are used in a balanced manner.

THE REQUIREMENT

Req. No	PCI DSS Requirement	Testing Procedure	Remark
A.1	*Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS.* *Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance As applicable*	*Specifically for a PCI DSS assessment of a shared hosting provider, to verify that shared hosting providers protect entities' (merchants and services providers) hosted environment and data, select a sample of severs (Microsoft Windows and Unix/Linux) across a representative sample of hosted merchants and service providers, and perform A1.1 through A1.4 below*	
A.1.1	*Ensure that each entity only runs processes that have access to that entity's cardholder data environment.*	• *If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example: No entity on the system can use a shared web server user ID.* • *All CGI scripts used by an entity must be created and run as the entity's unique user ID.*	*The application environments for different customers must be kept entirely segregated. This means that each should be running under its own distinct userid.* *For this requirement, a QSA will typically:* • *Review that the documentation describes the userids under which each hosted application runs.* • *Interview security personnel so as to understand how the application userid segregation works. This must be consistent with the documentation.* • *Examine evidence of userid access to the different environments to ensure that proper segregation is in place.* *See Segregation of Environments for further information.*
A1.2 **A.1.2.a**	*Restrict each entity's access and privileges to own cardholder data environment only.*	*Verify the user ID of any application process is not a privileged user (root/admin).*	*For this requirement, a QSA will typically:* • *Interview security personnel so as to understand how they have ensured that none of the customer userids have access to any area of the system other than their own hosted environment.* • *Examine evidence of userid/alias access to the different environments to ensure that proper segregation is in place. This may include an analysis of Safeguard access records, OSS directory/file security and relevant userids/aliases.* *See Segregation of Environments for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
A.1.2.b	*Restrict each entity's access and privileges to own cardholder data environment only.*	*Verify each entity (merchant, service provider) has read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.). IMPORTANT: An entity's files may not be shared by group.*	*For this requirement, a QSA will typically:* • *Interview security personnel so as to understand how they have ensured that customer userids have access to only their files, subvolumes and OSS directories.* • *Examine evidence of userid/alias access to the different environments to ensure that proper access restriction is in place. This may include an analysis of Safeguard access records, OSS directory/file security and relevant userids/aliases.* *See Segregation of Environments for further information.*
A.1.2.c	*Restrict each entity's access and privileges to own cardholder data environment only.*	*Verify an entity's users do not have write access to shared system binaries.*	*For this requirement, a QSA will typically:* • *Interview security personnel so as to understand how they have ensured that customer userids do not have write access to system objects, for example $SYSTEM.SYSTEM, $SYSTEM.SYSnn and so on.* • *Examine evidence of userid/alias access to the system subvolumes/directories to ensure that proper access restriction is in place. This may include an analysis of Safeguard access records, OSS directory/file security and relevant userids/aliases.* *See Segregation of Environments for further information.*
A.1.2.d	*Restrict each entity's access and privileges to own cardholder data environment only.*	*Verify that viewing of log entries is restricted to the owning entity.*	*For this requirement, a QSA will typically::* • *Interview security personnel so as to understand how they have ensured that customer userids can only read log entries associated with their specific customer application(s).* • *Examine evidence of userid/alias access to the log subvolumes/directories to ensure that proper access restriction is in place. This may include an analysis of Safeguard access records, OSS directory/file security and relevant userids/aliases.* *See Segregation of Environments for further information.*

Req. No	PCI DSS Requirement	Testing Procedure	Remark
A.1.2.e	*Restrict each entity's access and privileges to own cardholder data environment only.*	*To ensure each entity cannot monopolize server resources to exploit vulnerabilities (for example, error, race, and restart conditions, resulting in, for example, buffer overflows), verify restrictions are in place for the use of these system resources:* • *Disk space* • *Bandwidth* • *Memory* • *CPU*	*For this requirement, a QSA will typically:* • *Interview security personnel so as to understand how they have allocated resources to entities.* *See Resource Allocation for further information.*
A1.3 **A.1.3.a**	*Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.*	*Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment:* • *Logs are enabled for common third-party applications.* • *Logs are active by default.* • *Logs are available for review by the owning entity.* • *Log locations are clearly communicated to the owning entity.*	*For this requirement, a QSA will typically:* • *Interview security personnel so as to understand how they have ensured that each customer's audit data can only be read by the customer to whom it belongs.* • *Examine evidence of userid/alias access to the log subvolumes/directories to ensure that proper access restriction is in place. This may include an analysis of Safeguard access records, OSS directory/file security and relevant userids/aliases.*
A.1.4	*Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.*	*Verify the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise.*	*This typically applies to policies and procedures at the corporate level.*

GLOSSARY

Term	Description
ASV	Approved Scanning Vendor – approved by PCI SSC. List on website.
Cardholder	Customer to whom a card is issued or individual authorized to use the card
Cardholder Data	Full magnetic stripe or the PAN plus any of the following: * Cardholder name * Expiration date * Service Code
Cardholder Data Environment	Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment
Card Validation Value or Code	(1) Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. (2)The second type of card validation value or code is the three-digit value printed to the right of the credit card number in the signature panel area on the back of the card. For American Express cards, the code is a four-digit unembossed number printed above the card number on the face of all payment cards. The code is uniquely associated with each individual piece of plastic and ties the card account number to the plastic.
CAV	Card Authentication Value (JCB payment cards)
CVC	CVC Card Validation Code (MasterCard payment cards)
CVV	Card Verification Value (Visa and Discover payment cards)
CSC	Card Security Code (American Express)
CID	Card Identification Number (American Express and Discover payment cards)
CAV2	Card Authentication Value 2 (JCB payment cards)
CVC2	Card Validation Code 2 (MasterCard payment cards)
CVV2	Card Verification Value 2 (Visa payment cards)
Enscribe	The proprietary file system running on all HP NonStop servers. Enscribe files are managed by the FUP utility.
Event Management Service (EMS)	The event subsystem for the HP NonStop server where system and subsystem events can be collected and viewed.
Guardian	The proprietary operating system on which HP NonStop servers run. Guardian offers basic file level security with no auditing capabilities.
Netbatch	The batch scheduler typically running on HP NonStop servers. The Netbatch environment is managed by the BATCHCOM utility.
NonStop SQL	SQL subsystems for the HP NonStop. Could be either SQL/MP or SQL/MX.
OSS	The POSIX flavor of the operating system that runs on the HP NonStop server. The OSS subsystem needs to be specifically started for OSS to be running on a system.
PAN	Acronym for “primary account number” and also referred to as “account number.” Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
PCI SSC	Payment Card Industry Security Standard Council
PCI DSS	Payment Card Industry Data Security Standard
Pathway	The requestor/server based application environment for the NonStop.
Pathcom	The interactive utility for managing Pathway environments.

Term	Description
QSA	Qualified Security Assessor approved by PCI SSC. Listed on the PCI SSC website.
SAFEART	Safeguard Audit Reduction Tool used for viewing Safeguard audit records.
Safecom	Interactive utility for controlling and managing the Safeguard subsystem.
Safeguard	Security subsystem that provides increased and more flexible access control than Guardian security. Has the ability to provide auditing of object access attempts and attempts to manage security configuration. Used also for user/alias maintenance. Provided as a standard product with all NS and NB series HP NonStop servers.
SCF	Subsystem Control Facility used for managing hardware and a variety of subsystems on the HP NonStop server.
Sensitive Authentication Data	Security-related information (Card Validation Codes/Values, complete track data, PINs, and PIN Blocks) used to authenticate cardholders, appearing in plaintext or otherwise unprotected form. Disclosure, modification, or destruction of this information could compromise the security of a cryptographic device, information system, or cardholder information or could be used in a fraudulent transaction
SQL/MP	SQL implementation that runs on the HP NonStop server. SQL/MP runs in the Guardian environment and is managed by the SQLCI interactive utility.
SQL/MX	SQL implementation based on the ANSI standard that runs on the HP NonStop server. SQL/MX runs in the OSS environment and is controlled through the mxci utility.
Strong Cryptography	General term to indicate cryptography that is extremely resilient to cryptanalysis. That is, given the cryptographic method (algorithm or protocol), the cryptographic key or protected data is not exposed. The strength relies on the cryptographic key used. Effective size of the key should meet the minimum key size of comparable strengths recommendations. One reference for minimum comparable strength notion is NIST Special Publication 800-57, August, 2005 (http://csrc.nist.gov/publications/) or others that meet the following minimum comparable key bit security: * 80 bits for secret key based systems (for example TDES) * 1024 bits modulus for public key algorithms based on the factorization (for example, RSA) * 1024 bits for the discrete logarithm (for example, Diffie-Hellman) with a minimum 160 bits size of a large subgroup (for example, DSA) * 160 bits for elliptic curve cryptography (for example, ECDSA)
System Components	Any network component, server, or application included in or connected to the cardholder data environment
XYGATE Access Control (XAC)	Allows the functional properties of one NSK userid to be allocated and controlled for another userid while the user's inputs and outputs are being audited by XAC. Includes the ability to fully capture user sessions.
XYGATE CMON (XCM)	Full featured CMON process that acts as a control center for Command Interpreter and TACL process startups, logins and alter priorities. Via these three interfaces CMON balances the loads of the CPUs.
XYGATE Encryption Library (XEL)	An encryption library that can be used to encryption-enable applications, databases and communications using strong FIPS 140-2 validated encryption.
XYGATE Host Encryption (XHE)	Provides SSL encryption to any Telnet, FTP, RSC, ODBC server application or any TCP/IP communication session. XHE manages SSL encryption for TCP/IP communication between the HP NonStop and the PC desktop.
XYGATE Key Manager (XKM)	Software based encryption key management subsystem.
XYGATE Merged Audit (XMA)	Provides a facility to combine Safeguard, XYGATE, BASE24 and selected EMS Audit trails into a single SQL Database. Also provides real-time alerting functionality and the ability to send selected or all events to an “off box” audit logging appliance or server.
XYGATE Object Security (XOS)	Enables pattern-oriented security, using rules to reduce ACL counts and streamline security maintenance. Allows for access authorization based on criteria other than object name and has the ability to secure SQL/MP tables/views.
XYGATE Password Quality (XPQ)	Can run with or without Safeguard and allows the corporate policy to be

Term	Description
	enforced regarding password attributes in order to “strengthen” user passwords, making them more resistant against attack.
XYGATE Secure Client (XSC)	Works in conjunction with XHE or any other SSL enabled host program to enable secure encrypted sessions over TCP/IP between any windows PC and HP NonStop server.
XYGATE Secure Shell (XSH)	XYGATE SSH implementation for the HP NonStop server.
XYGATE Safeguard Manager (XSM)	Windows interface to streamline management of Safeguard globals, users/aliases and Object ACLs. Also operates in the OSS environment supporting OSS file/directory level security vectors and ACLs.
XYGATE Safeguard Reporting (XSR)	Simplifies and streamlines Safeguard audit trail information with flexible selection criteria and formatting. Host or GUI based reports.
XYGATE Security Compliance Wizard (XSW)	Provides a Windows-based method to establish, monitor and report on compliance with your information security policy and Best Practices for your HP NonStop server enterprise. Provides a built in File Integrity Monitor, customizable PCI DSS compliance reports and access matrix.
XYGATE User Authentication (XUA)	Delivers granular failed logon management, logon-specific audit reporting, logon control by IP address or requestor program and multi-factor authentication to associate all system logons to a specific person

For PCI DSS definitions of PCI DSS related terms, see the PCI DSS Glossary (https://www.pcisecuritystandards.org/pdfs/pci_dss_glossary.pdf)

RESOURCES

Resource	Location
PCI SSC Website	https://www.pcisecuritystandards.org/index.shtml
PCI DSS Specification (latest version)	https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
PCI DSS Supporting Documents	https://www.pcisecuritystandards.org/security_standards/pci_dss_supporting_docs.shtml
Navigating the PCI DSS Document	https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf
PCI DSS Glossary	https://www.pcisecuritystandards.org/security_standards/glossary.shtml
PCI DSS Requirement 6.6 Supplement (Application Reviews and Web Application Firewalls Clarified)	https://www.pcisecuritystandards.org/security_standards/docs/information_supplement_6.6.pdf
PCI Data Storage Do's and Don'ts	https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf
HP NonStop server Security- A Practical Handbook, By XYPRO Technology Corporation (ISBN: 1-55558-314-8)	http://www.elsevier.com/wps/find/bookdescription.cws_home/701262/description#description
Securing HP NonStop servers in an Open Systems World, By XYPRO Technology Corporation (ISBN: 1-55558-344-X)	http://www.elsevier.com/wps/find/bookdescription.cws_home/708269/description#description
HP NonStop Technical Library	http://h20000.www2.hp.com/bizsupport/TechSupport/Product.jsp?lang=en&cc=us&taskId=101&contentType=SupportManual&docIndexId=64255&prodTypeId=15351&prodCatId=407843
Security Management Guide	See HP NonStop technical Library
Safeguard Administrator's Manual	See HP NonStop technical Library
Safeguard Reference Manual	See HP NonStop technical Library
Safeguard User's Guide	See HP NonStop technical Library
Safeguard Audit Service Manual	See HP NonStop technical Library
HP NonStop Security – NSC Security Program	http://www.hp.com/go/nonstop/security/NSCSecurity
HP NonStop eServices Portal	https://onepoint.nonstop.compaq.com
ISO 8583 Financial transaction card originated messages — Interchange message specifications	http://en.wikipedia.org/wiki/ISO_8583
OWASP Top 10	http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
OWASP Cryptographic Storage Cheat Sheet	http://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet
Witham Laboratories Website	http://www.withamlabs.com/
Knightcraft Technology Website	http://www.knightcraft.com/
XYPRO Technology Website	https://www.xypro.com/

ACKNOWLEDGEMENTS

The authors would like to thank the following individuals and organizations for their contributions in reviewing the document, for providing technical assistance or for general assistance in making this document possible.

- Ik Heo (Knightcraft Technology)
- Mario Sist, Andrew Jamieson and Gina Miljevic (Witham Laboratories)
- Simon Siebert
- Morné Conradie (NSK System Services)
- Scott Uroff, Barry Forbes, Manuel Sunderland, Dan Lewis and Lisa Partridge (XYPRO Technology Corporation)