Payment Card Industry (PCI)

Card Production and Provisioning Report on Compliance

Enter company name
Enter city name, Enter country name

Enter Assessor company name

For use with Physical Security Requirements v3.0.1

ROC Version 3.0.1

November 2023

Document Changes

Date	Version	Description
July 2015	1.0	Initial version
December 2015	1.0a	Minor errata
June 2016	1.0b	Expanded sections 2.2, 3.2 and 3.3
April 2017	2.0	Updated for changes incorporated into v2 of the Security Requirements, including Mobile Provisioning.
December 2017	2.1	Updated with addition of Test Procedures
June 2022	3.0	Updated for release of new Requirements
November 2023	3.0.1	Minor errata

Contents

Introduction to the ROC Template

This document, the *PCI Card Production and Provisioning Report on Compliance for use with PCI Card Production and Provisioning Physical Security Requirements v3.0.1* ("ROC Reporting Template"), is the template for Payment Brand Assessors completing a Report on Compliance (ROC) for assessments against the *PCI Card Production and Provisioning Physical Security Requirements v3.0.1.*

The ROC Reporting Template serves two purposes:

- It serves as a declaration of the results of the card vendor's assessment of compliance with the *PCI Card Production and Provisioning Physical Security Requirements v3.0.1.*
- It provides reporting instructions and the template for assessors to use. This can help provide reasonable assurance that a consistent level of reporting is present among assessors.

Contact the requesting payment brand for reporting and submission procedures.

Use of this reporting template is subject to payment brand stipulations for all Card Production and Provisioning v3.0.1 submissions.

Tables have been included in this template to facilitate the reporting process for certain lists and other information as appropriate. Additional appendices may be added if the assessor feels there is relevant information to be included that is not addressed in the current format. However, the assessor must not remove any details from the tables provided in this document.

Do not delete any content from any place in this document, including this section and the versioning above. These instructions are important for the assessor as the report is written and for the recipient in understanding the context from which the responses and conclusions are made. Addition of text or sections is applicable within reason, as noted above.

The Report on Compliance (ROC) is originated by the card vendor and further refined by the payment brand-designated assessor during the onsite card production and provisioning vendor assessment as part of the card vendor's validation process. The ROC provides details about the vendor's environment and assessment methodology, and documents the vendor's compliance status for each Card Production and Provisioning Security Requirement. A PCI Card Production and Provisioning Security compliance assessment involves thorough testing and assessment activities, from which the assessor will generate detailed work papers. These work papers contain comprehensive records of the assessment activities including observations, results of system testing, configuration data, file lists, interview notes, documentation excerpts, references, screenshots, and other evidence collected during the course of the assessment. The ROC is effectively a **summary of evidence** derived from the assessor's work papers to describe how the assessor performed the validation activities and how the resultant findings were reached. At a high level, the ROC provides a comprehensive **summary of testing activities performed and information collected** during the assessment against the *PCI Card Production and Provisioning Physical Security Requirements v3.0.1*. The information contained in a ROC must provide enough detail and coverage to verify that the assessed entity is compliant with all PCI Card Production and Provisioning Security Requirements.

ROC Sections

The ROC includes the following sections and appendices:

1. Section 1: Contact Information and Report Date
2. Section 2: Summary of Non-Compliance Findings
3. Section 3: Inspection Overview
4. Section 4: Findings and Observations

Note: *Sections 1 through 4 must be thoroughly and accurately completed, in order for the assessment findings in Section 5 to have the proper context. The reporting template includes tables with reporting instructions built-in to help assessors provide all required information throughout the document. Responses should be specific but efficient. Information provided should focus on concise quality of detail, rather than lengthy, repeated verbiage. Parroting the testing procedure within a description is discouraged, as it does not add any level of assurance to the narrative. Use of template language for summaries and descriptions is discouraged and details should be specifically relevant to the assessed entity.*

ROC Vendor Self-Evaluation

The card vendor is asked to complete the card vendor self-evaluation in Section 5: Findings and Observations, for all requirements.

- Only one response should be selected at the sub-requirement level, and reporting of that should be consistent with other required documents.
- Select the appropriate response for “Compliant to PCI CP Requirement” for each requirement.
- In the “Comments/Remediation Date and Actions” section, the vendor may enter an explanation regarding its compliance that provides the payment brand assessor with additional information to be considered for the compliance assessment. In the event “No” is entered in the Compliance column, the vendor must state the planned remediation action and the date for the remediation. In the event "Not Applicable" is entered in the Compliance column, the vendor must explain why they believe the requirement does not apply for their situation.

ROC Summary of Assessor Findings

At each sub-requirement, under "Assessor Compliance Evaluation," there is a column in which to designate the result. There are five options to summarize the assessor's conclusion: Yes, New, Open, Closed, and Not Applicable.

The following table is a helpful representation when considering which selection to make and when to add comments. Remember, only one "Result" response may be selected at the sub-requirement level, and reporting of that should be consistent with other required documents.

Response	When to use this response:
Yes	Indicates the vendor is in compliance with this requirement
New	Indicates that this is a new non-compliance finding identified by the assessor for the first time.
Open	Indicates that this item was previously reported as a non-compliance finding and action (if any) taken by the vendor does not resolve the original condition. The "Non-Compliance Description" column must explicitly state when this finding was first reported, the non-compliance condition observed, and the action (or lack thereof) taken by the vendor to resolve the finding. Findings for which the vendor has taken corrective action that resolved the original finding but introduced new non-compliance condition are reported as new findings for the applicable requirement.
Closed	Indicates that this item was previously reported as a non-compliance finding and vendor corrective action has resolved the finding. The "Non-Compliance Description" column must describe the action the vendor has taken to resolve the finding.
Not Applicable	Indicates that the assessor's assessment confirms that the requirement does not apply to for the vendor. Not Applicable responses are only expected it the requirement applies to an activity that the vendor does not perform.
Comment/ Non-Compliance Assessment	Use this column to indicate: ▪ Clarification describing the conditions observed in support of the assessor's conclusion of compliance, or ▪ If non-compliance, a description of the reason for non-compliance. Note that specific payment brands may require additional supporting details where compliance is noted.

ROC Reporting Details

The reporting instructions in the Reporting Template explain the intent of the response required. There is no need to repeat the requirement or the reporting instruction within each assessor response. As noted earlier, responses should be specific and relevant to the assessed entity. Details provided should focus on concise quality of detail, rather than lengthy, repeated verbiage and should avoid parroting of the requirement without additional detail or generic template language.

Do's and Don'ts: Reporting Expectations

DO:	*DON'T:*
▪ Use this Reporting Template when assessing against v3.0.1 of the Card Production and Provisioning Security Requirements. ▪ Complete all sections in the order specified. ▪ Read and understand the intent of each requirement and testing procedure. ▪ Provide a response for every security requirement. ▪ Provide sufficient detail and information to support the designated finding, but be concise. ▪ Describe *how* a Requirement was verified per the Reporting Instruction, not just that it *was* verified. ▪ Ensure all parts of the Reporting Instructions are addressed. ▪ Ensure the response covers all applicable system components. ▪ Perform an internal quality assurance review of the ROC for clarity, accuracy, and quality. ▪ Provide useful, meaningful diagrams, as directed.	▪ Don't simply repeat or echo the security requirement in the response. ▪ Don't copy responses from one requirement to another. ▪ Don't copy responses from previous assessments. ▪ Don't include information irrelevant to the assessment.

ROC Template for PCI Card Production and Provisioning Security Requirements v3.0

This template is to be used for creating a Report on Compliance. Content and format for a ROC is defined as follows:

1 Contact Information and Report Date

1.1 Contact Information

Client		
▪ Company name:		Payment Brand Identification Code:
▪ Company address:		
▪ Company URL:		
▪ Company contact:	Name:	
	Phone number:	E-mail address:
Assessor Company		
▪ Company name:		
▪ Company address:		
▪ Company URL:		
Assessor		
▪ Primary Assessor:	Name:	
	Phone number:	E-mail address:
▪ Secondary Assessor:	Name:	
	Phone number:	E-mail address:
▪ Secondary Assessor:	Name:	
	Phone number:	E-mail address:
Assessor Quality Assurance (QA) Primary Reviewer for this specific report *(not the QA Contact for the CPSA)*		
▪ QA Reviewer:	Name:	
	Phone number:	E-mail address:

1.2 Location, Date, and Timeframe of Assessment

▪ Address of facility where assessment was performed:		
▪ Date of Report (yyyy/mm/dd):		
▪ Timeframe of assessment (start date to completion date):	Start date (yyyy/mm/dd):	Completion date (yyyy/mm/dd):
▪ Was the review done onsite or remotely:	Select	
▪ If remotely, state the rationale:		
▪ If applicable, identify date(s) spent onsite at the entity:	Start date (yyyy/mm/dd):	Completion date (yyyy/mm/dd):

1.3 Card Production Activities

Identify the functions for which a security assessment was performed and whether the function was added/discontinued since previous inspection.

▪ Card Manufacturing	Select	▪ Chip Embedding	Select
▪ Data Preparation	Select	▪ Card Personalization	Select
▪ Pre-Personalization	Select	▪ Chip Personalization	Select
▪ Fulfillment	Select	▪ Mailing	Select
▪ Packaging	Select	▪ Shipping	Select
▪ Storage	Select		
▪ PIN Printing and Mailing (personalized, credit or debit)	Select		
▪ PIN Printing (non-personalized prepaid cards)	Select		
▪ Electronic PIN Distribution	Select		
▪ Other (describe)			

1.4 Mobile Provisioning Activities

▪ Secure Element Provisioning Services	Select	▪ Cloud-based (HCE) Provisioning Services	Select

Secure Element Provisioning Services		
1. Select	Product/Solution	
	Description	
2. Select	Product/Solution	
	Description	
3. Select	Product/Solution	
	Description	
4. Select	Product/Solution	
	Description	
5. Select	Product/Solution	
	Description	

Cloud-based (HCE) Provisioning Services		
1. Select	Product/Solution	
	Description	
2. Select	Product/Solution	
	Description	
3. Select	Product/Solution	
	Description	
4. Select	Product/Solution	
	Description	
5. Select	Product/Solution	
	Description	

1.5 Security Operations Center and Security Control Room Reporting

Use this section to indicate:

- A Security Operations Center subject to *PCI Card Production and Provisioning Physical Security Requirements,* Appendix C, "Security Operations Center" requirements, is located on the premises of this facility.
- This facility has been monitored for any part of the audit cycle♦ by a SOC subject to *PCI Card Production and Provisioning Physical Security Requirements,* Appendix C, "Security Operations Center."
- This facility operates a Security Control Room (SCR) and was also monitored by a remote SOC (Subject to Appendix C) for part of the audit cycle.♦
- This facility operates a Security Control Room (SCR) and was not monitored by a remote SOC (Subject to Appendix C) for any part of the audit cycle.♦

<table>
<tr><td colspan="3">▪ Security Operations Center
This facility operates a SOC (Subject to Appendix C)</td><td colspan="6">Select</td></tr>
<tr><td colspan="3" rowspan="2">▪ Remote SOC
This facility is monitored by a SOC (Subject to Appendix C)</td><td>Select</td><td colspan="5">If yes, indicate the Country, City and Payment Brand Identification Code in the fields below of the remote SOC. If monitored by more than one remote SOC, enter the details for the primary remote SOC.
If the facility was monitored remotely for a period less than the full audit cycle, indicate the start and end dates that the facility was monitored by the remote SOC. If multiple start and end dates apply, enter the first start date and the last end date.</td></tr>
<tr><td>Remote SOC Location:</td><td>Country:</td><td></td><td>City:</td><td></td><td>Payment Brand Identification Code:</td><td colspan="2"></td></tr>
<tr><td colspan="2">Full Audit Cycle?</td><td>Select</td><td colspan="2">If not, enter the period that the facility was monitored by a remote SOC.</td><td>Start date (yyyy/mm/dd):</td><td></td><td>End date (yyyy/mm/dd):</td><td></td></tr>
<tr><td colspan="3">▪ Security Control Room
This facility operates an SCR and has not been monitored by a remote SOC (Subject to Appendix C) for any part of the current audit cycle.</td><td colspan="6">Select</td></tr>
</table>

♦ The audit cycle is the period of time from the completion date of the last full facility audit report, as indicated in Section 1.2, to the current audit completion date. An audit cycle is typically 12 months in duration.

2. Summary of Non-Compliance Findings

Please use the table on the following page to report, covering all sections under each heading. Write up findings and list non-compliances—including the section reference number the non-compliance relates to—within the findings text as each non-compliance occurs. List all non-compliances in order, including the relevant section reference number the non-compliance—for example:

2.1 Non-Compliance Findings – Example

Requirement	New	Previous		Non-Compliance Findings Description
		Open	Closed	
1.1.2.b	☒	☐	☐	*Pre-employment documentation and background checks are not carried out on part-time employees.*
3.7.1.r	☐	☒	☐	*Card components are not returned to the vault during non-production hours.*
5.1, 5.2	☐	☐	☒	*The vendor could not produce written authorization for packaging, shipping, or mailing the card and PIN together from its customer (issuer name).*

Notes for Consideration

- *Please ensure non-compliances are written exactly as the examples above and be as specific as possible down to the exact bullet that covers the non-compliance.*
- *Also list items that are **not** non-compliances but are items that either the assessor is unsure of, or the vendor has discussed with the assessor and questions arising from this discussion can only be answered by the applicable payment brands(s). This section is optional, so if not required, please delete it from the report.*

2.2 Non-Compliance Findings – Detail

Requirement	New	Previous		Non-Compliance Findings Description
		Open	Closed	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	

Requirement	New	Previous		Non-Compliance Findings Description
		Open	Closed	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	

Requirement	New	Previous		Non-Compliance Findings Description
		Open	Closed	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	

Requirement	New	Previous		Non-Compliance Findings Description
		Open	Closed	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	

3. Inspection Overview

3.1 Facility Description

The auditor must provide a general description of the vendor facility and Card Production and Provisioning environment. For example, “The facility consists of multiple buildings, and card production activities are performed in one building consisting of a High Security Area for Card Production and Provisioning. Administration functions are performed external to the HSA. The vendor being audited is the only occupant of this building.”

The introduction must also include any unusual conditions that may impact the audit scope or compliance assessment process. For example, “First audit after relocation, significant expansion / reconfiguration of the HAS, significant changes to key personnel, introduction of new technologies,” and any other unusual conditions.

▪ Vendor Facility and Card Production and Provisioning Environment	
▪ Conditions that may Impact Audit Scope	

3.2 Documentation Reviewed

Identify and list all reviewed documents. Include the following:

Reference Number	Document Name (including version, if applicable)	Brief description of document purpose	Document date (latest version)
Doc-1			
Doc-2			
Doc-3			
Doc-4			
Doc-5			
Doc-6			
Doc-7			
Doc-8			
Doc-9			
Doc-10			
Doc-11			
Doc-12			
Doc-13			
Doc-14			
Doc-15			
Doc-16			
Doc-17			
Doc-18			
Doc-19			
Doc-20			
Doc-21			
Doc-22			
Doc-23			
Doc-24			

Reference Number	Document Name (including version, if applicable)	Brief description of document purpose	Document date (latest version)
Doc-25			
Doc-26			
Doc-27			
Doc-28			
Doc-29			
Doc-30			
Doc-31			
Doc-32			
Doc-33			
Doc-34			
Doc-35			
Doc-36			
Doc-37			
Doc-38			
Doc-39			
Doc-40			
Doc-41			
Doc-42			
Doc-43			
Doc-44			
Doc-45			
Doc-46			
Doc-47			
Doc-48			
Doc-49			
Doc-50			

Reference Number	Document Name (including version, if applicable)	Brief description of document purpose	Document date (latest version)
Doc-51			
Doc-52			
Doc-53			
Doc-54			
Doc-55			
Doc-56			
Doc-57			
Doc-58			
Doc-59			
Doc-60			
Doc-61			
Doc-62			
Doc-63			
Doc-64			
Doc-65			
Doc-66			
Doc-67			
Doc-68			
Doc-69			
Doc-70			
Doc-71			
Doc-72			
Doc-73			
Doc-74			
Doc-75			
Doc-76			

3.3 Individuals Interviewed

Identify and list the individuals interviewed. Include the following:

Reference Number	Employee Name	Role/Job Title	Organization	Summary of Topics Covered / Areas or Systems of Expertise (high-level summary only)
Int-1				
Int-2				
Int-3				
Int-4				
Int-5				
Int-6				
Int-7				
Int-8				
Int-9				
Int-10				
Int-11				
Int-12				
Int-13				
Int-14				
Int-15				
Int-16				
Int-17				
Int-18				
Int-19				
Int-20				
Int-21				
Int-22				
Int-23				
Int-24				

Reference Number	Employee Name	Role/Job Title	Organization	Summary of Topics Covered / Areas or Systems of Expertise (high-level summary only)
Int-25				
Int-26				
Int-27				
Int-28				
Int-29				
Int-30				
Int-31				
Int-32				
Int-33				
Int-34				
Int-35				
Int-36				
Int-37				
Int-38				
Int-39				
Int-40				
Int-41				
Int-42				
Int-43				
Int-44				
Int-45				
Int-46				
Int-47				
Int-48				
Int-49				
Int-50				

Reference Number	Employee Name	Role/Job Title	Organization	Summary of Topics Covered / Areas or Systems of Expertise (high-level summary only)
Int-51				
Int-52				
Int-53				
Int-54				
Int-55				
Int-56				
Int-57				
Int-58				
Int-59				
Int-60				
Int-61				
Int-62				
Int-63				
Int-64				
Int-65				
Int-66				
Int-67				
Int-68				
Int-69				
Int-70				
Int-71				
Int-72				
Int-73				
Int-74				
Int-75				
Int-76				

4. Validating the Requirements

The validation methods identified for each requirement describe the expected activities to be performed by the assessor to validate whether the entity has met the requirement. The intent behind each validation method is described as follows:

- **Examine:** The assessor critically evaluates data evidence. Common examples include documents (electronic or physical), screenshots, configuration files, audit logs, and data files.
- **Observe:** The assessor watches an action or views something in the environment. Examples of observation subjects include personnel performing a task or process, system components performing a function or responding to input, system configurations/settings, environmental conditions, and physical controls.
- **Interview:** The assessor converses with individual personnel. Interview objectives may include confirmation of whether an activity is performed, descriptions of how an activity is performed, and whether personnel have particular knowledge or understanding.

The validation methods are intended to allow the assessed entity to demonstrate how it has met a requirement. They also provide the assessed entity and the assessor with a common understanding of the assessment activities to be performed. The specific items to be examined or observed and personnel to be interviewed should be appropriate for the requirement being assessed, and for each entity's particular implementation.

When documenting the assessment results, the assessor identifies the validation activities performed and the result of each activity. While it is expected that an assessor will perform all the validation methods identified for each requirement, it is also possible for an implementation to be validated using different or additional methods. In such cases, the assessor should document why they used validation methods that differed from those identified in this document.

5. Findings and Observations

Section 1: Roles and Responsibilities

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
1.1 Card Production Staff *The following set of requirements applies to all individuals that have access to card products, components, and the high security area (HSA).*					
1.1.1 Vendor Roles					
The following roles must be filled by employees of the vendor:					
a) Senior management and corporate officers	Select		Interview personnel to verify that roles a) through d) are filled by vendor employees. Examine the relevant appointment information for these positions.	Select	
b) Physical security manager	Select			Select	
c) Acting physical security manager is any qualified individual acting as the physical security manager during any operational period of a facility—i.e., there must be such a designated individual accessible on-site during any operational period of the facility.	Select			Select	
d) Card production supervisor is any card production staff that fulfills a supervisory role of other staff.	Select			Select	
1.1.2 Pre-employment Documentation and Background Checks The vendor must undertake a pre-employment documentation and background check using the same pre-employment procedures, employment application documents, and background checks for:					
a) Full-time employees	Select		Examine the pre-employment documentation for a sample of each	Select	
b) Part-time employees	Select			Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Temporary employees, consultants, and contractors	Select		category to verify it includes application documentation and a background check.	Select	
d) Guards (internal or external)	Select			Select	
1.1.3 Applicant/Employee Background Information Retention					
a) The vendor must retain all personnel's background information on file for at least 18 months after termination of the contract of employment.	Select		Examine policies and procedures to verify that all applicant and personnel background information is retained for at least 18 months after termination of the contract of employment.	Select	
b) This information must be available for the inspector during site security reviews.	Select		Examine a sample of documentation from personnel whose contract of employment has been terminated within the last 18 months.	Select	
1.1.4 Screening and Documentation Usage					
1.1.4.1 Employment Application Forms					
a) The vendor must use employment application forms that include the following detail relating to the applicant's past: • Details of any "alias" or any other names. • List of their previous addresses or residences for the last seven years • Previous employers for the last seven years • Applicants must satisfactorily explain gaps in employment.	Select		Examine a sample of employment applications to verify that they have the minimum information required.	Select	
b) The vendor must maintain a personnel file for each individual listed in Section 1.1.2 that includes but is not limited to the following information:					

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
i. Gathered as part of the hiring process: – Background check results – Verification of aliases (when applicable) – List of previous employers and referral follow-up results – Education history – Social security number or appropriate national identification number – Signed document confirming that the individual has read and understands the vendor's security policies and procedures – Fingerprints and results of search against national and regional criminal records	Select		Examine the personnel files of a sample of individuals to verify that they contain the minimum required documentation during their hiring process.	Select	
ii. Gathered as part of the hiring process and periodically thereafter: – Current photograph, updated at least every three years – Record of any arrests or convictions, updated annually – Annual credit checks	Select		Examine the personnel files of a sample of individuals to verify that they contain the minimum required documentation during their hiring process and during their time of employment as follows: • Current photograph, updated at least every three years • Record of any arrests or convictions, updated annually • Annual credit checks	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) These files must be available to the security inspectors during site reviews.	Select		See above.	Select	
1.1.4.2 Job and Sensitive Task Allocation – Restrictions					
a) The vendor is responsible for determining the level of job responsibilities assigned to any temporary or interim staff (including consultants and contractors), except where the job function is restricted to employees.	Select		Interview appropriate management personnel to verify the process of assigning job responsibility levels to temporary or interim staff (including consultants and contractors), except where the job function is restricted to employees	Select	
1.1.5 Personnel Changes					
1.1.5.1 Changes in Personnel Job Function					
The vendor must ensure that:					
a) The physical security manager is notified in writing of any personnel's expected job change prior to the change taking effect.	Select		Examine policies and procedures to verify that the physical security manager is notified in writing of any personnel's expected job change prior to taking effect. Examine a sample of documentation to verify that the security manager is notified in writing prior to an employee's job change taking effect.	Select	
b) The physical security manager must adapt the access control to restricted areas within one business day.	Select		Interview the physical security manager to verify that the access control to restricted areas of any personnel making a job change is modified within one business day after the job change takes effect. Examine documentation or logs of a sample of such access-control changes were appropriately made.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Where necessary, all combinations and other applicable access codes known to or utilized by employee are changed.	Select		Interview the physical security manager to verify that all necessary combinations and other applicable access codes previously used by the individual making a job change are modified.	Select	
1.1.5.2 Termination of Employment					
a) If termination of employment is a planned event, the physical security manager must be notified in writing prior to termination.	Select		Examine policies and procedures to verify that the physical security manager is notified in writing of any expected termination of personnel prior to it taking effect. Examine a sample of written notifications to the physical security manager of any termination of personnel to verify that such notifications were made prior to the termination's taking effect.	Select	
b) If termination of employment is an unscheduled event—e.g., termination or extended medical leave—the physical security manager must be notified in writing as soon as the decision is made.	Select		Examine policies and procedures to verify that the physical security manager is notified in writing for unscheduled terminations as soon as the decision is made.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Upon termination effective date of any personnel the physical security manager or designated representative must: • Deactivate all access rights. • Recover the photo ID badge. • Change all applicable vault combinations and other applicable access codes known to or utilized by individual. • Recover all company property used in association with card production or provisioning. • Verify completion of the individual's termination checklist activities in Section 1.1.5.3, below.	Select		Interview the physical security manager or designated representative and obtain sample documentation and/or logs to confirm that the following are conducted on any terminated personnel: • Deactivate all access rights. • Recover the photo ID badge. • Change all applicable vault combinations and other applicable access codes known to or utilized by individual. • Recover all company property used in association with card production or provisioning. • Verify completion of the individual's termination checklist activities in Section 1.1.5.3, below.	Select	
1.1.5.3 Termination Checklist					
The vendor must maintain a completed termination checklist on file confirming that staff members carry out the following procedures (where applicable) within one business day from the departure of any personnel:					
a) Disable or remove the individual's computer user IDs and passwords from all applicable systems.	Select		Examine documentation for a sample of terminated individual evidencing that such individual's computer user IDs and passwords have been disabled or removed.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Retrieve all software programs and documentation distributed to the individual.	Select		Examine documentation for a sample of terminated individuals evidencing that all software programs and documentation distributed to such individuals have been retrieved.	Select	
c) Disable the individual's access to computer data and applications.	Select		Examine documentation for a sample of terminated individuals evidencing that all such individuals' access to computer data and applications have been disabled.	Select	
d) Retrieve all company keys, badges, and company photo identification distributed to the individual.	Select		Examine documentation for a sample of terminated individuals evidencing that all company keys, badges, and company photo identification distributed to such individuals have been retrieved.	Select	
e) Change all applicable vault combinations and other applicable access codes known to or utilized by the individual.	Select		Examine documentation for a sample of terminated individuals evidencing that all applicable vault combinations and other access codes known to, accessible to, or utilized by such individuals have been changed.	Select	
1.1.6 Security Communication and Training					
The vendor must emphasize security by:					
a) Designating an individual—e.g., the CISO—responsible for all security matters and concerns, reporting to a senior company executive.	Select		Interview the appropriate personnel designated with responsibility for all security matters and concerns to confirm that they understand their responsibility, including reporting to a senior company executive.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Ensuring that individuals performing or managing tasks requiring access to card components or data or support the cloud-based provisioning processes and/or environment have a signed employment agreement with the vendor. The agreement includes stipulating that the card production staff complies with company polices and rules.	Select		Examine a sample of employment agreements to verify that all individuals performing or managing tasks requiring access to card components or data or support for cloud-based provisioning processes and/or environment: • Have a signed employment agreement; and • The agreement stipulates that the card production staff complies with company policies and rules.	Select	
c) Providing a copy of vendor's internal security manual to all card production staff and security personnel. The security manual must include the following sections: • Administration • HSAs • Security requirements and guidelines • Procedures that card production staff must follow while working in the secure facility • Specific requirements as they pertain to the cloud-based provisioning platforms and systems	Select		Examine policies and procedures to verify that a copy of the internal security manual is provided to all card production staff and security personnel. Examine the security manual to verify that it contains the minimum sections and related content required.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Evidence of positive affirmation by the card production staff of receipt and understanding of responsibilities and obligations under the security policy.	Select		Examine a sample of documentation indicating positive affirmation by card production staff and security personnel of receipt and understanding of responsibilities and obligations under the security policy.	Select	
e) Ensuring that vendor staff security training incorporates the obligation for card production staff to report any observed breaches of established security procedure.	Select		Examine the training materials for card production staff and security personnel to verify that they contain the obligation for card production staff to report any observed breaches of established security procedure.	Select	
f) Conducting mandatory training sessions at least annually. These sessions must include understanding the company security policies and the card production staff's responsibilities and their adherence to security policies.	Select		Examine a sample of documentation to verify the training occurred as stipulated.	Select	
g) Displaying information concerning security at key locations within the vendor facility via posters, notices, or electronic medium—e.g., monitors.	Select		Observe key locations within the vendor facility to verify that information concerning security is displayed.	Select	
h) Requiring that the individual with overall security responsibility reports to the board / Senior Executive Committee on a regular basis, preferably monthly, any security issues and the actions taken as a result.	Select		Examine documentation evidencing that the individual with overall security responsibility reports to the board / Senior Executive Committee on a regular basis, any security issues and actions taken as a result. The frequency must be documented in the report.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
1.1.7 Notification					
The vendor must notify the Vendor Program Administration (VPA) of any personnel changes that directly affect the security of card products and related components, including but not limited to:					
a) Senior management and corporate officers	Select		Examine a sample of notifications to the VPA of any personnel changes that directly affect the security of card products and related components, including but not limited to: • Senior management and corporate officers • Physical security manager • Card production staff authorized to receive or sign for any card components	Select	
b) Physical security manager	Select			Select	
c) Card production staff authorized to receive or sign for any card components	Select			Select	
1.2. Guards					
1.2.1 General Guidelines					
1.2.1.1 Prescreening					
a) In-house or contracted guards must meet the same prescreening qualification requirements as card production staff working in HSAs. For contracted guards, evidence of prescreening requirements may alternatively be provided by the guarding company, by copies of licenses, etc. The vendor must collect and retain this evidence provided by the guarding company.	Select		Examine a sample of pre-employment documentation to verify that the same prescreening qualification requirements are applied to in-house or contracted guards as card production staff working in HSAs.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) The vendor must ensure that any guard service contracted from an outside source maintains liability insurance to cover potential losses, or ensure that the vendor's own insurance policies provide suitable coverage.	Select		Examine all guard service agreement(s) for services contracted from outside sources to verify that they contain liability insurance coverage for potential losses, or that the vendor's own insurance policies provide suitable coverage.	Select	
1.2.1.2 Restrictions/Limitations					
a) Guards are not permitted to perform any of the functions normally associated with the production of card products or card components.	Select		Examine policies and procedures to verify that guards are not permitted to perform any of the functions normally associated with the production of card products or card components.	Select	
b) Guards must not have access to: • HSAs • Personnel records • Physical master keys that provide access to card production or provisioning areas • Audit logs	Select		Examine policies and procedures to verify that guards are not permitted access to the restricted areas and assets identified. Examine the access rights granted to a sample of guards on the access control system. Verify the guards do not have physical access to the HSA or to any restricted areas where the vendor processes, stores, or delivers card products and card components.	Select	
c) Guards must be prevented from modifying or altering the internal configuration settings on access system controls, intrusion alarm system, closed circuit television (CCTV).	Select		Interview system administrator(s) to verify the guards cannot modify or alter internal settings on access system controls, intrusion alarm system, closed circuit television (CCTV). Examine a sample of access permission settings to verify guards cannot modify or alter internal settings on access system controls, intrusion alarm system, closed circuit television (CCTV).	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Personnel who are pre-designated by management as first responders should have their badges pre-enabled to enter the HSA, even though prohibited under these security requirements. However, any such badge usage to enter the HSA constitutes a high-security event requiring mandatory incident reporting that must be escalated. To be allowed, the access must be automatically flagged by the access control system	Select		Examine policies and procedures to verify that management has pre-defined first responders to the HSA and that the use of such badge triggers a high-security event and is automatically flagged by the access-control system. Examine access-control system setting to verify that use of these first-responder access credentials is automatically flagged as a high-security event requiring mandatory incident reporting that must be escalated.	Select	
1.2.2 Role and Responsibilities					
The guards' main role is to (at a minimum, during working hours) protect the building, company assets, and staff by maintaining control of security systems, monitoring activities, and responding to alarms such as unauthorized access attempts. In addition, the vendor must ensure that:					
a) If an unauthorized access attempt is detected internally or reported by law enforcement agents, the guard must ensure emergency procedures are followed. The vendor must make an assessment of any unauthorized access attempt. Access attempts that are not accidental or testing must be reported to the VPA.	Select		Interview guards to confirm that they follow appropriate emergency procedures and give prompt attention to reports of unauthorized access to the facility received from law enforcement agents, and where necessary the VPA.	Select	
b) It maintains a clear segregation of duties and independence between the production staff and the guards.	Select		Interview guards and production staff to confirm that they have a clear segregation of duties and independence from the production staff.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Any time activities are performed in the HSA, the security control room is always occupied by at least one guard.	Select		Interview guards to confirm that at least one guard occupies the security control room any time activities are performed in the HSA. Examine a sample of access-control system activity logs, CCTV logs, or other mechanisms to verify that at least one guard is present in the security control room when the HSA is occupied.	Select	
1.2.3 Documentation					
1.2.3.1 Internal Security Procedures Manual					
The vendor must provide guards or any other person assuming the security functions outlined in this document with a copy of the vendor's internal security procedures manual, which at a minimum must include:			Examine the internal security procedures manual to verify that they contain the following minimum information:		
a) Guard's responsibilities, procedures, and activities by position	Select		• Guard's responsibilities, procedures, and activities by position	Select	
b) Vendor's security policies	Select		• Vendor's security policies	Select	
c) Interaction between production process management, contracted guard or monitoring services, the police, and other emergency services	Select		• Interaction between production process management, contracted guard or monitoring services, the police, and other emergency services	Select	
d) Access control at all entry and exit points of the facility, by date and time of activation	Select		• Access control at all entry and exit points of the facility, by date and time of activation	Select	
e) External resource response activities	Select		• External resource response activities	Select	
f) CCTV monitoring and video or digital recordings	Select		• CCTV monitoring and video or digital recordings	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
g) Administration of access credentials and photo ID badges	Select		• Administration of access credentials and photo ID badges	Select	
h) Access-control system and computer monitoring (such as the logging in and out of staff entering or leaving the facility and internal movement at area access points)	Select		• Access-control system and computer monitoring (such as the logging in and out of staff entering or leaving the facility and internal movement at area access points)	Select	
i) Company policy concerning card production staff, consultant, and visitor access to the facility (both exterior and interior)	Select		• Company policy concerning card production staff, consultant, and visitor access to the facility (both exterior and interior)	Select	
j) Property removal	Select		• Property removal	Select	
k) Shipping and receiving	Select		• Shipping and receiving	Select	
l) Alarm activation procedures	Select		• Alarm activation procedures	Select	
m) Response to alarms, including notification to law enforcement in cases of unauthorized access to the facility	Select		• Response to alarms, including notification to law enforcement in cases of unauthorized access to the facility	Select	
n) Daily activity and immediate incident report	Select		• Daily activity and immediate incident report	Select	
o) Potential threats—such as burglary or theft—to the facility's external or internal security	Select		• Potential threats—such as burglary or theft—to the facility's external or internal security	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
p) Handling of emergencies including but not limited to: • Fire • Earthquakes • Severe weather • Direct assault by armed felons • Bomb threats • Civil disturbances • Building evacuation • Ransom demands • Hostages • Kidnapping	Select		• Handling of emergencies including but not limited to: – Fire – Earthquakes – Severe weather – Direct assault by armed felons – Bomb threats – Civil disturbances – Building evacuation – Ransom demands – Hostages – Kidnapping	Select	
1.2.3.2 Guard Attestation of Security Procedures Manual Contents					
a) All guards, whether employees or contract, must sign a document indicating that they have read and fully understand the contents of this manual.	Select		Examine documentation that evidences signed acknowledgement by guards that they have read and fully understand the contents of the security procedures manual.	Select	
1.2.3.3 Security Procedures Manual Maintenance					
a) Procedures must be reviewed, validated and if necessary, updated annually.	Select		Examine documentation to verify updates occur annually as necessary.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
1.2.4 Security Training					
a) Guards must be trained and aware of all of their assigned tasks defined within the vendor's internal security procedures manual. Training must occur at least every 12 months and prior to the assignment of any new responsibilities. A record of the training session must be maintained.	Select		Interview guards to confirm that they have been trained and are aware of all of their assigned tasked as defined within the internal security procedures manual and that their training occurs at least every 12 months and prior to the assignment of any new responsibilities. Examine records evidencing the guards received the training at least annually.	Select	
b) Exceptional situations not specified within these manuals must be reported immediately to the physical security manager for appropriate action and possible inclusion into the manuals.	Select		Examine a sample of reports of any exceptional situations not specified within the security procedures manual to verify that they were reported to the physical security manager for appropriate action and possible inclusion into the security procedures manual.	Select	
1.3 Visitors					
a) Procedures for how visitors are managed at the vendor facility must be documented and followed.	Select		Examine the security procedures manual to verify it contains procedures for how visitors are managed at the vendor facility. Observe live visitor handling processes to confirm that the procedures are followed.	Select	
b) All visitors to the facility must be registered ahead of their arrival.	Select		Examine a sample of registration documentation to verify that all visitors are registered ahead of their arrival.	Select	
c) The registration must include name and company they represent.	Select		Examine a sample of registration documentation to verify that registration entries contain the visitor's name and the company they represent.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) If the visitor requires access to the HSA or cloud-based provisioning environment, this must be approved by both the physical security manager and the production manager.	Select		Examine a sample of documentation evidencing approval by both the security manager and the production manager for visitors that required access to the HSA or cloud-based provisioning environment.	Select	
e) Any unsolicited visitors must be turned away.	Select		Examine CCTV recordings or interview guards to verify that unsolicited visitors are turned away.	Select	
f) An authorized card production staff member must accompany all visitors at all times while they are in the facility.	Select		Interview the security manager to confirm that all visitors are accompanied by an employee at all times while they are in the facility. Observe the CCTV for previous visitors to determine that they were escorted by an employee at all times the visitors were in the facility. Examine documentation to verify procedures require that all visitors must be accompanied by employees at all times while within the facility.	Select	
g) Visitors must enter through the reception area.	Select		Examine the security procedures manual to verify it contains procedures for how visitors are managed at the vendor facility. Observe live visitor handling processes to confirm that the procedures are followed.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
1.3.1 Registration Procedures					
a) The vendor must apply the same registration procedures to all visitors entering their facility. These procedures must include the following: • Confirmation of previously agreed appointment • Verification of identification against an official, government-issued picture ID	Select		Examine documentation for registration of visitors entering the facility to verify the procedures include the procedures listed below. Examine a sample of documentation to verify that it contains evidence of the following: • Confirmation of previously agreed appointment • Verification of identification against an official, government-issued picture ID	Select	
b) The vendor must maintain records, manually or electronically, of all visitors who enter the facility. If a manual logbook is used, it must contain consecutive, pre-numbered, bound pages.	Select		Examine a sample of visitor logs to verify that they are maintained and that if the logs are maintained in a manual logbook, they contain consecutive, pre-numbered, bound pages.	Select	
c) All logs must be protected from modification.	Select		Examine the visitor logs to verify that they have protection from modification.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) The following information must be recorded in the logbook: • Name of the visitor, printed and signed • Number of the official ID document(s) presented and the date and place of issue • Company the visitor represents (if any) • Name of the person being visited or in charge of the visitor • Purpose of the visit • Visitor badge number • Date and time of arrival and departure • Signature of the card production staff member initially assigned to escort the visitor	Select		Examine the visitor logs to verify that the entries contain the minimum required information.	Select	
e) The vendor must retain visitors' registration records for at least 90 days.	Select		Examine the visitor logs to verify entries go back at least 90 days.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
1.3.2 Visitor Security Notification					
a) At a minimum, the vendor must make visitors aware of vendor security and confidentiality requirements, and the vendor-provided escort must ensure the visitor's adherence to those requirements.	Select		Interview the physical security manager to verify the vendor makes visitors aware of vendor security and confidentiality requirements, and the vendor-provided escort ensures the visitor's adherence to those requirements. Examine documentation to verify the vendor makes visitors aware of vendor security and confidentiality requirements.	Select	
1.3.3 Visitor Identification					
a) Each visitor entering the facility must be issued with and must wear visibly on their person a security pass or ID badge that identifies them as a non-employee.	Select		Observe live visitor processes to verify that visitors entering the facility are issued and wear visibly on their person a security pass or ID badge that identifies them as a non-employee.	Select	
b) If the security pass or ID badge is disposable, the visitor's name and date of entry to the facility and, if multi-day, the validity period must be clearly indicated on the front of the badge.	Select		Examine the visitor process and the disposable visitor security passes or ID badges handed out to the auditor to verify that the visitor's name, date of entry to the facility, and (if multi-day) the validity period are clearly indicated on the front of the badge.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) If the security pass or ID badge is the access-control type that enables a record to be kept of the visitor's movement throughout the facility: • The visitor must be instructed on its proper use. • The vendor must program the visitor access badge or card to enable the tracking of movement of all visitors. It should be activated only for areas that the visitor is authorized to enter. • Visitors must use their access card in the card readers to the room into which they enter. • Badging to track access must be used wherever feasible.	Select		Examine documentation to verify that if the security pass or ID badge is the access-control type that enables a record to be kept of the visitor's movement through the facility: • The visitor is instructed on its proper use. • The visitor access badge or card is programmed to enable the tracking of movement of that visitor and is activated only for areas that the visitor, while being escorted, is authorized to enter. • The visitor must use their access card in the card readers to the room into which they enter. • Badging to track visitor access is used wherever feasible.	Select	
d) Unissued visitor access badges must be securely stored.	Select		Observe the location where unissued visitor access badges are stored to verify that it is a secure location.	Select	
e) Any un-badged access must be recorded in a log. Logs may be electronic and/or manual.	Select		Examine a sample of visitor logs for entries of any un-badged visitor access to verify existence—e.g., vault or server room access.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) Card production staff responsible for escorting visitors while they are inside the facility must ensure that the visitor surrenders their ID badge to the receptionist or guard before leaving the building.	Select		Interview the receptionist or guard to verify that card production staff responsible for escorting visitors while they are inside the facility ensure the visitor surrenders their ID badge to the receptionist or guard before leaving the building.	Select	
1.4 External Service Providers					
1.4.1 General Guidelines					
The vendor must ensure that:					
a) Procedures that define how third parties are managed at the vendor facility are documented and followed.	Select		Examine the security manual to verify that procedures are documented for how third parties are managed at the vendor facility. Interview personnel to verify that the procedures are followed.	Select	
b) The requirements of Section 1.1.2, "Card Production Staff," of this document have been met by the employer of all suppliers, repair and maintenance staff, and any other external service provider.	Select		Examine documentation to verify that the employers of all suppliers, repair and maintenance staff, and any other external service providers comply with the requirements of Section 1.1.2.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) A pre-approved list of third parties is made available to the receptionist or to the guard on a daily or weekly basis for the preparation of ID badges. Only those persons with pre-approved ID badges may be granted facility access. The physical security manager or senior management must approve in writing any exceptions to this requirement.	Select		Interview the receptionist and the guard to confirm that one of them receives a pre-approved list of third parties with permitted access to the facility for the preparation of ID badges on a daily or weekly basis. Examine a sample of such lists against the visitor logs to verify that only those persons with pre-approved ID badges were granted facility access. Interview the physical security manager or senior management to confirm that they approve any exceptions to this requirement in writing.	Select	
d) An authorized card production staff member accompanies all external service providers at all times while they are in the HSA(s).	Select		Examine the security procedures manual to verify that all external service providers are required to be accompanied by an authorized card production staff member at all times while they are in the HSA(s). Examine a sample of CCTV footage to verify that procedures are followed.	Select	
e) All external service providers that require access to HSAs to service equipment have adequate liability insurance.	Select		Examine a sample of agreements with external service providers that require access to HSAs to service equipment to verify that they maintain adequate liability insurance.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) External service providers' staff requiring access to restricted or HSAs follow the visitor-registration procedures.	Select		Examine the security procedures manual to verify that external service providers' staff requiring access to restricted areas or HSAs are required to follow the visitor registration procedures. Examine documentation for a specific external service provider to verify that staff requiring access to restricted areas or HSAs follow the visitor-registration procedures.	Select	
1.5 Vendor's Agents					
1.5.1 General Guidelines					
a) Prior to conducting any business with an agent or third-party regarding card-related activities, the vendor must register the agent with the VPA and obtain the following information: • Agent's name, address, and telephone numbers • Agent's role or responsibility	Select		Examine the security procedures manual to verify that a process is in place to register with the VPA any agent or third party to conduct any business regarding card-related activities, prior to conducting such business. Examine a sample of registration documentation to verify it contains the following information: • Agent's name, address, and telephone numbers • Agent's role or responsibility	Select	
b) The vendor must inform the VPA whenever the agent relationship is changed or terminated.	Select		Examine the security procedures manual to verify that a process is in place to inform the VPA whenever the agent relationship is changed or terminated.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Agents of the vendor are not permitted to be in the possession of a card(s), card components, or card personalization data.	Select		Examine the security procedures manual to verify that agents are not permitted to be in the possession of a card(s), card components, or card personalization data. Interview the physical security manager to verify that agents of vendors are not permitted to be in the possession of a card(s), card components, or card personalization data.	Select	

Section 2: Facilities

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.1 External Structure					
2.1.1 External Construction					
a) Procedures for security controls implemented at the vendor facility must be documented and followed.	Select		Examine policy and procedures to verify security controls exist. Interview a sample of personnel to verify they are aware of the security controls policies and procedures and they are followed.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) The vendor must prevent unauthorized access to buildings, building areas, or structures containing technical machinery or equipment such as the heating system generator, auxiliary power supply, and air conditioning.	Select		Examine documentation to verify a process is in place to prevent unauthorized access to buildings, building areas, or structures containing technical machinery or equipment such as the heating system generator, auxiliary power supply, and air conditioning. Observe access and security-control mechanisms to verify they prevent unauthorized access to buildings, building areas, or structures containing technical machinery or equipment such as the heating system generator, auxiliary power supply, and air conditioning.	Select	
c) The vendor must protect doors that provide access to these by use of electrical or magnetic contacts that are permanently alarmed and that are connected to the security control-room panels.	Select		Examine settings of door contacts—electrical or magnetic—to verify they are permanently alarmed and are connected to the security control-room panels. Observe that doors that provide access to these by use of electrical or magnetic contacts are permanently alarmed and are connected to the security control-room panels.	Select	
d) The vendor must establish a specific procedure to disable these door alarms and to control the delivery of the access key any time that repair or maintenance staff must access this machinery or equipment.	Select		Examine security policy and procedures to verify security controls are in place when door alarms are disabled. Examine security controls to verify procedures are in place for delivery of access key(s) when repair/maintenance staff access technical machinery or equipment. Interview personnel to verify that specific procedures to disable these door alarms and security controls are in place for the delivery of the access key and at any time that repair or maintenance staff must access this machinery or equipment.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) The vendor must keep a log of the disabling of the alarm and the key exchange, describing at least: • Date • Time • Person(s) needing access • Purpose of the access	Select		Examine a sample of the logs for the activities of disabling the alarm and key exchange. Logs must describe at the minimum: • Date • Time • Person(s) needing access • Purpose of the access	Select	
2.1.2 Exterior Entrances and Exits					
All non-emergency exterior entrances and exits to the facility must be:					
a) Contact-alarm monitored	Select		Observe the exterior entrances and exits to verify they are contact-alarm monitored.	Select	
b) Locked or electronically controlled at all times	Select		Observe that all exterior entrances and exits are locked and are controlled at all times.	Select	
c) Reinforced, where applicable, to resist intrusion—e.g., steel or equivalent construction that meets local fire and safety codes.	Select		Observe external entrances and exits to determine whether they are reinforced, where applicable, to resist intrusion—e.g., steel or equivalent construction that meets local fire and safety codes.	Select	
d) Fitted with an access-control device—i.e., card reader or biometric—that automatically activates the locking mechanism	Select		Observe entrances and exits to determine whether they are fitted with an access-control device—i.e., card reader or biometric—that automatically activates the locking mechanism.	Select	
e) Fitted with a mantrap or interlocking configuration to prevent staff "piggybacking" or tailgating (excluding emergency exits)	Select		Observe entrances and exits to determine whether they are fitted with a mantrap or interlocking configuration to prevent staff "piggybacking" or tailgating (excluding emergency exits).	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.1.3 External Walls, Doors, and Windows					
a) All exterior walls must be pre-cast or masonry block or material of equivalent strength and penetration resistance. Any openings in the external wall that penetrate the building structure must be secured with security mesh, grating, or metal bars to prevent unauthorized access.	Select		Observe or examine documentation to determine all external walls, doors and windows are pre-cast or masonry block or material of equivalent strength and penetration resistance.	Select	
b) Windows, doors, and other openings must be protected against intrusion by mechanisms such as intruder-resistant—e.g., "burglar-resistant"—glass, bars, glass-break detectors, or motion or magnetic contact detectors.	Select		Observe to determine external windows, doors, and other openings are protected against intrusion by mechanisms such as intruder-resistant—e.g., "burglar-resistant"—glass, bars, glass-break detectors, or motion or magnetic contact detectors.	Select	
c) HSA windows must be non-openable.	Select		Observe to determine that all external HSA windows are non-openable.	Select	
2.1.4 Building Peripheral Protection					
a) The vendor must not place any device—e.g., carriers, waste containers, and tools—against the external wall protecting the outer perimeter of the vendor's facility.	Select		Observe vendor facility to verify any devices—e.g., carriers, waste containers, and tools—are not against the facility's external wall.	Select	
2.2 External Security					
a) The vendor facility must be located in an area serviced by public law enforcement and fire protection services in a timely manner.	Select		Interview personnel to determine the vendor facility is located in an area that is serviced on a timely basis by public law enforcement and fire protection services.	Select	
b) The facility must be secured with an intrusion alarm system as defined in Section 2.4.1, "Alarm Systems."	Select		Examine the policy and procedures (or appropriate documentation) to determine the facility is secured with an intrusion alarm system as defined in Section 2.4.1, "Alarm Systems."	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) The alarm system must be equipped with an auxiliary power or battery backup system with capabilities for ensuring operation for a minimum of 48 hours in the event of a power failure.	Select		Examine documentation to verify alarm system is equipped with an auxiliary power or battery backup system with capabilities for ensuring operation for a minimum of 48 hours in the event of a power failure. Observe that the alarm system is equipped with an auxiliary power or battery backup system with capabilities for ensuring operation.	Select	
d) All systems must notify the vendor in real time in the event the backup system is invoked.	Select		Examine documentation to verify all systems are to notify the vendor in real time in the event backup systems are invoked. Examine a sample of documentation—e.g., logs—to verify vendors are notified in real time in the event backup systems are invoked.	Select	
e) All external entry and exit points, including those for freight and maintenance, must be equipped with a peephole, a security window, or external CCTV that allows security personnel visual inspection of the immediate area, thus allowing action to be taken in the event of unauthorized access.	Select		Observe that all external entry and exit points, including those for freight and maintenance, are equipped with a peephole, a security window, or external CCTV cameras allowing security personnel to visually inspect the immediate area.	Select	
f) Alarms on external doors must be tested every three months.	Select		Examine a sample of evidentiary matter to verify external doors alarms have been tested every three months.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.2.1 Emergency Exits					
a) All emergency exits must be fitted with local audible alarms and monitored 24 hours a day and also must display a sign indicating "emergency exit door with alarm."	Select		Interview personnel to verify that emergency exits are monitored 24 hours a day. Observe via opening each emergency exit door to verify that: • Exits are fitted with local audible alarms and a sign is displayed indicating "emergency exit door with alarm." • Doors are fitted with an automatic closer to ensure self-latching of the door after being opened. • Doors are contact-alarm monitored.	Select	
b) Emergency exit doors must be fitted with an automatic closer to ensure self-latching of the door after being opened.	Select			Select	
c) Emergency exit doors must be contact alarm monitored.	Select			Select	
d) These doors must be used only in the event of an emergency and not used for any other purpose.	Select		Examine documents to verify emergency doors are used only in the event of an emergency. Interview personnel to verify that emergency doors are used only in the event of an emergency and not used for any other purpose.	Select	
e) During working hours, either the internal security control room or staff at a central monitoring service center must receive the signal from the emergency exits.	Select		Examine logs to verify security controls are in place for monitoring emergency exits based upon the aforementioned tests.	Select	
f) During non-business hours, the activation of an emergency-exit alarm must summon the local police, or a guard response directed by central monitoring service or on-site security control.	Select		Examine procedures to verify the central monitoring service responds to alarms during non-business hours when the emergency exit is open and that it summons the local police or onsite guard. Examine sample documents to verify the central monitoring services responds to emergency-exit alarms and summons the local police or on-site guard to response to the alert.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
g) Emergency exit doors must not be capable of being opened from the outside.	Select		Observe all emergency exit doors to verify they cannot be opened from the outside. Observe to verify that emergency exit door hinges have devices installed to prevent their being cut off from the outside and the door opened from the hinge side (hinge-protection bolts, hinge covers, hinged on the inside, etc.).	Select	
h) Emergency exits must not lead to a higher security area.	Select		Observe that all emergency exits do not lead to a higher security area.	Select	
2.2.2 Exterior Lighting					
a) Exterior lights must illuminate the exterior of the facility as well as all entrances and shipping and delivery areas, such that persons within these areas can be identified.	Select		Observe CCTV footage to verify that exterior lights illuminate the exterior of the facility as well as all entrances and shipping and delivery areas, such that persons within these areas can be identified.	Select	
b) The vendor must check all exterior lights monthly and must maintain a record for 24 months.	Select		Examine a sample of vendor logs to determine that all exterior lights are checked monthly and a record is maintained for 24 months.	Select	
2.2.3 Roof Access					
a) Trees, telegraph poles, fences, etc. located adjacent to the property line that might facilitate roof access must be removed, relocated, or otherwise secured against unauthorized access.	Select		Observe the facility to verify trees, telegraph poles, fences, etc. located adjacent to the property line that might facilitate roof access have been removed, relocated, or otherwise secured against unauthorized access.	Select	
b) All access points into the building from the roof must be locked or otherwise controlled from the inside.	Select		Observe to verify all access points into the building from the roof are locked or otherwise controlled from the inside.	Select	
c) All access points must have magnetic contacts or contact sensors both of which must have monitored access.	Select		Observe to verify all access points into the building from the roof have magnetic contacts or contact sensors, both of which have monitored access.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) All skylights, ventilation, and cooling system ducts that penetrate the building structure must be secured with security mesh, grating, or metal bars to prevent unauthorized access.	Select		Observe all skylights, ventilation, and cooling system ducts that penetrate the building structure are secured with security mesh, grating, or metal bars to prevent unauthorized access.	Select	
2.2.4 Exterior CCTV					
a) Exterior CCTV cameras must focus on all entrances and exits to the building and capture legible images of all persons entering or leaving the facility.	Select		Observe exterior CCTV cameras to verify they are focused on all entrances and exits to the building and capture legible images of all persons entering or leaving the facility.	Select	
b) Cameras must be monitored in the security control room during operational hours.	Select		Interview personnel to verify that cameras are monitored in the security control room during operational hours. Observe to verify that cameras are monitored in the security control room during operational hours.	Select	
2.2.5 Signage					
a) Signage on the exterior of the building must neither indicate nor imply that the vendor processes card products.	Select		Observe that signage on the exterior of the building neither indicates nor implies that the vendor processes card products.	Select	
2.3 Internal Structure and Processes					
2.3.1 Reception					
a) The main entrance to the building must lead visitors into a reception area that restricts any physical contact between visitor(s) and the receptionist/guard.	Select		Observe to verify that the main entrance to the building leads visitors into a reception area that restricts any physical contact between visitor(s) and the receptionist/guard.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) The reception area must be within a mantrap. *A mantrap is the secured space between doors operating on an electronic interlocking basis that may be accessed by a card-reader access system or a remote-control device, provided that all movement and activity is monitored.*	Select		Observe that the reception area for visitors is contained within a mantrap.	Select	
c) The receptionist or guard responsible for the entrance and departure of visitors must have an unobstructed view of the reception area at all times.	Select		Observe the receptionist(s) or guard(s) responsible for the entrance and departure of visitors to verify their view of the reception area is unobstructed at all times.	Select	
d) Visitors must be visually inspected in this area to confirm their identity and issued with identification badges before being admitted into the facility.	Select		Examine documents to verify visitors are visually inspected in this area to confirm their identity and are issued an identification badge before being admitted into the facility. Interview personnel to validate visitors are visually inspected in the reception area and: • Their identity is confirmed. • They are issued identification badges before being admitted into the facility.	Select	
e) The vendor must maintain a list at reception of all staff authorized to bring visitors into the vendor facility. Only people on the list are allowed to bring visitors into the facility.	Select		Examine documents to verify procedures are in place describing the process by which visitors are granted access to the facility and they stipulate that: • Only authorized staff can bring visitors into the facility • The list is maintained at the reception area. • Only people on the list are allowed to bring visitors into the facility. Examine evidence to verify that only authorized staff have been allowed to bring visitors into the facility.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) Visitors must only be allowed access beyond the reception area after identification has been established and the appropriate ID badge issued, which must be worn by the visitor at all times whilst inside the facility.	Select		Examine evidence to verify that visitors who are allowed access beyond the reception area have been identified and the appropriate ID badges have been issued. Observe to verify visitor(s) wear an ID badge at all times while inside the facility.	Select	
g) The electronic control points for operating this system must be located at the receptionist's desk or in the security control room.	Select		Observe the reception process to verify the electronic control points for operating the system are located at the receptionist's desk or in the security control room.	Select	
h) If the control points for operating the external doors are located at the receptionist's desk, the wall(s) separating the receptionist area from the reception room must be reinforced and fitted with a security window—i.e., a window of bullet-resistant transparent material containing a slot or device that allows the transfer of small packages and documents from the reception area to the receptionist or security guard.	Select		Observe whether the control points for operating the external doors are located at the receptionist's desk, then verify that the wall(s) separating the receptionist area from the reception room are: • Reinforced, and • Fitted with a security window—i.e., a window of bullet-resistant transparent material containing a slot or device that allows the transfer of small packages and documents from the reception area to the receptionist or security guard.	Select	
i) The vendor must provide card production staff working in these areas with a telephone and a duress button that activates a silent alarm at a remote, central monitoring service or police station or another vendor facility.	Select		Examine evidence that personnel working in these areas have at a minimum: • A telephone • A duress button that activates a silent alarm at a remote, central monitoring service or police station.	Select	
j) If the receptionist area houses or acts as a security control room, the requirements as defined in Section 2.3.2, "Security Control Room," must be met.	Select		Observe that if the receptionist area houses or acts as a security control room, the requirements as defined in Section 2.3.2, "Security Control Room," are met.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
k) Outside working hours, all security protection devices (including alarm activation and deactivation) must be monitored electronically by either an in-house security monitoring system or a private central monitoring company.	Select		Examine procedures to verify that outside working hours all security protection devices (including alarm activation and deactivation) are monitored electronically by either an in-house security monitoring system or a private central monitoring company. Examine a sample of documents to validate that outside working hours, all security protection devices (including alarm activation and deactivation) are monitored electronically by either an in-house security monitoring system or a private central monitoring company.	Select	
l) Card production staff may enter the facility through the main entrance area or through a card production staff-only entrance. The external entrance door of the building must not lead directly to the entrance of the HSA or the cloud-based provisioning area.	Select		Observe to verify that card production staff are entering the facility through the main entrance area or through an employee-only entrance. Observe the external entrance doors of the building to verify that it does not lead directly to the entrance of the HSA or the cloud-based provisioning area.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.3.2 Security Control Room					
This is the room housing the primary CCTV monitoring systems, intrusion, fire, and alarm-system control and access-control systems.					
2.3.2.1 Location and Security Protection					
The vendor must:					
a) Staff the room at all times while activity occurs in the HSA.	Select		Examine policy and procedures to verify that the room is staffed at all times while activity occurs in the HSA. Interview personnel to verify that the room is staffed at all times while activity occurs in the HSA. Observe random CCTV recordings of the security control room when activity occurs in the HSA. Examine access-control logs to verify the SCR was not left unoccupied.	Select	
b) Locate the security control room outside of the HSA and cloud-based provisioning environment to achieve the segregation of duties and independence between the guards and the HSA staff.	Select		Observe the location of the security control room to verify that it is located outside of the HSA and cloud-based provisioning environment.	Select	
c) Build the security control room of concrete block or other material offering similar resistance, if not part of the facility.	Select		Observe the build of the security control room to verify it is of concrete block or other material offering similar resistance, if not part of the facility.	Select	
d) Protect the room by an internal motion detector.	Select		Observe the security control room to determine it is protected by an internal motion detector.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) Fit the door giving access to the room with an in and out card reader access system plus an anti-pass-back software function connected to a computer that records all accesses and exits.	Select		Observe the access-control devices to verify the door providing access to the security control room has an in and out card reader access system plus an anti-pass-back software function connected to a computer that records all accesses and exits. Examine a sample of logs to verify all accesses and exits are being recorded. Observe via demonstration the anti-pass-back function by having the physical security manager badge the security control room access reader, open the door, then close the door. If the physical security manager badges the security control room access reader again, the door should not open, and this should be logged on the badge access system.	Select	
f) Ensure that the software counter registering the in and out card transactions in the access-control system logs the card transactions at the end of an access cycle (activation of the card reader with the access card, opening and closing of the door).	Select		Examine the access-control system logs to verify the software counter is registering the in and out card transactions at the end of an access cycle (activation of the card reader with the access card, opening and closing of the door).	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
g) Calibrate the security control room movement detector to generate an alarm if movement is detected inside the room when the software counter is zero (nobody registered in the room). The vendor must also calibrate the movement detector to generate an alarm if no movement within fifteen or fewer minutes is detected inside the room when the software counter is equal or greater than one (at least one person registered inside the room).	Select		Examine system configuration and interview personnel or observe a demonstration to verify the systems works as described: • An alarm is generated if movement is detected inside the room when the software counter is zero (nobody registered in the room). • An alarm is generated if no movement within fifteen or fewer minutes is detected inside the room when the software counter is equal or greater than one (at least one person registered inside the room). • The alarm is both locally audible and is sent directly to the alarm monitoring services (security control room and the external security company or police station).	Select	
h) Ensure that in both above scenarios the alarm is both locally audible and that an alarm must be sent directly to the alarm monitoring services (security control room and the external security company or police station).	Select		See g) above.	Select	
i) Fit the door with an automatic closing device. The opening of the door for more than 30 seconds must automatically activate a sound alarm. The access-control system must be programmed, whereby access is on a person-by-person basis—e.g., a full mantrap, turnstile, or similar that prevents more than one person entering at a time—and restricted to authorized personnel only. Person-by-person access may be fulfilled through a procedural control.	Select		Observe to verify that the door is fitted with an automatic closing device. Observe to verify that when the door is opened for more than 30 seconds an automatically activated alarm sounds. Examine the programmed setting to the access-control system to verify access is on a person-by-person basis and restricted to authorized personnel only. Examine evidence, if applicable, of how procedural controls are used for person-by-person access.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
j) Ensure that each individual entering or exiting completes the full cycle of badging in and badging out.	Select		Observe the process to validate each individual entering or exiting to verify the full cycle of badging in and badging out is followed. Examine a sample of logs to verify that each individual entering or exiting completed the full cycle of badging in and badging out.	Select	
k) Equip the security control room with two independent means of communication.	Select		Observe that the security control room is equipped with two independent means of communication.	Select	
l) Ensure that the access-control monitor permanently displays the access transactions on a real-time basis. Guards must be able to cross-check the access-control records with the CCTV images.	Select		Examine procedures to verify the access-control monitor displays the access transactions on a real-time basis and that guards cross-check the access-control records with the CCTV images. Observe that the access-control monitor displays the access transactions on a real-time basis. Observe the guards cross-check the access-control records with the CCTV images.	Select	
m) Train guards in the security control room in the effective use of the access-control system and CCTV system facility.	Select		Examine training documents to verify inclusion of training for the effective use of the access-control system and CCTV system facility. Examine training activity logs to verify all guards have gone through training.	Select	
n) Ensure that a security guard is assigned to watch real-time CCTV images on the monitors.	Select		Examine procedures to verify a process is in place for a security guard to be assigned to watch all real-time CCTV images on the monitors.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
o) Equip the room with a bullet-resistant security window facilitating the exchange of keys and documentation between the security control staff and external visitors or HSA staff while minimizing physical contact and access to unauthorized staff.	Select		Observe to verify the room is equipped with a bullet-resistant security window facilitating the exchange of keys and documentation between the security control staff and external visitors or HSA staff while minimizing physical contact and access to unauthorized staff. Examine documentation to validate the bullet-resistance of the security window facilitating the exchange of keys and documentation between the security control staff and external visitors or HSA staff.	Select	
p) Equip any other external-facing windows with bullet-resistant glass and mirror filming sufficient to prevent any observation from outside the building.	Select		Observe to verify that any other external-facing windows are equipped with bullet-resistant glass and mirror filming sufficient to prevent any observation from outside the building. Examine documentation to validate the bullet-resistance of any other external-facing windows.	Select	
q) Have mechanisms in place to prevent observation of security equipment—e.g., CCTV monitors—inside the security control room—for example, by covering all security control room windows with a one-way mirror film or other material preventing viewing from outside.	Select		Observe to verify mechanisms are in place to prevent observation of security equipment—e.g., CCTV monitors—inside the security control room—for example, by covering all security control room windows with a one-way mirror film or other material preventing viewing from outside.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
r) Ensure all other windows within the security control room are protected against intrusion by at least one of the following: iron bars, burglar-resistant glass, glass-break detectors, or motion detectors.	Select		Observe to verify all other windows within the security control room are protected against intrusion by at least one of the following: iron bars, burglar-resistant glass, glass-break detectors, or motion detectors. Examine documentation showing other windows are protected against intrusion by at least one of the following: iron bars, burglar-resistant glass, glass-break detectors, or motion detectors to validate that the security control is protected from intrusion.	Select	
s) Ensure that security room windows are non-openable.	Select		Observe to verify that security control room windows are non-openable.	Select	
t) Ensure that when the room is used for reception control, the conditions outlined in Section 2.3.1, “Reception,” apply.	Select		Examine to verify procedures are in place that when the room is used for reception control, the conditions outlined in Section 2.3.1, “Reception,” apply, in addition to SCR procedures. Interview personnel to verify procedures are following when the room is used for reception control.	Select	
u) The CCTV and access-control servers must be in the security control room or a room with equivalent security. The servers must not be in the HSA.	Select		Observe that the CCTV and access-control servers are in the security control room or a room with equivalent security. Observe that the servers are not in the HSA.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.3.3 High Security Areas (HSAs) *Areas in production facility where card products, components, or data are stored or processed are called high security areas. Only card production and provisioning-related activities shall take place within the HSA.*					
2.3.3.1 HSA Activities and General Controls					
a) At a minimum, the following activities must take place only in an HSA: • Card manufacturing • Chip embedding • Personalization • Storage • Packaging • Mailing • Shipping or delivery • Fulfillment • HCE and SE mobile provisioning	Select		Examine documentation to verify that the activities listed below only occur within the HSA. Observe to verify that the activities listed below, at a minimum, take place within the HSA and only within the HSA. Interview personnel to verify the activities listed below only occur within the HSA. • Card manufacturing • Chip embedding • Personalization • Storage • Packaging • Mailing • Shipping or delivery • Fulfillment • HCE and SE mobile provisioning	Select	
b) Card production staff may only bring items related to card production and provisioning activity into the HSA.	Select		Examine documentation to verify that card production staff are only allowed to bring in items related to card production and provisioning activity into the HSA. Observe that card production staff are only allowed to bring items related to card production and provisioning activity into the HSA. Interview personnel to verify that card production staff are only allowed to bring items related to card production and provisioning activity into the HSA.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) If a facility performs multiple production activities—e.g., card manufacturing and personalization—these activities must be performed in separate areas within the HSA.	Select		Examine documentation of HSA design to verify that if the facility performs multiple production activities, they are performed in separate areas within the HSA. Observe to verify that if the facility performs multiple production activities, they are performed in separate areas within the HSA. Interview personnel to verify that if the facility performs multiple production activities, they are performed in separate areas within the HSA.	Select	
d) With the exception of mobile provisioning, if multiple HSAs are within the same building, they must be contiguous.	Select		Examine documentation to verify that if multiple HSAs are within the same building, they are contiguous, with the exception of mobile provisioning. Observe to verify that if multiple HSAs exist within the same building, they are contiguous, with the except of mobile provisioning.	Select	
e) Equipment that is purely associated with test activities is not allowed in the HSA.	Select		Interview personnel to verify equipment that is associated with test activities is not allowed in the HSA. Observe that equipment associated with test activities is not allowed in the HSA.	Select	
f) A mobile provisioning system must exist in either a server room in the HSA or, if the only activity by the vendor, its own room meeting the criteria for an HSA.	Select		Interview personnel to verify that any mobile provisioning system exists in either a server room in the HSA or, if the only activity by the vendor, its own room meeting the criteria for an HSA. Observe that any mobile provisioning system exists in either a server room in the HSA or, if the only activity by the vendor, its own room meeting the criteria for an HSA.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.3.4 HSA – Security Protection and Access Procedures					
2.3.4.1 Access Control					
a) Access to the HSA must be restricted to authorized persons through an access-control system, working on a strict person-by-person basis.	Select		Examine policy and procedures to verify that access controls to the HSA are in place. Examine a sample of logs and access-control settings to verify access to the HSA is restricted to authorized persons through an access-control system, working on a strict person-by-person basis. Observe that access to the HSA is restricted to authorized persons through an access-control system, working on a strict person-by-person basis.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Access-control systems must: • Always be connected to the computer that monitors and logs all staff and visitor movements. • Prevent personnel from piggybacking. • Enforce person-by-person access. • Implement anti-pass-back mechanisms. • Enforce dual presence. If the number of authorized card production staff is less than two for more than a minute, the alarm must be activated.	Select		Examine access-control systems documentation to verify that they: • Are always connected to the computer that monitors and logs all staff and visitor movements. • Prevent personnel from piggybacking. • Enforce person-by-person access. • Implement anti-pass-back mechanisms. • Enforce dual presence. If the number of authorized card production staff is less than two for more than a minute, the alarm must be activated. Observe access-control systems to verify that they: • Are always connected to the computer that monitors and logs all staff and visitor movements. • Prevent personnel from piggybacking. • Enforce person-by-person access. • Implement anti-pass-back mechanisms. • Enforce dual presence. If the number of authorized card production staff is less than two for more than a minute, the alarm must be activated.	Select	
c) The vendor must program the software access-control system, whereby access is on a person-by-person basis and restricted to authorized personnel.	Select		Examine access settings to verify that the vendor has programmed the software access-control system access to a person-by-person basis and is restricted to authorized personnel.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) The access-control system must activate the alarm system each time the last person leaves the HSA.	Select		Examine access-control system settings to verify the access-control system will activate an alarm system each time the last person leaves the HSA. Examine a sample of logs to verify that the access-control system activated the alarm system each time the last person left the HSA.	Select	
e) The HSA and all separate rooms within the HSA must be protected by internal motion detectors, even if no production occurs in the room.	Select		Observe the HSA and all separate rooms within the HSA to verify they are protected by internal motion detectors, even when no production occurs in the room. Observe via inspection that every enclosed room has motion detectors installed, and open-plan areas have sufficient devices installed to ensure motion will be detected by someone walking through the area (100% coverage is not required).	Select	
f) The motion detector must generate an alarm if movement is detected inside the HSA or rooms within the HSA when the access-control system indicates the room is not occupied—e.g., the software counter is zero—nobody registered in the room.	Select		Examine motion detector settings to verify that it generates an alarm if movement is detected inside the HSA or rooms within the HSA when the access-control system indicates the room is not occupied—e.g., the software counter is zero—nobody registered in the room. Observe via demonstration for each enclosed room inside the HSA by arranging for all personnel to exit the room using their badge or biometric and leaving one person behind when the occupancy is zero to verify that an alarm is raised locally and at the SCR (2.3.4.1.g).	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
g) The warning must be a local sound alarm and notification (silent and/or audible alarm) within the security control room. Additionally, after working hours, a simultaneous alarm to the local external security company or local police must occur.	Select		Examine documentation policy and procedures to verify that: • The alarm is a local sound alarm; • Notification (silent and/or audible alarm) occurs within the security control room; and • After working hours, a simultaneous alarm to the local external security company or local police occurs. Observe that the warning is a local sound alarm and notification (silent and/or audible alarm) occurs within the security control room.	Select	
h) No one is allowed to bring personal items (for example, packages, lunch containers, purses) or any electronic devices (including but not limited to mobile telephones, photo cameras, and PDAs) into the high security area. Medical items such as medications and tissues are acceptable if in clear containers that can be examined. No external food or beverages are allowed. Company may provide water stations with disposable bottles and cups. These must be brought in/out through the goods/tools trap and be discarded in the trash before exiting the HSA.	Select		Examine documentation to validate what is allowed and not allowed in the HSA. This includes but not limited to: • No personal items (for example, packages, lunch containers, purses) or any electronic devices (including but not limited to mobile telephones, photo cameras, and PDAs) into the high security area. • No personal food or beverages are allowed. • Medical items such as medications and tissues are acceptable if in clear containers that can be examined. Interview personnel to verify policy is being followed. Observe that no personal items are brought into the HSA and that any company-provided water is brought in/out through the goods/tools trap and is discarded in the trash before existing the HSA.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
i) If the access-control server is not located in the security control room, it must be located in a room of equivalent security. The access-control server cannot be located in the HSA but must be located in the same facility.	Select		Observe to verify that if the access-control server is not located in the security control room that it is located in a room of equivalent security. Observe to verify that the access-control server is not located in the HSA.	Select	
2.3.4.2 Person-by-Person Access Control and Anti-pass-back Software Function					
a) Access must be enforced by the use of an air lock, single sluice, or security turnstile, which must be controlled by logical means, ensuring strict compliance with the person-by-person mandate.	Select		Observe to verify that access is enforced by the use of an air lock, single sluice, or security turnstile. Examine security settings to verify that access controls are activated by logical means, ensuring strict compliance with the person-by-person mandate. Observe via demonstration the person-by-person access control, by attempting for two personnel to cross the control point together.	Select	
b) Activation of the access device must be controlled by a card reader that enforces an anti-pass-back function.	Select		Examine settings to verify activation of the access device is controlled by a card reader that enforces an anti-pass-back function. Observe via demonstration that activation of the access device is controlled by a card reader that enforces an anti-pass-back function.	Select	
c) The card readers must be permanently connected to a computer that centralizes the logging of any card reader activation.	Select		Observe to verify the card readers are permanently connected to a computer that centralizes the logging of any card reader activation. Examine a sample of logs to verify the computer is the centralized mechanism that is logging all card reader activations.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) The status of the access must change only when the person has successfully completed the access cycle.	Select		Examine access-control settings to verify that the status of access changes only when the person has successfully completed the access cycle. Examine a sample of logs to verify the status of access changes only when the person has successfully completed the access cycle.	Select	
2.3.4.3 Transfer of Materials					
a) All physical materials required for production must be transferred to the HSA through either a goods-tools trap or the shipping and delivery area.	Select		Examine documentation to verify that all physical materials required for production are transferred to the HSA through either a goods-tools trap or the shipping and delivery area. Observe to verify that all physical materials required for production must be transferred to the HSA through either a goods-tools trap or the shipping and delivery area.	Select	
b) A goods-tools trap or a shipping and delivery area must be used to transfer physical materials between different HSAs within the same facility.	Select		Observe that a goods-tools trap or similar mechanism is used to transfer physical materials between different HSAs.	Select	
2.3.4.4 Security Controls					
a) Bullet-resistant—e.g., UL 752—glass or iron bars must protect all windows in HSAs that are on an exterior wall or door of the building.	Select		Examine documentation to verify bullet-resistant—e.g., UL 752—glass or iron bars protects all windows in HSAs. Observe that bullet-resistant glass or iron bars are used to protect all windows in HSAs.	Select	
b) It must not be possible to view activities in the HSA from the exterior of the building—e.g., by use of opaque or non-transparent glass.	Select		Observe to validate that activities in the HSA cannot be viewed from the exterior of the building—e.g., by use of opaque or non-transparent glass. ***Note:*** *See Annex A for further clarification.*	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Walls and ceilings must be constructed around the HSA consistent with the enforcement of dual presence—e.g., prevention of access via false ceilings or raised floors.	Select		Examine documentation to verify that the walls and ceilings are constructed around the HSA consistent with the enforcement of dual presence—e.g., prevention of access via false ceilings or raised floors. Observe to validate that the walls and ceilings are constructed around the HSA consistent with the enforcement of dual presence—e.g., prevention of access via false ceilings or raised floors.	Select	
d) All access points—e.g., electrical conduits, opening windows, and ventilation shafts—in HSAs must have physical barriers.	Select		Examine documentation to verify that all access points—e.g., electrical conduits, opening windows, and ventilation shafts—in/to the HSAs have physical barriers. Observe a sufficient sample of access points to verify that all access points—e.g., electrical conduits, opening windows and ventilation shafts—in/to the HSAs have physical barriers.	Select	
e) Windows are not permitted to be opened. Windows that are openable windows must additionally be fitted with contact monitors to detect the opening of the window in order to prevent card components from being passed through the windows.	Select		Examine documentation to verify that windows are not permitted to be opened, and if openable, they are fitted with contact monitors to detect the opening of the window in order to prevent card components from being passed through the windows. Observe to validate that the windows in the HSAs either cannot be opened, or if openable have been fitted with contact monitors to detect the opening of the window.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) The entire HSA must be covered by CCTV as defined in Section 2.4.5, "Closed Circuit Television (CCTV)."	Select		Examine security-control documentation to verify the HSA has CCTV coverage as defined in Section 2.4.5, "Closed Circuit Television (CCTV)." Observe to verify the HSA is covered by CCTV as defined in Section 2.4.5, "Closed Circuit Television (CCTV)."	Select	
g) All doors and gates to these areas must be contact monitored and fitted with automatic closing or locking devices and audible alarms that sound if the door or gate remains open for more than 30 seconds.	Select		Examine access-control system settings to validate audible alarms sound if the door or gate remains open for more than 30 seconds. Observe that all doors and gates to these areas are contact monitored and fitted with automatic closing or locking devices. Examine a sample of logs to verify the audible alarms are sounded if the door or gate remains open for more than 30 seconds.	Select	
h) All doors must be fitted with an in and out card reader access system plus an anti-pass-back function connected to a computer that records all movements.	Select		Examine settings to validate that all doors are fitted with an in and out card reader access system plus an anti-pass-back function connected to a computer that records all movements. Observe to verify that all doors are be fitted with an in and out card reader access system plus an anti-pass-back function connected to a computer that records all movements.	Select	
i) Doors must not open directly to the building's exterior unless they are alarmed emergency exit doors.	Select		Observe to verify that doors do not open directly to the building's exterior unless they are alarmed emergency exit doors.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
j) Emergency exits must be fitted with local audible alarms and monitored 24 hours a day and also must display a sign indicating "emergency exit door with alarm."	Select		Observe emergency exits to verify they: • Are fitted with local audible alarms. • Display a sign indicating "emergency exit door with alarm." • Are monitored 24 hours a day.	Select	
2.3.4.5 Minimum Number of Persons					
a) Whenever any room within the HSA is occupied, it must contain a minimum of two authorized card production staff. This must be enforced by the access-control system.	Select		Observe via demonstration the access-control system by requesting that one authorized person authenticates to the access reader: • If the door opens, does a "single occupancy" alarm sound within a 60-second period? • If the door does not open, verify that it opens after two authorized authentications have been presented.	Select	
2.3.5 Rooms					
a) Separate rooms within the HSA must meet all of the HSA requirements with the exception of person-by-person access.	Select		Examine HSA documentation to verify separate rooms within the HSA meet all of the HSA requirements with the exception of person-by-person access. Observe that separate rooms within the HSA meet the HSA requirements with the exception of person-by-person access.	Select	
b) Toilet rooms are prohibited except where required by local law. Where used, the entry/exit way must be camera-monitored.	Select		Examine documentation to verify that toilets, if present, are required by local law. Observe to determine that, if present, the toilet room's entry/exit ways are camera-monitored.	Select	
c) If the HSA contains fire doors and these doors are normally closed or can be manually closed, then these doors are subject to the same access controls as any other door that provides access to a room.	Select		Observe to verify that any fire doors present in the HSA are normally closed or can be manually closed, and these doors are subject to the same access controls as any other door that provides access to a room.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) If the HSA contains fire doors and these doors are locked open and only closed automatically when a fire alarm is activated, then the access controls that normally apply for accessing a room do not apply.	Select		Observe to verify that any fire doors present in the HSA that are locked open and only closed automatically when a fire alarm is activated, do not require the access controls that normally apply for accessing a room.	Select	
Within the HSA, the following separate rooms may exist:					
2.3.5.1 Pre-Press Room					
a) The pre-press process must be performed in a separate room within the HSA.	Select		Observe to verify that the pre-press process is performed in a separate room within the HSA.	Select	
b) The pre-press room is where the vendor produces or stores film, plates, or electronic media.	Select		Observe to verify that the pre-press room is the location where the vendor stores film, plates, or electronic media.	Select	
2.3.5.2 Work in Progress (WIP) Storage Room					
a) This room must be segregated from production and protected at a minimum by wire mesh.	Select		Observe the WIP storage room to verify it is segregated from production and is protected by at a minimum by wire mesh.	Select	
b) If wire mesh is used in the construction of such areas, it must extend from the floor to enclose the entire room on all surfaces, including a top (if below the ceiling).	Select		Observe to verify that if wire mesh was used in the construction of such areas, it extends from the floor to enclose the entire room on all surfaces, including a top (if below the ceiling).	Select	
c) Doors to these areas must be contact monitored and fitted with an audible alarm that sounds when the door remains open for more than 60 seconds.	Select		Observe to verify that the doors to these areas are contact monitored and fitted with an audible alarm that sounds when the door remains open for more than 60 seconds.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Reinforced exterior walls may be used as part of the perimeter of these areas provided that these walls do not contain any door(s) or window(s).	Select		Examine construction documentation where reinforced exterior walls are used as part of the perimeter to verify that the walls do not contain any door(s) or window(s). Observe where reinforced exterior walls are used as part of the perimeter to verify that the walls do not contain any door(s) or window(s).	Select	
e) CCTV surveillance is mandatory and must cover the entire area, ensuring that there are no blind spots.	Select		Observe CCTV surveillance camera video to determine that coverage exists for the entire area, ensuring that there are no blind spots.	Select	
2.3.5.3 Card Product and Component Destruction Room(s)					
a) Destruction of card product and component waste must take place in a separate room(s) within the HSA that is dedicated for destruction.	Select		Observe to verify that destruction of card product and component waste takes place in a separate room(s) within the HSA that is dedicated for destruction.	Select	
b) Destruction by a third party may take place in the loading bay using portable/mobile equipment. All requirements for a destruction room must be met for this temporary usage.	Select		Examine documentation to verify that destruction by a third party takes place in the loading bay using portable/mobile equipment. Examine a sample of video logs to verify all requirements for a destruction room are met for this temporary usage. Interview personnel to verify destruction by a third party that takes place in the loading bay using portable/mobile equipment meets all requirements for a destruction room for this temporary usage.	Select	
2.3.5.4 PIN Mailer Production Room					
a) PIN mailer production must be performed in a separate room within the HSA.	Select		Observe to verify that PIN mailer production is performed in a separate room within the HSA.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Card production staff involved in personal identification number (PIN) printing and mailing processes must not monitor or be involved in the personalization, encoding, and embossing of the related cards. Individuals may perform other non-personalization activities in addition to PIN printing, except for those that give access to cardholder data such as data administration, packaging, or mailing activities.	Select		Examine documentation to verify that card production staff involved in personal identification number (PIN) printing and mailing processes must not monitor or be involved in the personalization, encoding, and embossing of the related cards, but can perform other non-personalization activities in addition to PIN printing, except for those that give access to cardholder data such as data administration, packaging, or mailing activities. Interview personnel to determine procedures are followed as stated.	Select	
c) Personnel involved in personalization must never be involved in PIN printing of the associated cards. Defined procedures must demonstrate that these personnel are not involved in the production of the associated cards.	Select		Examine procedures to verify that personnel involved in personalization are never involved in PIN printing of the associated cards. Interview personnel involved in personalization to verify they are never involved in PIN printing of the associated cards.	Select	
d) PIN mailers must be printed in such a way that the plaintext PIN cannot be observed until the envelope is opened. The envelope must display the minimum data necessary to deliver the PIN mailer to the correct customer. PIN mailers must be tamper-evident so that it is highly likely that accidental or fraudulent opening will be obvious to the customer.	Select		Examine documentation to verify PIN mailer procedures exist. Examine a sample of PIN mailers to verify: • PIN mailers are printed in such a way that the plaintext PIN cannot be observed until the envelope is opened. • The envelope displays the minimum data necessary to deliver the PIN mailer to the correct customer. • PIN mailers are tamper-evident so that it is highly likely that accidental or fraudulent opening will be obvious to the customer.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) PIN mailers must be mailed as defined in Section 4.5, "Delivery."	Select		Examine a sample of logs to verify PIN mailers are mailed as defined in Section 4.5, "Delivery." Observe to verify that PIN mailers are mailed as defined in Section 4.5, "Delivery."	Select	
f) No activity other than PIN mailer production may take place in the room.	Select		Interview personal to verify that no activity other than PIN mailer production takes place in the room. Observe to verify that no activity other than PIN mailer production takes place in the room.	Select	
g) All re-runs of jobs to print PINs must be pre-approved in writing by management.	Select		Examine policy and procedures to verify that re-runs of jobs to print PINs are pre-approved in writing by management. Examine a sample of logs to verify that re-runs of jobs to print PINs are pre-approved in writing by management.	Select	
h) Reports and PIN mailers must not display printed PIN data in the clear.	Select		Examine a sample of Reports and PIN mailers to verify that printed PIN data is not displayed in the clear.	Select	
i) PIN mailers must not contain the associated cardholder account number.	Select		Examine a sample of PIN mailers to verify that they do not contain the associated cardholder account number.	Select	
j) PIN mailers must be stored in the vault or the PIN printing room prior to shipment.	Select		Interview personnel to validate that PIN mailers are stored in the vault or the PIN printing room prior to shipment. Observe that PIN mailers are stored in the vault or the PIN printing room prior to shipment.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
k) All waste material from the PIN-printing process must be destroyed as defined in Section 3, "Production Procedures and Audit Trails."	Select		Examine policy and procedures to verify that all waste material from the PIN-printing process must be destroyed as defined in Section 3, "Production Procedures and Audit Trails." Interview personnel to verify that all waste material from the PIN-printing process is destroyed as defined in Section 3, "Production Procedures and Audit Trails." Observe that all waste material from the PIN-printing process is destroyed as defined in Section 3, "Production Procedures and Audit Trails."	Select	
2.3.5.5 Server Room & Key Management Room					
a) Server processing and key management must be performed in a separate room within the personalization HSA. Data preparation must occur here. Server processing and key management may occur in the same room or each in a separate room.	Select		Observe to verify server processing, key management, and data preparation are performed in a separate room within the personalization HSA.	Select	
b) Systems and applications that make up the cloud-based provisioning network must be physically segregated from other vendor networks and Internet-connected networks. This includes separation of servers, firewall, and HSM. *For example, in a traditional card vendor environment this could be:* • *A separate rack in a server room, or* • *In a provisioning-only entity, housed in a separate room or cage in a data center.*	Select		Observe the location where cloud-based provisioning network components are located to verify the servers, firewalls, and HSMs are: • Physically separated from similar components used for other purposes—e.g., not in the same rack as other similar components used for other purposes; or • In a provisioning-only entity, housed in a separate room or cage in a data center.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Systems and applications that make up the cloud-based provisioning network cannot be in the same rack as other servers used for different purposes.	Select		Observe the cloud-based provisioning network to verify that its systems and applications are not located in the same rack as other servers used for different purposes.	Select	
d) An internal CCTV camera must be installed to cover the access to this room and provide an overview of the room whenever there is activity within it.	Select		Observe that internal CCTV cameras: • Are installed to cover the access to the key-management and server room. • Provide an overview of the room. • Are positioned in such a manner to not allow observation of keystroke entry or the monitoring of the screen.	Select	
e) The camera must not have zoom or scanning functionality and must not be positioned in such a manner as to allow observation of keystroke entry or the monitoring of the screen.	Select		Examine CCTV camera settings to verify configurations of the cameras do not have zoom or scanning functionality.	Select	
2.3.5.6 Vault *The vault is the primary security area in the vendor facility.*					
a) The following must be stored in the vault: • Cards awaiting personalization • Security components • Materials awaiting destruction • Samples and test cards prior to distribution and after return • Any card that is personalized with production data • If the facility is closed, personalized cards that will not be shipped within the same working day • Products awaiting return to the supplier	Select		Examine documentation to verify the following, at a minimum, are to be stored in the vault: • Cards awaiting personalization • Security components • Materials awaiting destruction • Samples and test cards prior to distribution and after return • Any card that is personalized with production data • If the facility is closed, personalized cards that will not be shipped within the same working day • Products awaiting return to the supplier Observe the contents of the vault to verify that the aforementioned are stored in the vault.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Vaults must be constructed of reinforced concrete (minimum 15 centimeters or 6 inches) or at least meet the Underwriters Laboratories Class 1 Burglary Certification Standard—e.g., UL 608 or the European Standard for Secure Storage Units (EN1143-1 class 6)—which provides for at least 30 minutes of penetration resistance to tool and torch for all perimeter surfaces—i.e., vault doors, walls, floors, and ceilings. ***Note:*** *EN 1143-1 Secure storage units - Requirements, classification, and methods of test for resistance to burglary - Part 1: Safes, ATM safes, strongroom doors and strongrooms: Grade 6 or higher may be used as equivalent to UL 608 Class 1 Burglary Certification.*	Select		Examine documents for the design of the vault to verify that it is constructed of reinforced concrete or at least meets the Underwriters Laboratories Class I Burglary Certification Standard—e.g., UL 608 or EN1143-1 class 6). Observe the vault to verify the design is constructed as stated above.	Select	
i. An outside wall of the building must not be used as a wall of the vault.	Select		Observe to verify that an outside wall of the building is not used as a wall of the vault.	Select	
ii. If the construction of the vault leaves a small (dead) space between the vault and the outside wall, this space must be constantly monitored for intrusion—e.g., via motion sensors.	Select		Observe to verify that if the construction of the vault leaves a small (dead) space between the vault and the outside wall, the space is constantly monitored for intrusion—e.g., via motion sensors. Examine evidence to verify that any small (dead) space between the vault and the outside wall is constantly monitored for intrusion.	Select	
iii. No windows are permitted.	Select		Observe to verify that no windows are in the vault.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
iv. There must be no access to the vault except through the vault doors and gate configurations meeting these requirements. The vault must be protected with a sufficient number of intruder-detection devices that provide an early attack indication—e.g., seismic, vibration/shock, microphonic wire, microphone, etc.—on attempts to enter and also provide full coverage of the walls, ceiling, and floor.	Select		Observe access to the vault to verify the following exist to protect access to the vault: • The vault has a sufficient number of intruder-detection devices that provide early attack indication—e.g., seismic, vibration/shock, microphonic wire, microphone, etc.—for any attempts to enter as well as full coverage of the walls, ceiling, and floor; and • Access to the vault is only through vault doors and gates configured with intruder-detection devices.	Select	
v. The vault must be fitted with a main steel-reinforced door with a dual-locking mechanism (mechanical and/or logical—e.g., mechanical combination and biometrics) that requires physical and simultaneous dual-control access. The access mechanism requires that access occurs under dual control and does not allow entry by a single individual—i.e., it is not feasible for a single individual to use credentials belonging to someone else to simulate dual access.	Select		Observe to verify the protection of the vault includes but is not limited to: • Vault is fitted with a main steel-reinforced door with a dual-locking mechanism (mechanical and/or logical—e.g., mechanical combination and biometrics) that requires physical and simultaneous dual-control access. • Vault has access mechanism that requires access under dual control and does not allow entry by a single individual—i.e., it is not feasible for a single individual to use credentials belonging to someone else to simulate dual access.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Opening of the main vault door must always be under dual control requiring two authorized staff to be simultaneously present and involved in the opening and closing of the door.	Select		Examine procedures to verify opening and closing of the main vault door is always under dual control. Examine a sample of logs to verify opening and closing the main vault door is always under dual control. Observe the opening and closing of the main vault door to verify it is under dual control.	Select	
d) If the vault door is required to remain open during production hours, an inner grille must be used. The vault door or inner grille must remain closed and locked at all times, except when staff require access to the vault for example to store or remove items. The inner grille must meet the same access-control criteria as other rooms within the HSA.	Select		Observe (if the vault door is required to remain open during production hours) to verify: • An inner grille is used • The inner grille remains closed and locked at all times, except when staff require access to the vault—for example, to store or remove items. • The inner grille meets the same access-control criteria as other rooms within the HSA.	Select	
e) The vault door or the inner grille must be equipped with an automatic closing device and must automatically activate a simultaneous sound alarm, locally and in the security control room, if opened for more than 60 seconds.	Select		Observe that the vault door or the inner grille are equipped with: • An automatic closing device • An automatically activated simultaneous sound alarm that will be heard locally and in the security control room, if opened for more than 60 seconds. • Observe sample documents—e.g., logs—to verify the existing controls are in place.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) Emergency exit doors from the vault to the HSA must meet the strength requirements for a vault door, must be alarmed and not capable of being opened from outside, and must conform to the requirements for emergency exits.	Select		Examine documentation to verify emergency exit doors from the vault to the HSA: • Meet the strength requirements for a vault door. • Have alarms. • Are not capable of being opened from outside. Observe to verify emergency exit doors meet the requirements in place.	Select	
g) Card components being taken in or out must be recorded in a vault log and confirmed by at least two card production staff.	Select		Examine documentation—e.g., a sample of logs—to verify card components taken in or out of the vault are recorded in a vault log and confirmed by at least two card production staff. Interview personnel to verify procedures are followed.	Select	
h) Maintenance of these audit control logs is mandatory as defined in Section 3.7.2, “Vault Audit Controls.” These logs must be retained for the longer of five years or the oldest card in the vault.	Select		Examine a sample of the logs to verify that they are retained for the longer of five years or the oldest card in the vault.	Select	
i) If the vault also is used to store non-payment products, it must be physically segregated—e.g., stored on dedicated aisles or shelves—to create a physical separation between payment products and other card types.	Select		Observe to verify that if the vault is used to store non-payment products, these non-payment products are physically segregated to create a physical separation between payment products and other card types.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
j) All boxes with payment cards must have a label, visibly attached, describing the product type, a unique product identifier number, the quantity of cards contained in the box and the date of control.	Select		Observe boxes with payment cards to verify they have a label visibly attached, detailing: • The product type, • A unique product identifier number, • The quantity of cards contained in the box, and • The date of control.	Select	
k) Unsealed boxes are only permitted for stock that requires multiple pulls per day. Unsealed boxes must be in a centralized area within the vault. The counting process must be applied during the pull process, and an inventory count under dual control must be performed for each unsealed box at the end of each shift. All other boxes must be sealed.	Select		Observe a sample of unsealed boxes to verify: • Unsealed boxes are only permitted for stock that requires multiple pulls per day. • Unsealed boxes must be in a centralized area within the vault. • Counting processes are applied during the pull process. • Inventory counts under dual control are performed for each unsealed box at the end of each shift. All other boxes are sealed.	Select	
l) Vault storage must be organized so that it is possible to identify the location of any stock item within the vault.	Select		Observe the vault storage to verify that it is organized to be able to identify the location of any stock item within the vault.	Select	
m) CCTV surveillance is mandatory and must cover the entire area, ensuring that there are no blind spots.	Select		Examine a sample of CCTV surveillance media to verify coverage is the entire vault area is covered including that there are no blind spots. Observe the vault to identify whether blind spots exist that are not covered.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.3.6 Other Areas					
2.3.6.1 Goods-tools Traps					
Goods-tools trap configuration options are as follows:					
a) One-room configuration: The goods-tools trap is composed of a unique, closed, solid construction room (goods transfer room) and two doors (inner and external) minimizing the physical contact between the individuals collecting or delivering materials and the HSA staff. In this configuration, the goods-tools trap must be operated as follows: • The movement detector is deactivated when someone swipes the access card in the card reader. • The person opens the door, introduces the package, and closes the door. • The movement detector is reactivated automatically, so any person inside the goods-tools trap is detected. If someone is detected, the cycle cannot be completed, and the other goods-tools trap door cannot be opened to take the package back. • If no motion is detected in the trap, and the first door has been closed, the second door in the HSA can be opened for someone to take the package.	Select		Observe good tools trap configuration: • If a one room configuration is used, perform test procedures for Requirement a). • If a two-room configuration is used, perform the test procedures for Requirement b) below. Observe the room configuration to verify the goods-tools trap one-room is configured and operated as follows: • Composed of a unique, closed, solid construction room (goods transfer room) and two doors (inner and external), minimizing the physical contact between the individuals collecting or delivering materials and the HSA staff. • Movement detector is deactivated when someone swipes the access card in the card reader. • The person opens the door, introduces the package, and closes the door. • Movement detector is reactivated automatically, so any person inside the goods-tools trap is detected. • If someone is detected, the cycle cannot be completed, and the other goods-tools trap door cannot be opened to take the package back. • If no motion is detected in the trap, and the first door has been closed, the second door in the HSA can be opened for someone to take the package.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Two-room configuration: • In this configuration, the goods-tools trap is composed of two consecutive rooms, similar to the classical shipping and delivery room configuration. • Security requirements, protection devices, and access procedures are the same as for the standard shipping and delivering area configuration, as defined below.	Select		Observe to verify it is configured and operated as follows: • Goods-tools trap is composed of two consecutive rooms, similar to the classical shipping and delivery room configuration. • Security requirements, protection devices, and access procedures are the same as for the standard shipping and delivering area configuration, as defined below.	Select	
2.3.6.2 Shipping and Delivery Areas					
a) To facilitate the shipment and delivery of card components, the loading/unloading area must be composed of at least two consecutive enclosed rooms and three doors (external, intermediate, and inner), which minimizes physical contact between the individuals collecting or delivering materials and the shipment/delivery card production staff. ***Note:*** *If existing facilities have used wired enclosures for the outer room, they may continue. All new facilities requiring initial validation against these requirements must comply with the requirement as written—i.e., a room that is part of the building structure.*	Select		Observe to verify the shipping and delivery areas (loading/unloading) of card components to have at a minimum: • At least two consecutive enclosed rooms and three doors (external, intermediate, and inner), and • Minimization of physical contact between the individuals collecting or delivering materials and the shipment/delivery card production staff.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) All shipping and delivery doors must operate on an electronic and interlocking basis so that when one of the doors is open the others are electronically locked.	Select		Observe a demonstration of the shipping and delivery processes to verify the shipping and delivery doors operate on an electronic and interlocking basis so that when one of the doors is open the others are electronically locked. Test in multiple configurations with different doors starting in the open position. With all doors closed, try opening multiple doors at the same time—i.e., badging and/or pressing open buttons together for different doors.	Select	
c) An intercom communications system must be contained in this area to allow identification of incoming drivers.	Select		Observe to verify that an intercom communications system is operational in this area to allow identification of incoming drivers.	Select	
d) One of the rooms in the shipping area must contain a solution to allow the exchange of control documents without coming into contact with external personnel, as well as being able to communicate with and visually identify them—e.g., a security window, video intercom, CCTV monitors, etc.	Select		Observe to verify that one of the rooms in the shipping area: • Contains a solution to allow the exchange of control documents without coming into contact with external personnel; and • Allows communication with and visual identification of external personnel.	Select	
e) The inner shipping/delivery area door must have access control installed to restrict access to authorized users and to record usage. The logging at a minimum must include each opening and closing of the door.	Select		Examine to verify the inner shipping/delivery area door to verify it has access control installed to restrict access to authorized users and to record usage are in place. Examine a sample of logs to verify the shipping/delivery area doors have access controls installed to restrict access to authorized users and that these records log each opening and closing of the doors, at a minimum.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) The guards may operate the external door of the outer room area only after the driver is identified and the production staff is informed about the ongoing shipment or delivery operation. To prevent unauthorized access to the HSAs through the shipping and delivery rooms, the inner room must be protected by an internal movement detector that prevents the opening of the internal door and the intermediate door of the inner room if movement is detected inside this inner room.	Select		Examine policy and procedures to verify access-control mechanisms exist to support the prevention of unauthorized access to the HSAs to include that the inner room is protected by an internal movement detector that prevents the opening of the internal door and the intermediate door of the inner room if movement is detected inside this inner room. Example a sample of logs to identify activity times and the associated CCTV recordings to verify the guards operate the external door of the outer room area only after the driver has been identified and the production staff is informed about the ongoing shipment or delivery operation. Interview a sample of guards and other personnel to verify that procedures are followed.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
g) An alarm must be generated automatically and logged in the central alarm system, and all shipment and delivery area doors must be blocked each time movement is detected by the movement detector located inside the inner room when the intermediate and inner doors are both closed and locked.	Select		Examine policy and procedures to verify the central alarm system generates an alarm when movement is detected by the movement detectors located inside the inner room when the intermediate and inner doors are both closed and locked. Examine policy and procedures to verify the shipment and delivery area doors are blocked each time movement is detected by the movement detectors located inside the inner room when the intermediate and inner doors are both closed and locked Examine a sample of logs to verify an alarm was generated automatically and logged in the central alarm system, and that all shipment and delivery area doors were blocked each time movement is detected by the movement detector located inside the inner room when the intermediate and inner doors are both closed and locked.	Select	
h) To liberate a person detected inside the room and stop the alarm, the software monitoring the access-control system must only allow the opening of the last activated door. Either a logical (software) or physical (alarm report book) log of the event must be kept for at least two years.	Select		Examine the procedures to verify a process is in place to release a person found inside the room and that the software monitoring the access-control system allows the opening of only the last activated door. Examine either a logical (software) or a physical (alarm report book) log of such events to validate a record is kept.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
i) The vendor must install CCTV cameras and orient the cameras to cover the external and inner access doors to the shipping and delivery areas and capture all activities during shipping and delivery operations.	Select		Observe the CCTV camera locations to verify the CCTV cameras cover the external and inner access doors to the shipping and delivery areas, and capture all activities during shipping and delivery operations. Observe displayed or recorded images to verify the CCTV cameras cover the external and inner access doors to the shipping and delivery areas, and capture all activities during shipping and delivery operations.	Select	
j) The vendor must install at least: • One external CCTV camera covering the external shipping and delivery area door and its environment • Two CCTV cameras inside the outer room covering all sides of the vehicle • One CCTV camera inside the inner room covering the shipping and delivery operations	Select		Observe to verify the CCTV cameras from the security control room have been installed to cover at a minimum: • One external CCTV camera covering the external shipping and delivery area door and its environment • Two CCTV cameras inside the outer room covering all sides of the vehicle • One CCTV camera inside the inner room covering the shipping and delivery operations	Select	
k) The images captured and recorded by these CCTV cameras must be displayed on the security control room monitors in real time, allowing the guards to control the shipping and delivery operations.	Select		Observe to verify that the images for the cameras noted in the prior section are displayed on the security control room monitors in real time.	Select	
l) These images must also be displayed on a monitor located beside the security window, allowing the production staff to oversee the shipping and delivery operations.	Select		Observe the monitor located beside the security window to verify the images are displayed on that monitor visible to the production staff overseeing the shipping and delivery operations.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.4 Internal Security					
2.4.1 Alarm Systems					
a) To alert personnel working in the vicinity of and in the security control room, local alarms or flashing lights must activate when a door or gate to a restricted area is left open for more than 30 seconds except where otherwise specified in this document.	Select		Observe a sample demonstration to verify that local alarms or flashing lights are activated when a door or gate to a restricted area is left open for more than 30 seconds except where otherwise specified in the security requirements.	Select	
b) The alarm system must be protected by an auxiliary power or battery backup system with capabilities for ensuring operation for a minimum of 48 hours in the event of a power failure.	Select		Examine documentation to verify the alarm system is protected by an auxiliary power or battery backup system with capabilities for ensuring operation for a minimum of 48 hours in the event of a power failure. Observe the presence of an auxiliary power or battery backup system to verify the alarm system is protected with backup power in the event of a power failure.	Select	
c) The system must notify the vendor in real time in the event the backup system is invoked.	Select		Examine documentation to verify a process is in place for the backup system to notify the vendor in real time in the event the backup system is invoked. Examine a sample of documents—e.g., logs or alarm testing—to verify the system notified the vendor in real time when backup systems were invoked. Interview the physical security manager to determine the method and technology used to notify the vendor in real time in the event back-up systems are invoked.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) The alarm activation and deactivation must be checked and confirmed by an electronic device, guards, private security company, or local police force to ensure that the pre-arranged alarm time settings have been respected. The alarm deactivation process must allow for the generation of a fast, silent alarm in case of threat.	Select		Examine alarm policy and procedures to verify at a minimum: • The alarm activation and deactivation are checked and confirmed by an electronic device, guards, private security company, or local police force to ensure that the pre-arranged alarm time settings have been respected. • The alarm deactivation process allows for the generation of a fast, silent alarm in case of threat. Examine a sample of logs to verify the alarm activation and deactivation is checked and confirmed by an electronic device, guards, private security company, or local police force to ensure that the pre-arranged alarm time settings have been respected. Interview personnel to verify the alarm deactivation process allows for the generation of a fast, silent alarm in case of threat.	Select	
i. A specific procedure must be established to ensure quick corrective action in case an alarm is not activated in accordance with pre-arranged alarm time settings.	Select		Examine documentation to verify that a specific procedure has been established to ensure quick corrective action in case an alarm is not activated in accordance with pre-arranged alarm time settings. Interview personnel to verify they are knowledgeable of and able to execute the procedure.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
ii. Alarm activation and deactivation codes must be known only by guards or security team members authorized to use them.	Select		Interview personnel to verify alarm activation and deactivation codes are known only by the guards or security team members authorized to use them. Examine documentation to verify alarm activation and deactivation codes are known only by the card production staff authorized to use them.	Select	
iii. Codes must be deactivated upon termination of any guards or security team members with knowledge of the code.	Select		Interview personnel to verify alarm activation and deactivation codes are deactivated upon termination of any staff with knowledge of the code. Examine documentation to verify alarm activation and deactivation codes are deactivated upon termination of any staff with knowledge of the code.	Select	
iv. Guards and card production staff must follow these procedures in case of alarm system activation. These procedures must be clearly described and included in the internal security procedures manual.	Select		Examine the internal security procedures manual to verify that it states guards and card production staff must follow described procedures in case of alarm system activation. Interview guards and card production staff to verify they know the procedures in case of an alarm system activation. Examine a sample of training materials to verify guards and card production staff know the procedures in case of an alarm system activation.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) Access contacts and motion detectors must be activated in zones where no staff are present—e.g., vault, storage, production areas, shipping and delivery areas.	Select		Examine documents to verify access contacts and motion detectors are to be activated in zones where no staff are present—e.g., vault, storage, production areas, shipping and delivery areas. Examine a sample of logs to verify access contacts and motion detectors are activated in zones where no staff are present—e.g., vault, storage, production areas, shipping and delivery areas. Observe a demonstration of someone badging in and badging out, but not actually egressing the restricted area to verify the detection works.	Select	
2.4.2 Badge Administration					
2.4.2.1 Identification Badges					
a) Procedures must be documented and followed for managing identification (ID) badges.	Select		Examine badging administration documentation to verify procedures are defined for managing ID badges. Examine a sample of logs to verify procedures are followed in managing ID badges.	Select	
b) The vendor must issue a photo identification (ID) badge to each card production staff member and consultant. A temporary badge valid ONLY for the work shift does not need to contain a picture.	Select		Examine documented procedures to verify the vendor issues a photo identification badge to each card production staff member and consultant. Examine a sample of logs to verify badge issuance to card production staff and consultants.	Select	
c) ID badges and lanyards must not be imprinted with the company name or logo and are not allowed to be imprinted with any information that may identify the vendor's name or location.	Select		Observe to verify that ID badges and lanyards do not contain the corporate name or logo or any information that may identify the vendor's name or location.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Access credentials (which may be the ID badge) must be programmed only for the access required based on job function.	Select		Examine access-control procedures to verify that the access credentials (which may be the ID badge) are programmed only for the access required based on job function. Examine to verify a sample of access credentials (which may be the ID badge) are programmed only for the access required based on job function. Interview personnel to verify access is required based on job function.	Select	
2.4.2.2 ID Badge or Access Card Usage					
a) The access-control system must grant physical access to card production staff or consultants only during authorized working hours, and only to those areas required by the card production staff or consultants' job functions.	Select		Examine access-control system settings to verify physical access to card production staff or consultants is only during authorized working hours, and only to those areas required by the card production staff or consultants' job functions. Examine a sample of logs to verify that the physical access is only granted during authorized working hours and only to the areas required by the individual's job functions. Observe a demonstration of one or more individuals attempting to access areas they are not authorized for to verify the access-control system prevents that access.	Select	
b) Personnel must display their ID badges at all times while in the facility.	Select		Observe that personnel display their ID badges at all times while in the facility.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Card production staff and consultants are responsible for their ID and access badges and must report any lost/stolen or broken badges to the physical security manager immediately.	Select		Examine documentation to verify policies and procedures address but are not limited to: • Card production staff and consultants are responsible for securing their ID badge from loss or theft. • If an individual determines his/her ID badge has been lost or misplaced, they must notify the physical security manager immediately. Interview personnel to verify they have knowledge to report any lost/stolen or broken badges to the physical security manager immediately. Examine sample reports to verify lost/stolen or broken badges have been reported to the security manager.	Select	
d) The audit logs of the ID badge access-control system changes and exception conditions must be reviewed weekly to ensure badge assignments are appropriate and the system is functioning appropriately.	Select		Examine logs to verify that the audit logs of the ID badge access-control system changes and exception conditions are reviewed weekly to ensure badge assignments are appropriate and the system is functioning appropriately.	Select	
2.4.2.3 ID Badge or Access Card Inventory and Management					
The physical security manager is responsible for unassigned ID badges and must:					
a) Maintain an inventory of unassigned ID badges.	Select		Examine the unassigned badge inventory log to verify completeness.	Select	
b) Ensure dual control exists for badge access and distribution to individuals.	Select		Examine procedures to validate a process is in place to have dual control for badge access and distribution to individuals. Examine a sample of logs to verify dual control for badge access and assignments.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Ensure ID badges are retrieved from terminated individuals prior to their departure from the facility.	Select		Examine procedures to validate a process is in place to retrieve ID badges from terminated individuals prior to their departure from the facility. Examine a sample of terminated personnel documentation to verify ID badges were retrieved from each terminated individual prior to their departure from the facility.	Select	
d) Ensure all access rights are immediately deactivated.	Select		Examine procedures to validate a process is in place to deactivate all access rights immediately on a departure of an individual. Examine a sample of terminated personnel documentation to verify all access rights were immediately deactivated.	Select	
e) Maintain precise documentation accounting for all lost badges.	Select		Examine documentation to verify a process is in place to maintain documentation to account for all lost badges. Examine a sample of documentation to verify existence of an audit trail of all lost badges.	Select	
2.4.3 Access-Control System					
a) The vendor must document, follow, and maintain procedures for access-control system administration.	Select		Examine policy and procedures to verify access-control system administration is documented and maintained. Interview personnel to verify personnel follow the procedures for access-control system administration.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Access-control systems that allow entry into restricted areas must have a backup electrical power source capable of maintaining the system for 48 hours.	Select		Examine documentation to verify the access-control systems into restricted areas are protected by a backup electrical power source with capabilities for ensuring operation for a minimum of 48 hours in the event of a power failure. Observe the presence of a backup electrical power source with capabilities for ensuring operation of the access-control system for a minimum of 48 hours in the event of a power failure.	Select	
c) Contingency plans must exist for securing card components in the event of an outage greater than 48 hours.	Select		Examine contingency plans to verify procedures exist to secure card components in the event of an outage greater than 48 hours. Interview personnel to verify procedures are known and followed for securing card components in the event of an outage greater than 48 hours.	Select	
d) For multiple buildings within the same facility, a single central location for an access-control system can administer all buildings. Either a private or public network may be used. If a public network is used, a VPN as defined in the *PCI Card Production and Provisioning – Logical Security Requirements and Test Procedures* in conformance with the requirements stipulated therein must be used.	Select		Interview personnel to determine if a single central location for the access-control administration system is used to administer multiple buildings within the same facility and if so, whether a private or public network is used. If yes to central administration *and* use of a public network above, examine documentation to determine that a VPN as defined in the PCI CP&P Logical Security Requirements is used.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.4.3.1 Activity Reports					
a) All procedures for access control must be documented and kept current.	Select		Examine documentation to verify access-control procedures exist and are current. Interview the access-control system administrator to validate access documents are current.	Select	
b) The access-control system must log sufficient information to produce the daily card activity reports detailed below: • Card reader • Card reader status • Card identification • Date and time of access • Access attempts results • Unauthorized attempts • Anti-pass-back violation and corrective actions taken • Access-control system changes describing: – The date and time of the change, – The reasons for the change, and – The person who made the change.	Select		Examine a sample of access-control system logs to verify they contain the following information at a minimum: • Card reader • Card reader status • Card identification • Date and time of access • Access attempts results • Unauthorized attempts • Anti-pass-back violation and corrective actions taken • Access-control system changes describing: – The date and time of the change, – The reasons for the change, and – The person who made the change.	Select	
c) The physical security manager must review these reports weekly.	Select		Examine evidence that the physical security manager is reviewing reports weekly.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) The access-control system audit trail must be maintained for at least three months.	Select		Examine access-control system setting to verify that audit trails are enabled and are kept for three months. Examine a sample of reports to verify the access-control system audit trail is maintained for at least three months.	Select	
2.4.3.2 System Administration					
The vendor must ensure that:					
a) Each access-control system administrator uses his or her own user ID and password.	Select		Examine access-control system documentation to validate each access-control system administrator uses his or her own user ID and password. Interview personnel to verify that each access-control system administrator uses his or her own user ID and password.	Select	
b) Passwords are changed at least every 90 days.	Select		Examine documentation to verify procedures are in place that passwords are changed at least every 90 days. Examine a sample of system configurations to verify passwords required to be changed at least every 90 days. Interview personnel to verify that passwords are changed at least every 90 days.	Select	
c) User IDs and passwords are assigned to the physical security manager and authorized personnel, who must be employees.	Select		Examine documentation to verify that user IDs and passwords are assigned to the physical security manager and authorized personnel Interview personnel to verify that access-control system administrators are vendor employees. Examine a sample of logs to verify user IDs and passwords are assigned to the physical security manager and authorized personnel.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) The physical security manager and other authorized personnel (who must be employees) are the only individuals able to modify the access- control system controls. All changes to the system must be logged.	Select		Examine documentation to verify that the physical security manager and other authorized personnel (who must be employees) are the only individuals able to modify the access-control system controls and that all changes to the system are logged. Examine a sample of logs to verify the physical security manager and other authorized personnel are the **only** individuals who modified the access-control system controls.	Select	
e) At the end of each session, the individual who initiated the session must log off the system.	Select		Interview personnel to verify at the end of each session, the individual who initiated the session is the one who must log off the system.	Select	
f) All changes to card production, provisioning, and security-relevant systems are recorded and reviewed monthly by a senior manager who is not the individual initially involved in changing the system.	Select		Examine documentation to verify all changes to card production, provisioning, and security-relevant systems are required to be recorded and reviewed monthly by a senior manager who is not the individual initially involved in changing the system. Examine a sample of change-management documents to verify that all changes to card production, provisioning, and security-relevant systems are recorded and reviewed monthly by a senior manager who is not the individual initially involved in changing the system. Interview personnel to verify all changes to card production, provisioning, and security-relevant systems are reviewed monthly by a senior manager who is not the individual initially involved in changing the system.	Select	
g) Access-control systems are physically and logically isolated on a dedicated network from the main office network.	Select		Interview personnel to verify that the access-control systems are physically and logically isolated on a dedicated network from the main office network.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.4.3.3 Remote-access Controls					
a) Offsite access to the access-control system is not permitted.	Select		Examine documentation to verify that the remote-access requirements listed below are met where system administration is performed remotely. Examine a sample of reports to verify system administrators follow requirements for remote access as stipulated below. Examine documentation to verify vendor facilities not subject to logical security audits have a written statement that requirements are being met. Interview personnel to verify that the following remote-access requirements are met where system administration is performed remotely: • Offsite access to the access-control system is not permitted. • Access-control system data must be backed up on a weekly basis. • Access-control systems administration must be performed from within the security control room. • For generic administrative accounts that cannot be disabled, the password must be used only for emergency. The password must be changed from the default value and managed under dual control. In addition, the access-control system must meet the logical security requirements in Appendix B.	Select	
b) Access-control system data must be backed up on a weekly basis.	Select			Select	
c) Access-control systems administration must be performed from within the security control room.	Select			Select	
d) For generic administrative accounts that cannot be disabled, the password must be used only for emergency. The password must be changed from the default value and managed under dual control.	Select			Select	
e) In addition, the access-control system must meet the logical security requirements in Appendix B.	Select			Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.4.4 Duress Buttons					
2.4.4.1 Location					
Duress buttons must be located in the following areas:					
a) Reception	Select		Observe that the duress buttons are located in the following areas: • Reception • Security control room • The vault • Shipping and delivery area • Every card production staff entrance	Select	
b) Security control room	Select			Select	
c) The vault	Select			Select	
d) Shipping and delivery area	Select			Select	
e) Every card production staff entrance	Select			Select	
2.4.4.2 Activation					
a) When a duress button is activated, a warning or emergency signal must be sent to an on-site security control room, a remote central monitoring station, or the local police station. The anticipated initial response—i.e., event verification—must be within two minutes.	Select		Examine a sample of past events or of testing documentation to demonstrate when a duress button is activated the following occurs but not limited to: • A warning or emergency signal is sent to an on-site security control room. • A remote central monitoring station, or the local police station. • The anticipated initial response—i.e., event verification—is within two minutes.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) All details relating to the activation of the duress button and the response by the remote central monitoring service or the local police must be recorded in the control log, including the following: • Time and date when the duress button was activated • Time taken by the remote central monitoring service to respond • Time taken by the police or other help to respond/arrive on site • Chronology of all related activities, including names of personnel involved • Reason for activating alarm	Select		Examine that procedures are in place related to the activation of the duress button to require that the response by the remote central monitoring service or the local police be recorded in the control log. Examine a sample of logs to verify that details related to the activation of the duress button and the response by the remote central monitoring service or the local police was recorded in the control log, including the following at a minimum: • Time and date when the duress button was activated • Time taken by the remote central monitoring service to respond • Time taken by the police or other help to respond/arrive on site • Chronology of all related activities, including names of personnel involved • Reason for activating alarm	Select	
2.4.4.3 Testing					
a) All duress buttons must be tested, and the results documented on a quarterly basis.	Select		Examine a sample of logs to verify quarterly tests are performed on all duress buttons and that the results are documented.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.4.5 Locks and Keys					
2.4.5.1 Key Receipt and Return *The term "key" as used below refers to any physical key or combination giving access to a restricted area, including those inside the HSA or cloud-based provisioning area.*					
a) Procedures for managing keys must be documented and followed.	Select		Examine documentation to verify that key-management procedures exist and are followed. Interview personnel to verify that key-management procedures are known and are followed. Examine sample documents to validate key-management procedures are followed.	Select	
b) Card production staff who are issued keys must sign a consent form indicating they received such keys and that they will ensure that the key(s) entrusted to them cannot be accessed by unauthorized individuals.	Select		Examine procedures for issuance of keys and the requirement that they be entrusted to authorized personnel. Examine evidence to verify those who are issued keys have signed a consent form indicating they received keys and they understand they are entrusted these keys and the keys cannot be accessed by unauthorized individuals.	Select	
c) All unissued keys, master keys, and duplicate keys must be maintained under dual control in a safe or secure cabinet.	Select		Examine policy and procedures that all unissued keys, master keys, and duplicate keys are maintained under dual control in a safe or secure cabinet. Interview personnel to verify unissued keys, master keys, and duplicate keys are maintained under dual control. Observe storage of all unissued keys, master keys, and duplicate keys to verify they are maintained under dual control in a safe or secure cabinet.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Any transfer of responsibility between the staff issuing the key and the key recipient must be recorded in a specific key logbook.	Select		Examine documentation to verify procedures for personnel who transfer responsibility between the staff issuing the key and the key recipient require recording in a specific key logbook. Examine a sample of key logbook entries to verify that any transfer of responsibility between the staff issuing the key and the key recipient is recorded in a specific key logbook.	Select	
2.4.5.2 Audits and Accountability					
a) The key logbook must have consecutive, pre-numbered, bound pages and must contain at least the following information: • Key identification number • Date and time the key is issued (transfer of responsibility) • Name and signature of the card production staff member issuing the key • Name and signature of the authorized recipient • Date and time the key is returned (transfer of responsibility) • Name and signature of the authorized individual returning the key • Name and signature of the card production staff member receiving the key	Select		Examine documentation to verify procedures require the key logbook to contain the information listed below at a minimum. Examine a sample of the key logbook to verify the key logbook has consecutive, pre-numbered, bound pages and contains at least the following information at a minimum: • Key identification number • Date and time the key is issued (transfer of responsibility) • Name and signature of the card production staff member issuing the key • Name and signature of the authorized recipient • Date and time the key is returned (transfer of responsibility) • Name and signature of the authorized individual returning the key Name and signature of the card production staff member receiving the key	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) If an electronic system is used to control access to keys, that system must be administered under dual control and be able to produce a report with equivalent information.	Select		Examine procedures to verify that if an electronic system is used to control access to keys, the system is administered under dual control and is able to produce a report with equivalent information as above. Observe the electronic system used to control access to keys to verify it is administered under dual control and is able to produce a report with equivalent information.	Select	
c) For keys that allow access to sensitive materials, the physical security manager must conduct a quarterly review of: • The key logbook • The list of card production staff authorized to hold keys • The locks each key operates	Select		Examine documentation to verify that a process exists for the physical security manager to review the following for keys issued that allow access to sensitive materials. • The key logbook • The list of card production staff authorized to hold keys • The locks each key operates Examine evidence that for keys that allow access to sensitive materials, the physical security manager performed a quarterly review of: • The key logbook • The list of card production staff authorized to hold keys • The locks each key operates	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) The physical security manager must sign and date each of the key-control documents, attesting that the review process was completed.	Select		Examine documentation to verify a process is in place for the physical security manager to, at a minimum: • Sign and date each of the key-control documents; and • Attest that the review process was completed. Examine a sample of records to verify the physical security manager performed the key-control process as noted above.	Select	
2.4.5.3 Master Keys					
a) The physical security manager and executive managers are the only employees authorized to possess master or overriding keys to restricted areas.	Select		Examine documentation to verify that the physical security manager and executive managers are the only employees authorized to possess master or overriding keys to restricted areas. Examine a sample of logs to verify the physical security manager and the executive managers are the only employees who have used master or overriding keys to restricted areas.	Select	
2.4.5.4 Safe and Vault Combinations					
a) Combinations for any combination locks where a combination holder had access must be changed when a combination holder is removed from the list of authorized combination holders.	Select		Examine documentation to verify that combinations for any combination locks where a combination holder had access must be changed when a combination holder is removed from the list of authorized combination holders. Examine a sample of logs to verify that combinations for any combination locks where a combination holder had access was changed when a combination holder was removed from the list of authorized combination holders.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.4.6 Closed Circuit Television (CCTV)					
2.4.6.1 CCTV Cameras					
a) Procedures for managing the facility's CCTV must be documented and followed.	Select		Examine documentation to verify CCTV procedures are documented. Interview personnel to verify they are aware of and follow the CCTV procedures. Examine a sample of documents to verify CCTV media are managed per the policy.	Select	
b) All CCTV cameras must be tested, and the images displayed by the monitors checked for clear visibility at least monthly. The vendor must maintain a record of such testing on file for a minimum of two years.	Select		Examine documentation to verify a process for all CCTV cameras to be tested and the images displayed by the monitors checked for clear visibility at least monthly; and that a maintenance record is retained on file for a minimum of two years. Observe CCTV footage from different times of day (including nighttime) to verify that identifiable images of individuals entering or leaving the facility are captured at all times. Interview security personnel and examine evidence to verify that: • Cameras are tested and monitors checked at least monthly to confirm clarity of images. • Records of such testing are retained for a minimum of two years.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) In case of CCTV disconnection, the "video loss" notification displayed by the monitors located in the security control room must be accompanied by a sound alarm.	Select		Interview personnel to validate that when a CCTV disconnection occurs, the "video loss" notification displayed by the monitors located in the security control room is accompanied by a sound alarm. Observe—e.g., by requesting that authorized personnel disconnect a camera for a short moment—the "video loss" notification displayed by the monitors located in the security control room is accompanied by a sound alarm; or Examine a sample of records to verify that for a CCTV disconnection, the "video loss" notification displayed by the monitors located in the security control room was accompanied by a sound alarm.	Select	
d) Both the digital recording and access-control systems must be synchronized with real time. The synchronization of the systems must be within two seconds of one another.	Select		Observe the digital recording and access-control systems to verify both are synchronized with real time—e.g., an external NTP source—and that the systems are within two seconds of one another.	Select	
e) The recording system must be able to replay any recorded sequence without stopping the normal recording operation.	Select		Observe a sample of CCTV media to verify the recording system is able to replay any recorded sequence without stopping the normal recording operation.	Select	
f) CCTV cameras in server rooms and PIN-mailer rooms must not contain (or must have disabled) zoom or scanning functionality.	Select		Examine CCTV camera settings located in server rooms and PIN-mailer rooms to verify zoom or scanning functionality are disabled. Observe that CCTV cameras in server rooms and PIN-mailer rooms do not contain (or have disabled) zoom or scanning functionality.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.4.6.2 Monitor, Camera, and Digital Recorder Requirements					
a) Each monitor, camera, and digital recorder must function properly and produce clear images on the monitors without being out-of-focus, blurred, washed out, or excessively darkened. The equipment must record at a minimum of four frames per second.	Select		Examine each monitor, camera, and digital recorder settings and documentation to verify that camera recordings provide the following at a minimum: • Four (4) picture frames per second on motion or four (4) picture frames per second permanently; and • Clear images on the monitor without being out-of-focus, blurred, washed out, or excessively darkened.	Select	
b) CCTV cameras must record all activity, including recording events during dark periods through the use of infrared CCTV cameras or automatic activation of floodlights in case of any detected activity. This recording may be via motion activation. The recording must capture any motion at least five seconds before and after the detected motion.	Select		Examine CCTV camera settings and documentation to verify that camera recordings—e.g., via motion activation—provide a minimum of the requirements listed below. Observe a demonstration (including dark periods) to verify the CCTV that camera recordings—e.g., via motion activation—provide a minimum of: • Recording to capture any motion at least five seconds before and after the detected motion. • Recording all activity, including events during dark periods through the use of infrared CCTV cameras or automatic activation of floodlights in case of any detected activity.	Select	
c) CCTV monitors and recorders must be located in an area that is restricted from unauthorized personnel.	Select		Observe that CCTV monitors and recorders are in a location restricted from unauthorized personnel.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) CCTV cameras must be connected at all times to: • Monitors located in the control room • An alarm system that will generate an alarm if the CCTV is disrupted • An active image-recording device	Select		Observe that CCTV cameras are connected (via a list of known cameras) and active at all times to but not limited to: • Monitors located in the control room • An alarm system that will generate an alarm if the CCTV is disrupted • An active image-recording device	Select	
2.4.6.3 View Requirements					
a) Each camera view must include all activities necessary to provide adequate security coverage. Blind spots must not exist.	Select		Observe a sample of CCTV cameras media to verify camera footage captures all activities to provide adequate security coverage and that there are no blind spots.	Select	
b) The recording must capture sufficient images to identify the individual—e.g., head and shoulder's view—as well as the activity being performed.	Select		Examine sample of recording to verify that it captured sufficient images to identify the individual—e.g., head and shoulder's view—as well as any activity being performed.	Select	
c) Each internal CCTV camera and recording system must be equipped with an automatic recording capability in case of an alarm event.	Select		Examine a sample of video recordings or live video to verify internal CCTV cameras recording system have been equipped with an automatic recording capability when an alarm event occurs.	Select	
2.4.6.4 Retention of Video Recordings					
a) CCTV images must be kept for at least 90 days and must be backed up daily. Both primary and backup copies must exist for a minimum of 90 days.	Select		Examine documentation and a sample of archived video to verify CCTV images are: • Kept for at least 90 days; • Backed up daily; and that • Both primary and backup copies exist for a minimum of 90 days.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) The backup recording or mirror image must be stored in a separate, secure location within the facility and must ensure segregation of duties between the users and administrators of the system. Backups may also be stored in other approved facilities of the card vendor via techniques such as disk mirroring, provided the storage is secure in accordance with these requirements. An approved facility is one evaluated as compliant to these requirements and is participating in the applicable card brand program.	Select		Examine documentation to verify backup recording and storage requirements exist. Observe to verify that backup recordings are stored in a separate, secured location within the facility or stored in other facilities via techniques such as disk mirroring in accordance with the retention policy requirements. Interview personnel to verify that segregation of duties exists between the users and the system administrators.	Select	
2.4.6.5 System Administration					
a) The CCTV system must meet the logical security requirements in Appendix B.	Select		See Appendix B.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.4.7 Security Device Inspections					
2.4.7.1 Semi-Annual Inspections					
a) A semi-annual inspection and testing must be conducted on all security devices and hardware including but not limited to: • Alarm system • Access-control system • Window and door contacts • Glass-break detectors • Emergency door alarms • Passive infrared detectors • Microwave sensors • CCTV monitors • CCTV image recorders	Select		Examine documentation to verify inspections on all security devices and hardware were performed at least semi-annually and include but were not limited to: • Alarm system • Access-control system • Window and door contacts • Glass-break detectors • Emergency door alarms • Passive infrared detectors • Microwave sensors • CCTV monitors • CCTV image recorders	Select	
b) Inspections must be carried out by an external organization qualified to perform such functions.	Select		Examine sample documents to verify security inspections are performed by a qualified external organization.	Select	
c) A copy of the inspection reports must be retained for at least 18 months. This inspection report must list all devices within the Security Systems installed on site, the inspection conducted, results of the test, and evidence of any remediation required.	Select		Examine a sample of documents to verify a copy of the inspection reports is retained for at least 18 months. This inspection report must list all devices within the Security Systems installed on site, the inspection conducted, results of the test, and evidence of any remediation required.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.4.7.2 Battery Testing					
a) Batteries used in local alarms must be tested at least monthly. Batteries must be replaced annually or in accordance with technical specifications provided by the manufacturer or if failing testing.	Select		Examine documentation to verify there is a process in place to test batteries used in local alarms at least monthly and the batteries are replaced annually or in accordance with technical specifications provided by the manufacturer or if failing testing. Examine a sample of logs to verify batteries were tested in local alarms at least monthly and the batteries are replaced annually or in accordance with technical specifications provided by the manufacturer or if failing testing.	Select	
b) Evidence (logs) must be retained for this testing for at least 18 months.	Select		Examine evidence (logs) to verify battery test logs have been retained for at least 18 months.	Select	
2.5 Vendor Security Contingency Plan					
a) The vendor must have a written contingency plan to guarantee that security for card components, products, and data is maintained in case of critical business interruption.	Select		Examine documentation to verify the vendor has a written contingency plan to guarantee that security for card components, products, and data are maintained in case of critical business interruption. Interview personnel to validate they understand the process of the contingency plans to guarantee that security for card components, products, and data are maintained in case of critical business interruption.	Select	
2.6 Decommissioning Plan					
a) The vendor must document its policies and procedures by which assets associated with card production and provisioning activities are secured in the event production activities are terminated.	Select		Examine the vendor's policy and procedures to verify they include that assets associated with card production and provisioning activities are secured in the event production activities are terminated.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) The procedures must identify all data storage, card design materials, cards, card components, physical keys, cryptographic keys, and hardware utilized for production activities that must be secured.	Select		Examine procedures to verify the process identifies and secures all of the following but not limited to: • Data storage • Card design materials • Cards • Card components • Physical keys • Cryptographic keys • Hardware utilized for production activities	Select	
c) The disposition expectations for each identified item must be defined. For example, items may be returned to the owner, transported to an authorized user, or destroyed.	Select		Examine the vendor's policy and procedures to verify they include the disposition expectations for each identified item.	Select	

Section 3: Production Procedures and Audit Trails

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
3.1 Order Limitations					
a) The vendor must only manufacture card products or components in response to a specific, signed order from a representative of the payment brand, issuer, or issuer's authorized agent.	Select		Examine the documented procedures in place when vendor starts production of card products or component runs regarding specific orders. Examine a sample of signed work orders to verify: • The order is signed by representative of the payment brand, issuer, or issuer's authorized agent. • The completed work order matches the corresponding inventory of card products or components.	Select	
b) The vendor must only produce sufficient cards to meet the quantity specified on the order.	Select		Examine documentation to verify procedures are in place to ensure the vendor only produces sufficient cards to meet the quantity specified on the order. Examine a sample of work orders to production run totals to verify procedures are followed.	Select	
c) If a function normally associated with card production or provisioning is subcontracted, the vendor must obtain authorization from the VPA and the issuer.	Select		Interview production management to determine whether any functions associated with card production or provisioning are subcontracted. Examine documentation to identify what card-production/provisioning functions are subcontracted. Examine a sample of completed documentation to verify the vendor received authorization from the VPA and the issuer.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) The information on the reverse of the cards must always identify the vendor that produces the card.	Select		Examine a sample of stock in place and, if a production run is in process, the back of the cards to verify they identify the producing vendor.	Select	
3.2 Card Design Approvals					
3.2.1 Proof Submission					
a) The vendor must follow submission procedures mandated by the appropriate payment brand to receive approval for the card design in order to confirm the design's compliance to the applicable payment brand standards.	Select		Examine the various card-design approval processes to verify that payment brand reviews are appropriately understood and documented by the design team. Examine documentation with vendor to verify that all mandated approvals have been received and are on file to be reviewed upon request.	Select	
3.2.2 Approval Response					
a) The vendor must proceed with card manufacturing only after the submission has been approved.	Select		Interview production management to verify what controls are in place to verify vendor only starts a manufacturing run after approvals have been received. Examine a sample of artwork approval timeframes compared with production runs to verify approval has occurred prior to production.	Select	
3.3 Samples					
3.3.1 Sample Retention					
The vendor must maintain the following for each order:					
a) All records of approval for the job from the applicable payment brand	Select		Examine a sample of order documentation to verify all payment brand job-approval records have been retained.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) A sample of the partially processed product or component	Select		Examine a sample of production run retentions to verify they include partially processed products or components.	Select	
c) A portion of a printed sheet	Select		Examine a sample of production run retentions to verify they each include a portion of a printed sheet.	Select	
d) Documentation indicating the source, quantities, and the distribution of each product received from an external company	Select		Examine a sample of production run retentions to verify they include documentation of each product received from an external company.	Select	
e) All samples visually voided and functionally inoperable	Select		Examine a sample of production run retentions to verify their inoperability and void markings.	Select	
3.3.2 Required Samples					
a) When requested by the payment brand, the vendor must send samples of the finished cards or components from each production run before shipping the finished card products. These samples must be functionally inoperative, and it must be visibly apparent that they are not live cards.	Select		Examine policies/procedures to verify that when requested by the payment brand, the vendor sends samples of the finished cards or components from each production run before shipping the finished card products. Examine a sample of payment brand requests for samples to verify the samples are functionally inoperative and it is visibly apparent that they are not live cards.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
3.4 Origination Materials and Printing Plates – Access and Inventory					
a) The vendor must restrict access to the department or to the dark room where film, plates, or electronic media are produced or stored to authorized personnel.	Select		Examine policies/procedures to verify restricted access exists where film, plates, or electronic media are produced. Observe that restricted access is in place for any room or area that includes the film, plates, or electronic media. Examine a sample of physical access-control logs to verify that authorized personnel are only allowed within these areas.	Select	
b) Transfer of the printing films or printing plates and related responsibility from the pre-press staff to the card-printing staff must be documented in a specific audit sheet to be signed by the two persons involved on this transfer.	Select		Interview personnel to verify that it is required that two persons are involved in the transfer. Examine a sample of audit-sheet documentation regarding the transfer of printing films or printing plates from the pre-press staff to the card-printing staff to verify a two-person rule is in place and is properly documented on the audit sheet.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) The audit sheet must contain at least the following: • Signature of the pre-press staff delivering or collecting the printing films • Job number identification and description of item(s) to be transferred • Signature of the card printing staff collecting or delivering the printing films • Quantity of item(s) transferred (number of films, front and reverse) • Date and time of transfer	Select		Examine a sample of completed audit sheets to verify proper completion to include: • Signature of the pre-press staff delivering or collecting the printing films • Job number identification and description of item(s) to be transferred • Signature of the card printing staff collecting or delivering the printing films • Quantity of item(s) transferred (number of films, front and reverse) • Date and time of transfer	Select	
d) The vendor must inventory the films, printing plates, and duplicates including a record of plates issued from and returned to the printing department.	Select		Interview printing department staff to verify how often, by whom, and what documentation is in place regarding the inventory of films, printing plates, and duplicates issued and returned to the printing department.	Select	
e) The vendor must audit this inventory quarterly.	Select		Examine documentation to verify the vendor conducts audits on a quarterly basis.	Select	
f) The vendor must keep films and printing plates locked under dual control when not in use.	Select		Observe security controls in place for films and printing plates and verify there are dual-control storage requirements when films and printing plates are not in use.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
g) Materials maintained must be limited to the final approved version of the last production run of a particular card type.	Select		Examine what materials are in place within the production area. Observe production staff and verify what procedures are in place to ensure proper levels of materials are maintained on hand for the last production runs of particular card types.	Select	
h) After final use, films and printing plates must be voided or destroyed, and the log of destruction must be signed simultaneously by at least two persons in a specific destruction logbook.	Select		Examine destruction logbook on final use for films and printing plates and verify that two persons are simultaneously signing the destruction log.	Select	
i) All discrepancies must be documented and immediately reported to management. Any loss or theft of materials must be reported to the VPA within 24 hours of discovery.	Select		Examine documentation and verify security controls are in place such that all discrepancies are documented and immediately reported to management. Examine a sample of documentation to verify that any loss or theft is reported to the VPA within 24 hours of discovery.	Select	
3.5 Core Sheets and Partially Finished Cards					
3.5.1 Core Sheets					
3.5.1.1 Access					
a) Access to unbundled core sheets must be restricted at all times.	Select		Observe to verify unbundled core sheets are under restricted access at all times.	Select	
b) Core sheets must be allocated for production use under a materials/production regimen.	Select		Observe the material/production regimen for allocation of core sheets for production runs to verify existence.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
3.5.1.2 Partially or Fully Printed Sheets					
a) When partially or fully printed sheets are stored outside the vault for more than one week, they must be stored in a work-in-progress (WIP) storage room.	Select		Examine documentation to verify that the WIP storage room is utilized for storage longer than one week. Observe storage controls in place by vendor for both partially and fully printed sheets.	Select	
b) Audit or accountability forms for core sheets must provide the following information for every order processed: • Good sheets • Rejected sheets • Set-up sheets • Quality control sheets • Unused core sheets	Select		Examine a sample of orders processed and validate that audit or accountability forms for core sheets contain: • Good sheets • Rejected sheets • Set-up sheets • Quality control sheets • Unused core sheets	Select	
c) Sheets printed with the payment system brand or issuer design must not be used as set-up sheets unless clearly marked void over the payment-system brand/issuer design.	Select		Examine set-up sheet system used by vendor to verify it is in compliance with this section, restricting sheets unless clearly marked void over the payment-system brand/issuer design.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Once core sheets have been printed with a payment system brand mark, company logo, standard product design features, or an issuer design bearing the appropriate windows for the application of the logo, the printed sheet must become a part of the audit and accountability process. An accurate sheet count must be made and recorded in the initial count production control system.	Select		Examine the audit and accountability process in place to verify that it includes printed core sheets that have been printed with a payment system brand mark, company logo, standard product design features, or an issuer design bearing the appropriate windows for the application of the logo. Observe production control system to verify that there is an accurate sheet count recorded.	Select	
e) If either side of a core sheet has been printed with what could be mistaken for payment system brand marks, card images or issuer designs, it must not be used as a set-up sheet on subsequent jobs, but instead be destroyed with other printed sheets that are unusable.	Select		Examine the security/documentation controls in place to verify that core sheets are not reused and are destroyed with other printed sheets that are unusable.	Select	
3.5.2 Partially Finished Cards					
a) When partially finished cards—e.g., pre-personalized—are temporarily stored outside the vault, they must be stored in a secure, locked container in the HSA under dual control. Cards shall not be stored outside of the vault except as WIP while the facility is in operation.	Select		Observe to verify cards stored outside the vault are stored in secure, locked containers in the HSA under dual controls. Examine procedures for use of the WIP area to verify that partially finished cards are stored properly in the HSA.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
3.6 Ordering Proprietary Components					
a) The vendor must obtain proprietary components—e.g., signature panels, holographic materials, special dies—only from authorized suppliers.	Select		Examine documentation to determine what supplier the vendor is receiving proprietary components from, and whether they are authorized suppliers.	Select	
b) The vendor must provide the supplier with both the street and mailing addresses of the vendor's facility, as well as names and signatures of the vendor's authorized representatives that will be ordering components.	Select		Examine sample orders to verify that the vendor provided the supplier with both the street and mailing addresses of the vendor's facility, as well as names and signatures of the vendor's authorized representatives that are allowed to order components.	Select	
3.7 Audit Controls – Production					
3.7.1 General *An order may be separated into multiple jobs, which may be split into different batches.*					
a) The vendor must apply audit controls to each job/batch received, whereby an effective audit trail is established for each production step.	Select		Examine policies/procedures to verify audit controls and an audit trail are in place for each job/batch and production step. Examine a complete job run to verify procedures are followed.	Select	
b) All card products and components—both good and rejected, including samples—must be counted and reconciled prior to any transfer of responsibility.	Select		Observe a sample production job/run and validate that all card products and components—both good and rejected, including samples—are counted and reconciled prior to any transfer of responsibility.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) An effective audit trail is comprised of a series of audit logs that must contain but are not limited to the following information: • Description of the component or card product(s) being transferred • Name and signature of the individual releasing the component or card product(s) • Name and signature of the individual receiving the component or card product(s) • Number of components or card products transferred • Number of components used • Number returned to vault or WIP storage • Number rejected or damaged • Number to be destroyed • Date and time of transfer • Name and signature of supervisor • Signatures of persons inventorying components	Select		Examine a sample of audit logs used during a production runs to verify that they contain: • Description of the component or card product(s) being transferred • Name and signature of the individual releasing the component or card product(s) • Name and signature of the individual receiving the component or card product(s) • Number of components or card products transferred • Number of components used • Number returned to vault or WIP storage • Number rejected or damaged • Number to be destroyed • Date and time of transfer • Name and signature of supervisor • Signatures of persons inventorying components	Select	
d) At the end of each production step, two persons must simultaneously count the card components and related components and sign the audit control documents.	Select		Observe production run to verify the security controls in place include a dual count of cards after each step of the production run.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) Audit control documents must be completed and reconciled at the end of each production step and when changing shifts. They must be attached to or included with the work in process.	Select		Examine a sample of audit control documentation to verify it is completed and reconciled at the end of each production step and when changing shifts. Observe a sample production run to witness reconciliation of audit-control documents and that they are attached to or included with the work in process.	Select	
f) The vendor must be able to confirm that the material, including waste, used in the manufacture of card products matches the amount of material indicated in the inventory control logs. The audit trail must be kept for at least 24 months. This information must be available for inspection.	Select		Examine a sample of documentation to verify: • Accurate and complete inventory of materials is completed. • Audit trails of the past 24 months are maintained by the vendor and available for inspection.	Select	
g) The vendor must maintain an original or a copy of both the purchase order and invoice for procured materials to serve as an audit control log.	Select		Examine documentation to verify that originals or copies of both the purchase order and invoice for procured materials are being maintained.	Select	
h) The vendor must conduct inventory counts to ensure that invoices are correct and that they comply with the purchase order.	Select		Examine a sample of inventory counts to verify accuracy of the invoices related to the purchase orders.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
i) During the processing of card products (encoding, embossing, and personalizing), only the minimum number of boxes or sleeves required may be opened at one time. The contents of partially used boxes or sleeves must be verified against the inventory control documents. Before additional boxes or sleeves are opened, any partially used boxes or sleeves must be fully used. The number of cards in partially used boxes and sleeves must be verified, and each box or sleeve must be rewrapped and sealed before being stored in the vault.	Select		Observe the processing of card products to verify that: • The process includes only the minimum number of boxes or sleeves required be opened at one time. • The contents of partially used boxes or sleeves are verified against the inventory control documents. • Any partially used boxes or sleeves are fully used before additional boxes or sleeves are opened • The number of cards in partially used boxes and sleeves are verified. • Each box or sleeve is rewrapped and sealed before being stored in the vault	Select	
j) Card components must be received and initially inventoried against the supplier's shipping documentation under dual control.	Select		Observe or review a sample of card components received to verify they are inventoried under dual control against the supplier's shipping documentation for accuracy.	Select	
k) A physical count of the boxes containing the card components must be completed at delivery to confirm accuracy of the shipper's documents.	Select		Observe or review a delivery sample to verify that there is a physical count of the boxes containing the card components and that it matches the shipper's documents.	Select	
l) An authorized card production staff member must sign for all component stock received by the vendor. The person delivering the stock must also sign the transfer document.	Select		Examine a sample of transfer documentation to validate: • An authorized card production staff member signs for the component stock received by the vendor. • The person delivering the stock also signs the transfer documentation.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
m) Card components must be transferred to the vault immediately.	Select		Observe or review the process in place to verify immediate storage of card components into the vault.	Select	
n) The exact quantity of card components must be counted and registered in the inventory book before vault storage.	Select		Examine the inventory book to verify accurate counts of card components are being maintained by vendor.	Select	
o) In the case of holograms, the hologram identification number to be registered as initial stock inventory must be the first good hologram image on the reel (this may be different from the number of holograms indicated in the delivery note).	Select		Examine the inventory book to validate that: • The hologram identification number is being registered and listed. • If new reels are present, the first hologram number has been listed and matches the reel stored in the vault.	Select	
p) The card component inventory log must include but is not limited to: • The reel number or equivalent control that provides unique identification. • Date of usage • Customer job number • Number of images or modules placed on cards • Number of rejected images or modules from header and trailer scrap • Number of and reason for rejected images	Select		Examine the card component inventory log to verify that it includes at least: • The reel number or equivalent control that provides unique identification • Date of usage • Customer job number • Number of images or modules placed on cards • Number of rejected images or modules from header and trailer scrap • Number of and reason for rejected images	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
q) Card components must be removed from the machine and locked within a secure container when not in use.	Select		Examine policies/procedures to verify that card components are removed from the machine and locked within a secure container when not in use. Observe and verify that card components are removed from the machine and locked within a secure container when not in use.	Select	
r) Card components must be returned to the vault during non-production hours.	Select		Examine policies/procedures to verify that card components are returned to the vault during non-production hours. Observe and verify that card components are returned to the vault during non-production hours.	Select	
s) Rejected card components awaiting return for credits must be maintained under dual control.	Select		Observe and verify that rejected cards awaiting return for credits are maintained under dual control.	Select	
3.7.1.1 Log Modifications					
a) If modifications are to be made to the audit log, a single line must be made through the original figure.	Select		Examine a sample of audit logs to verify that all modifications to the audit logs are being made in the authorized and designated manner.	Select	
b) The updated figure and the initials of the card production staff member making the changes must be placed adjacent to the incorrect figure.	Select		Examine a sample of logs to verify that all modifications to the audit log are being made in the authorized and designated manner.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
3.7.1.2 Log Review					
a) All logs must be reviewed and validated for completeness at least weekly by an individual who is not involved in the direct operation of the equipment.	Select		Examine a sample of logs to verify that they are being reviewed and validated for accuracy at least weekly by an individual not involved in the direct operation of the equipment.	Select	
b) The review must be signed and dated as part of the log.	Select		Examine a sample of logs and verify that it is signed and dated as required and by the proper individual.	Select	
c) All logs referenced in this document must be retained for a minimum of two years unless otherwise stated.	Select		Examine a sample of logs and verify that logs are retained for a minimum of two years unless required otherwise.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
3.7.2 Vault Audit Controls					
a) A log is required for items moved in or out of the vault and must contain: • Name of the card issuer • Type of card • Number of cards originally placed in inventory • Reason for transaction—e.g., job number • Number of cards removed from inventory • Number of cards returned to inventory • Balance remaining in the vault • Date and time of activity • Names and signatures of the card production staff who handled the transaction	Select		Examine the vault log to verify that at a minimum it contains: • Name of the card issuer • Type of card • Number of cards originally placed in inventory • Reason for transaction—e.g., job number • Number of cards removed from inventory • Number of cards returned to inventory • Balance remaining in the vault • Date and time of activity • Names and signatures of the card production staff who handled the transaction Observe items being logged in and out of the vault to verify that proper documentation is accurately completed.	Select	
b) Two card production staff must create a written, physical inventory of card and card components monthly.	Select		Examine a sample of monthly inventory to verify that an inventory of cards and card components is being completed on a monthly basis by two card production staff.	Select	
c) Card production staff performing the inventory must not have knowledge of the results of the last inventory.	Select		Interview personnel to verify controls are in place to restrict knowledge of any previous inventory.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) At a minimum, the monthly inventory log must contain: • Date of the review • Name of the card issuer • Type of card • Number of cards indicated in the inventory • Number of cards counted • Name and signature of both card production staff who conducted the inventory	Select		Examine a sample of monthly inventory logs and verify that they contain at a minimum: • Date of the review • Name of the card issuer • Type of card • Number of cards indicated in the inventory • Number of cards counted • Name and signature of both card production staff who conducted the inventory	Select	
e) Any discrepancies must be reported to management and resolved.	Select		Examine procedures related to discrepancies to verify they are reported to management for resolution.	Select	
3.7.3 Personalization Audit Controls					
a) During personalization, cards and cardholder data must be handled in a secure manner to ensure accountability.	Select		Observe personalization process and validate controls are in place that ensure a secure method of handling and accountability.	Select	
b) An audit control log must be maintained for each job/sub-job (batch) designating: • Job number • Issuer name • Card type	Select		Examine a sample of audit control logs to verify they include job number, issuer name, and card type.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) For each personalization batch, include: • Initial card procurement (beginning balance) • Card re-makes • Cards returned to inventory • Spoiled cards • Sample/test cards • Machine/operation identification • Date and time of reconciliation • Operator name and signature • Name and signature of an individual other than the operator, who is responsible for verifying the count	Select		Examine a sample of a personalization batches and verify they include: • Initial card procurement (beginning balance) • Card re-makes • Cards returned to inventory • Spoiled cards • Sample/test cards • Machine/operation identification • Date and time of reconciliation • Operator name and signature • Name and signature of an individual other than the operator, who is responsible for verifying the count	Select	
d) For accounts/envelopes, include: • Number of accounts • Number of card carriers printed • Number of carriers wasted • Number of envelopes that contain cards • Operator name and signature • Name and signature of an individual other than the operator, who is responsible for verifying the count	Select		Examine a sample of a personalization batches and verify they include: • Number of accounts • Number of card carriers printed • Number of carriers wasted • Number of envelopes that contain cards • Operator name and signature • Name and signature of an individual other than the operator, who is responsible for verifying the count	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) For PIN mailers, include: • Number of mailers to be printed • Number of mailers actually printed • Wasted mailers that have been printed • Number of mailers transferred to the mailing area/room • Operator name and signature • Name and signature of an individual other than the operator, who is responsible for verifying the count	Select		Examine a sample of a personalization batches and verify they include: • Number of mailers to be printed • Number of mailers actually printed • Wasted mailers that have been printed • Number of mailers transferred to the mailing area/room • Operator name and signature • Name and signature of an individual other than the operator, who is responsible for verifying the count	Select	
3.8 Production Equipment and Card Components					
3.8.1 Personalization Equipment					
a) The vendor must maintain a log of personalization equipment failures, including at a minimum: • Operator name • Supervisor name and signature • Machine description/number • Job number • Date • Time • Cause of the malfunction	Select		Examine a sample of logs for personalization equipment failures to verify they include at a minimum: • Operator name • Supervisor name and signature • Machine description/number • Job number • Date • Time • Cause of the malfunction	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
3.8.2 Indent Printing Module					
The vendor must:					
a) Use payment system proprietary typefaces within indent-printing modules only for payment system cards	Select		Examine cards to verify that authorized payment system proprietary typefaces with indent-printing modules are used only for payment system cards	Select	
b) Destroy, under dual control, payment system proprietary typefaces within indent-printing modules that are no longer to be used.	Select		Examine polices/procedures to verify they exist to destroy, under dual control, payment system proprietary typefaces within indent-printing modules that are no longer to be used.	Select	
c) Record the destruction of modules.	Select		Examine a sample of documentation to verify that a record of this destruction is maintained.	Select	
3.8.3 Tipping Foil					
a) The vendor must shred completely used tipping foil reels containing cardholder data as follows: • In-house—i.e., within the facility, • Under dual control, and • The destruction can occur as frequently as the vendor deems necessary but—in all cases—weekly at a minimum. The vendor must maintain proper controls over these materials at all times prior to destruction, and the destruction must occur within the HSA.	Select		Examine policies and procedures for handling completely used tipping foil reels to verify they require the destruction of tipping foil reels containing cardholder data, with dual-control handling requirements, in-house, within the HSA. Examine a sample of destruction logs to verify that destruction is occurring at a minimum on a weekly basis, in house, under dual control, and within the HSA.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Used tipping foil must be removed from the machine during non-production hours.	Select		Examine documentation to verify it requires that tipping foil be removed during non-production hours. Observe procedure of removal of tipping foil to verify it is followed by vendor.	Select	
c) Prior to destruction—e.g., shredding—the foil must be stored within the HSA under dual access control.	Select		Observe security controls are in place to store tipping foil under dual control within the HSA prior to shredding.	Select	
d) When destroyed the results must be non-readable and non-recoverable.	Select		Examine a sample of waste to verify proper shredding and destruction of materials is being followed.	Select	
e) An inventory of the number of used reels must be maintained and reconciled with the number of reels shredded.	Select		Examine a sample of inventory logs to verify the number of used reels is maintained and reconciled with the number of reels shredded.	Select	
f) A log, pre-numbered and bound, of the destruction of the foil must be maintained and include at a minimum: • Number of reels—partial or full. All used foil must be accounted for and destroyed. • Date and time • Written initials of both individuals who witnessed the destruction	Select		Examine documentation to verify logs are maintained for the destruction of the foil and they contains at a minimum: • Number of reels—partial or full. All used foil must be accounted for and destroyed. • Date and time • Written initials of both individuals who witnessed the destruction	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
3.8.4 Thermal Transfer Foil ***Note:*** *The following requirements apply* ***ONLY*** *to thermal transfer foil reels/cassettes used within a production environment to apply cardholder data—e.g., those used in personalization or PIN printing processes.*					
a) Prior to use, thermal transfer foil reels/cassettes must be marked with a unique, tamper-evident security identifier.	Select		Examine documented processes and procedures for the handling of thermal transfer foil reels/cassettes and tracking thermal.	Select	
b) Records must be maintained pertaining to the reel/cassette for tracking purposes from first use through destruction.	Select		Examine documented processes and procedures for the tracking thermal transfer foil reels/ cassettes.	Select	
c) The vendor must shred completely used thermal transfer foil reels/cassettes containing cardholder data as follows: • In-house—i.e., within the facility, • Under dual control, and • The destruction can occur as frequently as the vendor deems necessary but—in all cases—weekly at a minimum. The vendor must maintain proper controls over these materials at all times prior to destruction, and the destruction must occur within the HSA.	Select		Examine policies and procedures for handling completely used thermal transfer foil reels and/or cassettes to verify they require the destruction of thermal transfer foil reels/cassettes containing cardholder data, with dual-control handling requirements, in-house, within the HSA. Examine a sample of destruction logs to verify that destruction is occurring at a minimum on a weekly basis, in house, under dual control, and within the HSA.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Thermal transfer foil reels and/or cassettes that are not yet at the end of their usable life must be removed from thermal transfer units during non-working hours and managed as per requirement e) below. .	Select		Examine documentation to verify it requires that thermal transfer foil reels/cassettes are required to be removed during non-production hours. Examine a sample of audit trails related to the removal of thermal transfer foil reels and/or cassettes to verify that they are stored securely during non-working hours and are placed back into the thermal transfer unit during the next working period or are marked for destruction.	Select	
e) Thermal transfer foils must be removed from the machine under dual control. These must then be immediately: • Destroyed, or • Stored in manner such that the contents are not viewable and moved to a secure location inside of the HSA pending re-installation into a thermal transfer unit during the next working period, or • Stored in manner such that the contents are not viewable and moved to a secure location inside of the HSA pending destruction at a later time.	Select		Examine documentation to verify it requires that thermal transfer foils are removed for only the following reasons: • Immediate destruction • Stored in manner such that the contents are not viewable and moved to a secure location inside of the HSA pending re-installation into a thermal transfer unit during the next working period. • Stored in manner such that the contents are not viewable and moved to a secure location inside of the HSA pending destruction at a later time. Observe procedure of removal of tipping foil to verify the process.	Select	
f) Prior to destruction—e.g., shredding—the foil must be stored within the HSA under dual access control.	Select		Observe security controls are in place to store thermal transfer foil under dual control within the HSA prior to destruction.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
g) When destroyed the results must be non-readable and non-recoverable.	Select		Examine a sample of waste to verify proper destruction of materials is being followed.	Select	
h) An inventory of the number of used reels and/or cassettes must be maintained and reconciled with the number of used reels and/or cassettes destroyed.	Select		Examine a sample of inventory logs to verify the number of used reels and/or cassettes is maintained and reconciled with the number of reels and/or cassettes destroyed.	Select	
i) A log, pre-numbered and bound, of the destruction of the thermal transfer foil must be maintained and include at a minimum: • Number of reels and/or cassettes—partial or full. All used foil must be accounted for and destroyed. • Date and time • Written initials of both individuals who witnessed the destruction.	Select		Examine documentation to verify logs are maintained for the destruction of the foil and they contain at a minimum: • Number of reels and/or cassettes—partial or full. All used foil must be accounted for and destroyed. • Date and time • Written initials of both individuals who witnessed the destruction.	Select	
3.9 Returned Cards/PIN Mailers					
3.9.1 Receipt					
The vendor must:					
a) Maintain a log of all returned cards and PIN mailers.	Select		Examine polices/procedures to verify that a log is required for all returned cards and PIN mailers. Examine a sample of logs to verify procedures are followed to maintain a log of all returned cards and PIN mailers.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Store all returned cards in a secure container under dual control.	Select		Observe that a secure container is utilized to store all returned cards under dual control.	Select	
c) Either send returned cards to the issuer or destroy them as defined in Section 3.10, "Destruction and Audit Procedures."	Select		Examine polices/procedures to verify returned cards are either sent to the issuer or destroyed according to "Destruction and Audit Procedures." Interview personnel to verify procedures are known and followed.	Select	
d) Destroy returned PIN mailers as defined in Section 3.10 below.	Select		Observe the method of destruction of PIN mailers to verify it is in accordance with "Destruction and Audit Procedures."	Select	
e) Place cards collected by the vendor from a third-party location in a secure container under dual control before leaving the third-party location.	Select		Interview personnel to identify third-party providers with access to PIN mailers. Observe that the method and container utilized by the vendor for the collection of cards from a third-party location are handled under dual controls.	Select	
3.9.2 Accountability					
a) The opening of the container and an accounting of the number of envelopes/cards must take place under dual control immediately upon receipt at the personalization facility.	Select		Examine documentation to verify the opening of the container and an accounting of the number of envelopes/cards takes place under dual control immediately upon receipt at the personalization facility.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) The log must contain at a minimum: • Date of receipt, • Written initials of both card production staff counting the cards, • The issuer name, and • For each package: – The card type – The number of envelopes – The number of cards	Select		Examine a sample of logs to verify they contain at a minimum: • Date of receipt, • Written initials of both card production staff counting the cards, • The issuer name, and • For each package: – The card type – The number of envelopes – The number of cards	Select	
3.10 Destruction and Audit Procedures					
a) All waste components must be counted before being destroyed in-house—i.e., within the facility—and under dual control. A record of destruction by reel number and item count must be maintained for 24 months.	Select		Examine a sample of destruction logs to verify that it is maintained and includes the reel number and item count. Verify that the log has been maintained for 24 months. Observe in-house destruction process to verify all waste components are counted before being destroyed in-house and under dual control.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) The following materials must be destroyed on a batch basis by shredding or grinding such that the resulting material cannot be reconstructed: • Spoiled or waste card products • Holographic materials • Signature panels • Sample and test cards • Any other sensitive card component material or courier material related to any phase of the card production and personalization process	Select		Observe destruction process to verify it includes all of the listed materials and that the destruction is sufficient to ensure that materials cannot be reconstructed. This includes: • Spoiled or waste card products • Holographic materials • Signature panels • Sample and test cards • Any other sensitive card component material or courier material related to any phase of the card production and personalization process	Select	
c) Destruction of chips, modules, or chip cards must ensure that the chip itself is destroyed.	Select		Observe destruction process to verify that destruction of chips, modules, or chip cards ensures that the chip itself is destroyed.	Select	
d) An exception to the above is that holograms failing the hot-stamping process must be rendered unusable at the machine.	Select		Observe that holograms failing the hot-stamping process are rendered unusable at the machine. If destruction cannot be observed, examine the documented security controls in place.	Select	
e) The material waiting to be destroyed must be stored securely, under dual control.	Select		Observe that materials to be destroyed are stored in a secure location under dual control.	Select	
f) Destruction must be carried out in a separate room as defined in Section 3.10	Select		Observe destruction is carried out under dual control in a separate room that has restricted access and is under CCTV coverage.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
g) Proper destruction requires the following: • Individuals destroying the materials must ensure that they are rendered unusable and unreadable. • Two card production staff must simultaneously count and shred the material. • Before leaving the room, both card production staff must ensure that all material has been destroyed and not displaced in the machinery or equipment. • Card production staff must prepare, sign, and maintain a destruction document. • Once the destruction process is initiated, the process must not be interrupted.	Select		Examine destruction process by reviewing the destruction logbook, destroyed materials in a waste bin, and CCTV coverage of the destruction occurring to verify it requires the following: • Individuals destroying the materials ensure they are rendered unusable and unreadable. • Two card production staff simultaneously count and shred the material. • Before leaving the room, both card production staff ensure that all material has been destroyed and not displaced in the machinery or equipment. • Card production staff prepare, sign, and maintain a destruction document. • The destruction process, once initiated, is not interrupted.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
h) An audit log must be created which, at a minimum, contains the following information: • Signatures of the individuals presenting waste material • Description of item(s) to be destroyed (such as product type, job number, and issuer name) • Signatures of the persons observing or carrying out the waste destruction • Quantity of item(s) to be destroyed • Date and time of destruction	Select		Examine a sample of audit logs to verify that, at a minimum, it contains the following information: • Signatures of the individuals presenting waste material • Description of item(s) to be destroyed (such as product type, job number, and issuer name) • Signatures of the persons observing or carrying out the waste destruction • Quantity of item(s) to be destroyed • Date and time of destruction	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
3.11 Lost and Stolen Reports					
a) The vendor must immediately (within 24 hours) report to the VPA, the issuer, and appropriate law-enforcement agencies any loss or theft of card products or components.	Select		Examine policies/procedures to verify that reporting of loss or theft of card products is: a) Handled immediately (within 24 hours). b) Reported to the VPA, the issuer, and appropriate law-enforcement agencies. Examine a sample of notifications sent to the VPA/issuer for any loss or theft of card products or components reported within the past 24 months to verify adherence to procedures.	Select	
b) The report must include but is not limited to: • The complete and detailed chronology of events • Cardholder account numbers • Personal identification numbers (PINs) • Printing plates • Encoding or personalizing equipment • Signature panels • Holograms • Electronic storage media • Chips or any carrier containing card components • The vendor's technical specification manual	Select		Examine a sample of lost-or-stolen report logs to verify the information includes, but is not limited to: • The complete and detailed chronology of events • Cardholder account numbers • Personal identification numbers (PINs) • Printing plates • Encoding or personalizing equipment • Signature panels • Holograms • Electronic storage media • Chips or any carrier containing card components • The vendor's technical specification manual	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) The written communication must contain information regarding the loss or theft, including but not limited to the following: • Name of issuer • Type of card or product • Name and address of the vendor • Identification of source of cards • Description of the incident including: • Date and time of incident • Details of companies and persons involved • Details of the investigation • Name, e-mail address, and telephone number of the person reporting the loss or theft • Name, e-mail address, and telephone number of the person to contact for additional information (if different from the person reporting the incident) Additional or follow-up reports should be forwarded to the VPA, issuer, and the appropriate law-enforcement agencies as activities or actions occur.	Select		Examine a sample of VPA/Issuer notifications to verify that it includes, at a minimum: • Name of issuer • Type of card or product • Name and address of the vendor • Identification of source of cards • Description of the incident including: – Date and time of incident – Details of companies and persons involved – Details of the investigation – Name, e-mail address, and telephone number of the person reporting the loss or theft – Name, e-mail address, and telephone number of the person to contact for additional information (if different from the person reporting the incident) Examine a sample of notifications to verify that reports of follow-up actions involving loss or theft have been forwarded to the VPA, issuer, and appropriate law-enforcement agencies.	Select	

Section 4: Packaging and Delivery Requirements

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
4.1 Vendor Responsibility and Shipment Documentation					
a) If the vendor has subcontracted the manufacturing process to another approved vendor, the subcontracting vendor must assume responsibility during transportation for the loss/theft/misplacement of the cards and/or materials.	Select		Examine a sample of the vendor's agreements with subcontracting manufacturing vendors to verify that they contain language stating that the subcontracting vendor assumes responsibility during transportation for the loss/theft/misplacement of the cards and/or materials.	Select	
b) These shipments must be documented to include at least the following information: • Name of the issuer • Destination • Date of shipment • Name of courier • Manifest number	Select		Examine a sample of shipment labels to verify they contain the minimum information required: • Name of the issuer • Destination • Date of shipment • Name of courier • Manifest number	Select	
c) The vendor must report to the VPA when a shipment request is not in compliance with these shipping requirements and must withhold shipment until instruction from VPA is received.	Select		Examine policies and procedures to verify that a process is in place to report to the VPA when a shipment request is not in compliance with Requirements 5a) and b) and that shipment is withheld until instruction from VPA is received.	Select	
4.2 Preparation					
The vendor must:					
a) Count all card products under dual control.	Select		Observe an example (live or recorded previous count if live not available) of a count to verify that counts of all card products are performed under dual control.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Complete audit-control documentation before the cards are packaged.	Select		Observe an example (live or recorded previous count if live not available) to verify that audit-control documentation is completed before the cards are packaged.	Select	
c) Reconcile all counts with amount to be shipped prior to packaging.	Select		Observe an example (live or recorded previous count if live not available) to verify that all counts of card products to be shipped prior to packaging are reconciled.	Select	
d) Immediately seal containers for final packaging.	Select		Observe an example (live or recorded previous count if live not available) to verify that the containers for the card products to be shipped are immediately sealed for final packaging.	Select	
e) Immediately investigate and resolve discrepancies.	Select		Examine policies and procedures to verify that all discrepancies in the preparation process are immediately investigated and resolved before packaging.	Select	
4.3 Packaging					
The vendor must:					
a) Use materials for the packaging of cards and components with sufficient strength to minimize breakage during shipment.	Select		Observe an example to verify the use of packaging materials of sufficient strength to minimize breakage during shipment.	Select	
b) Use packaging that does not indicate or imply the nature of the contents.	Select		Observe an example to verify the packaging does not indicate or imply the nature of the contents.	Select	
c) Use reinforced, tamper-evident, color-coded tape that is not in common use to band the containers.	Select		Observe an example to verify the tape used for sealing the packaging is reinforced, tamper-evident, unique, and color-coded.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Use containers that are uniquely numbered and labeled.	Select		Observe an example to verify the containers are uniquely numbered and labeled.	Select	
e) Record the number of containers and cards on a packing list.	Select		Observe an example to verify that the number of containers and cards on a packing list are recorded.	Select	
f) Package all un-enveloped cards shipped in bulk in double-walled cartons that must have a bursting strength capable of handling a minimum of 250 PSI, 1724 kPa or 17.6 kg/cm^2.	Select		Examine evidence to verify that the packaging used for un-enveloped cards shipped in bulk are in double-walled cartons that have a bursting strength capable of handling a minimum 250 PSI, 1724 kPa or 17.6 kg/cm^2.	Select	
g) Each carton within a shipment must have the number of cards it contains printed on the carton, and the batch/shipment details of which it forms part.	Select		Observe an example to verify that each carton that contains shipments of cards has: • The number of cards contained therein printed on the carton. • The batch/shipment details of which it forms part.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
4.4 Storage before Shipment					
a) Card products awaiting shipment must be maintained under dual control in a vault when the facility is closed or in an HSA, where access is limited to authorized personnel only, when the facility is operational.	Select		Interview shipping personnel to verify that polices/procedures exist for card products awaiting shipment to be stored in an access-controlled area within the HSA or the vault when the facility is closed. Observe the area where cards are stored for shipment to verify that: • They are stored in the HSA, and • Access is limited to authorized personnel. Observe CCTV for an example to verify that when the facility is closed cards awaiting shipment are stored in the vault under dual control.	Select	
b) Packages that are opened or damaged must not be shipped until the contents are recounted and repackaged.	Select		Examine policies/procedures for handling opened or damaged packages to verify they are not shipped until the contents are recounted and repackaged. Observe CCTV for an example to verify that opened or damaged packages are not shipped until the contents are recounted and repackaged under dual control.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
4.5 Delivery					
a) Except for cards delivered directly to individual cardholders, all shipments must be to the issuer, an approved vendor, or (with written issuer and VPA consent) to another destination.	Select		Interview personnel to verify that except for cards delivered directly to individual cardholders, all shipments are to the issuer, an approved vendor, or (with written issuer and VPA consent) to another destination. Examine a sample of shipping logs to verify that except for cards delivered directly to individual cardholders, all shipments are to the issuer, an approved vendor, or (with written issuer and VPA consent) to another destination.	Select	
b) Sending payment cards to a destination other than the cardholder, issuer, or an approved vendor requires issuer authorization and VPA approval. A copy of the issuer's authorization letter—i.e., release of liability signed by an issuer corporate officer—must be provided to the VPA when requesting shipping approval from the VPA. The issuer authorization letter must be signed by a corporate officer indicating the destination of the card shipment and acceptance of liability for any loss, theft, or misplacement of cards during transport.	Select		Interview personnel to verify that sending payment cards to a destination other than the cardholder, issuer or an approved vendor requires issuer authorization and VPA approval. Examine documentation for a sample of shipments of payments cards to a destination other than the cardholder, issuer or an approved vendor to verify that: • An issuer authorization letter exists, and • The letter is signed by a corporate officer indicating the destination of the card shipment and acceptance of liability for any loss, theft, or misplacement of cards during transport, and A copy of the shipping approval from the VPA is on file, if the VPA requires it.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) PIN mailers and cards must be dispatched separately, a minimum of two days apart. The only exception is for the distribution of non-personalized prepaid cards, which may be distributed the same day in accordance with Section 5 of this document.	Select		Interview personnel to identify the path each order takes in the personalization and PIN printing process, including identifying the associated data files and electronic logs of each step of the process for any given order. Interview personnel to identify logs associated with the physical movement of product associated with order numbers. Examine policies and procedures to verify that PIN mailers and cards are dispatched separately and at least two days apart except for non-personalized prepaid cards. Observe electronic and physical logs for a sample of orders for each step of the personalization and PIN printing process to verify the information gathered above.	Select	
d) Electronic distribution of PINs may occur on the same day in accordance with the Logical Security Requirements – Section 9.			*Informational only – Addressed under Logical Security Review.*		

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
4.5.1 Card Mailing					
a) Personalized cards must be placed in envelopes that do not have any visual or implied indication there is a card inside. The envelopes may utilize similar marking as all other issuer and/or co-brand communications. This applies whether conveyed by courier or not. A return address is required.	Select		Observe a sample of envelopes containing personalized cards to be mailed to verify that they do not have any visual or implied indication there is a card inside, and the envelopes have a return address.	Select	
b) After applying postage and sealing, the envelopes must be counted under dual control and placed in locked or sealed containers or bags.	Select		Observe an example (live or recorded previous count if live not available) to verify that envelopes to be mailed are counted under dual control and placed in locked or sealed containers or bags after being sealed and applied with postage.	Select	
c) The loading and transfer process must use the shipping and delivery areas as defined in Section 2.3.6, “Other Areas.”	Select		Observe the loading and transfer process to verify that they are conducted in the shipping and delivery areas as defined in Section 2.3.6, “Other Areas.”	Select	
d) Packages containing card envelopments must be sent to the postal service, presort facility, or issuer.	Select		Examine a sample of packages containing card envelopments to verify they are only sent to the postal service, a presort facility, or issuer.	Select	
e) Transfer to the mail facility by vendor-owned or commercially contracted vehicles must occur by one of the secure transport options meeting the following security controls:					
i. The card transport vehicle must not carry any signs or logos indicating it belongs to a card vendor.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language if outsourced, to verify that any vehicle used for deliveries does not carry any signs or logos indicating it belongs to a card vendor.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
ii. The card transport vehicle must be equipped with a communication device that enables two-way contact with the security controller.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify the card transport vehicle is equipped with a communication device that enables two-way contact with the security controller.	Select	
iii. The contents are secured with tamper-evident straps and checked upon delivery.	Select		Examine vendor policies and procedures to verify the contents are secured with tamper-evident straps and checked upon delivery.	Select	
iv. The vehicle is loaded using dual control and locked during transport.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify the card transport vehicle is loaded using dual control and locked during transport.	Select	
v. Vehicle drivers do not have a key or access to contents.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify the card transport vehicle drivers do not have a key or access to contents.	Select	
vi. Two persons are in the vehicle equipped with a device to communicate with the security control room.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify that two persons are in the card transport vehicle with a device to communicate with the security control room.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
vii. The transport between the vendor location and the destination location must be non-stop whenever possible—i.e., non-emergency stops are not permitted.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify that all transports between the vendor location and the destination location are required to be nonstop whenever possible.	Select	
f) A receipt of delivery must be signed by a representative of the receiving organization, and a signed copy of the receipt must be retained by the vendor.	Select		Examine policies and procedures to verify that they require that a receipt of delivery be signed by the representative of the receiving organization and that a signed copy of the receipt be retained by the vendor. Observe an example (live or recorded previous if live not available) to verify that a receipt of delivery is signed by a representative of the receiving organization, and a signed copy of the receipt is retained by the vendor.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
4.5.1.1 Emergency Cards and PINs					
a) Vendors may include the PIN with the mailing of emergency cards only with written approval from the issuer. Card vendors will be responsible for ensuring an appropriate officer of the card issuer has signed the authorization letter and that a copy of the letter is maintained in their files. The authorization letter must acknowledge that the issuer accepts all risk inherent in shipping cards and PINs together and must confirm that the expedited process is permitted only for emergency card replacement orders. Issuers may provide the card vendor with a standing letter of instruction and do not need to approve each emergency card replacement order.	Select		Examine policies and procedures to verify that: • The inclusion of the PIN with the mailing of emergency cards is allowed only with written approval from the issuer; • An appropriate officer of the card issuer is required to sign the authorization letter for emergency card replacement orders; • Such letters contain acknowledgment from the issuer accepting all risk inherent in shipping cards and PINs together; • Such letters confirm that the expedited process is permitted only for emergency card replacement orders; and • The issuer may issue a standing letter of instruction and does not need to approve each emergency card replacement order.	Select	
4.5.1.2 Mail Trays (Awaiting Delivery)					
a) Mail must be in tamper-evident packaging and/or strapped to prevent the removal of envelopes or placed in locked carts.	Select		Examine a sample of mail awaiting delivery to verify that it is in tamper-evident packaging and/or strapped to prevent the removal of envelopes or placed in locked carts.	Select	
b) The packaging must be the same as that used by the local mail service.	Select		Examine a sample of mail trays to verify that their packaging is the same as that used by the local mail service.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Labels on packages sent to the postal service or presort facility must not indicate the name of the vendor or issuer.	Select		Examine a sample of packages intended for the postal service or a presort facility to verify that their package labeling does not indicate the name of the vendor or issuer.	Select	
d) Labels on packages sent to the issuer must not indicate the name of the vendor.	Select		Examine a same of packages for issuers to verify that their package labeling does not indicate the name of the vendor.	Select	
e) If postal service mailbags are used in place of trays or locked carts, the bags must be sealed until transferred to the postal service.	Select		Examine a sample of postal service mailbags used in place of trays or locked carts to verify that they are sealed until transferred to the postal service.	Select	
4.5.2 Courier Service					
a) The vendor must secure packages under dual control with access limited to authorized personnel.	Select		Observe that the packages are secured under dual control with access limited to authorized personnel prior to transfer to courier service.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) The vendor must only utilize a courier service that assigns a unique tracking number for each package. A tracking system in conjunction with the tracking number must enable the vendor to identify the successful completion of delivery milestones and exception conditions during the delivery process commencing with initial pick-up and ending with delivery.	Select		Examine policies and procedures to verify that: • Only a courier service that assigns a unique tracking number for each package is used, • A tracking system is in place to enable the identification of: – Successful completion of delivery milestones during the delivery process from initial pick-up to final delivery. – Exception conditions during the delivery process commencing with initial pick-up and ending with delivery. Observe a sample of activity to verify the ability to track the package in accordance with the aforementioned.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) The vendor must ensure packages sent by courier service contain a manifest prepared by the vendor that describes the package contents and enables content-verification upon receipt. The manifest prepared by the vendor must include but is not limited to: • The type of each card • The quantity per card type • The job number(s) • The date of shipment • The date of receipt • Name of receiving organization • Name and signature of person receiving the cards	Select		Examine a sample of packages sent by courier to verify that each package contains a manifest prepared by the vendor that describes the package contents and enables content-verification upon receipt. Examine a sample of manifests to verify that they contain the minimum information required.	Select	
d) The contents of the manifest must be reconciled with the audit trail for the job.	Select		Examine policies and procedures to verify that the contents of the manifest are reconciled with the audit trail for each job.	Select	
e) Shipping of packages must not take place on the last working day of the week or the day before a public holiday unless the courier's operations and that of the recipient facilitate the delivery in the same manner as all other working days—i.e., they are both open for business).	Select		Examine policies and procedures to verify that packages are not shipped on the last working day of the week or the day before a public holiday unless the courier's operations allow for delivery during weekend days and holidays. Observe a sample of shipping before the last working day of the week or the day before a public holiday to verify it only occurs if the courier's operations and those of the recipient facilitate the delivery in the same manner as all other working days.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) Receipt of the shipment and count of contents must be confirmed by the recipient, immediately upon receipt under dual control.	Select		Examine policies and procedures to verify that a process is in place to immediately confirm from the recipient the receipt of the package(s) and the count of contents for each package, and that the receipt was handled under dual control. Observe a sample of shipping logs to verify that upon receipt of shipment the contents are confirmed by the recipient under dual control.	Select	
g) For unpersonalized bulk cards, shipments are limited to 500 per package per day per issuer location per vendor. No more than five packages per month for a given destination must occur.	Select		Interview personnel to verify that unpersonalized bulk cards shipments are limited to 500/package/day/issuer location/vendor and that no more than five packages per month for a given destination occur. Examine documentation for a sample of unpersonalized bulk cards shipments to verify that the shipments were limited to 500 per package per day per issuer location per vendor and that no more than five packages per month for a given destination occurred.	Select	
4.5.3 Secure Transport					
a) The vendor must confirm with the VPA whether specific requirements apply to its geographic locations.	Select		Examine evidence of VPA guidance for whether specific requirements apply to its geographic locations.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Secure transport originates at the vendor or issuer and must terminate at a vendor, issuer, mail facility, pre-sort facility, or courier facility shipping area unless otherwise approved by the VPA.	Select		Examine policies and procedures to verify secure transport originates at the vendor or issuer and terminates at a vendor, issuer, mail facility, pre-sort facility, or courier facility shipping area unless otherwise approved by the VPA. Observe a sample of shipping logs to verify that secure transport originates at the vendor or issuer and terminates at a vendor, issuer, mail facility, pre-sort facility, or courier facility shipping area unless otherwise approved by the VPA.	Select	
c) Secure transport must occur in one of the following manners: armored vehicle, unarmored vehicle, air freight, sea freight, or rail freight, as outlined below.					
4.5.3.1 Armored Vehicle					
a) This service must be carried out under dual control.	Select		Examine the agreement(s) with the armored transport service to verify it contains language that ensures that armored services used employ dual control during card transport.	Select	
b) The card transport vehicle must not carry any signs or logos indicating it belongs to a card vendor.	Select		Examine the agreement(s) with the armored transport service to verify it contains language that ensures that card transport vehicles do not carry any signs or logos indicating they belong to a card vendor.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) If intermediate stops are made during transport, the carrier must ensure the integrity of the shipment remains intact:					
i. The cargo must never be left unattended unless the cargo area is armored.	Select		Examine the agreement(s) with the armored transport service to verify it contains language that ensures the card transport vehicle's cargo must never be left unattended unless the cargo area is armored.	Select	
ii. If the cargo area is unarmored, the vehicle transporting the cards must be under dual control at all times—e.g., a driver accompanied by a guard—and never left unattended during the trip.	Select		Examine the agreement(s) with the armored transport service to verify it contains language that ensures the card transport vehicles are always under dual control—e.g., a driver accompanied by a guard—and never left unattended during any trips if the cargo area of the vehicle is unarmored.	Select	
4.5.3.2 Unarmored Vehicle					
a) The card transport vehicle must not carry any signs or logos indicating it belong to a card vendor.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language if outsourced, to verify that any unarmored vehicle used for deliveries does not carry any signs or logos indicating it belongs to a card vendor.	Select	
b) An accompanying escort vehicle must be used in conjunction with the unarmored transport vehicle. This vehicle must not also be used as a card transport vehicle.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement if outsourced, to verify that any unarmored vehicle used for deliveries is accompanied by another vehicle that is not used for card transport.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) The card transport vehicle used between the vendor facility and the destination must be under dual control at all times (a driver accompanied by a guard) and never left unattended during the trip until the shipment enters a controlled environment at the destination.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify the card transport vehicle is under dual control at all times (a driver accompanied by a guard) and never left unattended during the trip until the shipment enters a controlled environment at the destination.	Select	
d) The card transport vehicle must be equipped with a communication device that enables two-way contact with the security controller.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify the card transport vehicle is equipped with a communication device that enables two-way contact with the security controller.	Select	
e) The transport between the vendor location and the destination location must be non-stop whenever possible—i.e., non-emergency stops are not permitted.	Select		Examine vendor policies and procedures, if done in-—i.e., using internal staff—or service provider agreement language to verify that all transports between the vendor location and the destination location are required to be nonstop whenever possible.	Select	
4.5.3.3 Air Freight					
a) Goods must be secured in locked or sealed containers.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify that shipments made via air freight are secured in locked or sealed containers.	Select	
b) Goods registered as consolidated cargo are not permitted.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify that goods registered as consolidated cargo are not permitted.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) The card transport vehicle must not carry any signs or logos indicating it belong to a card vendor.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language if outsourced, to verify that any vehicle used for transfer to the air freight terminal does not carry any signs or logos indicating it belongs to a card vendor.	Select	
d) An accompanying escort vehicle must be used in conjunction with the card transport vehicle. This vehicle must not also be used as a card transport vehicle.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement if outsourced, to verify that an accompanying escort vehicle is used. This vehicle is not to also be used as a card transport vehicle.	Select	
e) The card transport vehicle used between the vendor facility and the air freight facility must be under dual control at all times (a driver accompanied by a guard) and never left unattended during transfer until the shipment enters a customs or other controlled environment at the air freight facility—both sending and receiving.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify the card transport vehicle is under dual control at all times (a driver accompanied by a guard) and never left unattended during the transfer until the shipment enters a customs or other controlled environment at the air freight terminal.	Select	
f) The transport between the vendor location and the destination location must be non-stop whenever possible—i.e., non-emergency stops are not permitted.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify that all transports between the vendor location and the destination location are required to be nonstop whenever possible.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
g) The card transport vehicle must be equipped with a communication device that enables two-way contact with the security controller.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify the card transport vehicle is equipped with a communication device that enables two-way contact with the security controller.	Select	
h) If intermediate stops are made during air transport, the vendor must ensure the integrity of the shipment remains intact.	Select		Examine service provider agreement language to verify that the integrity of the shipment remains intact if intermediate stops are made during air transport.	Select	
i) An air freight facility capable of handling secure cargo must be used.	Select		Examine service provider agreement language to verify that packages on shipments via air freight are transported exclusively via air freight facilities capable of handling secure cargo.	Select	
j) If any ground storage is required before, during, or after the flight, the location must be secured and inaccessible to unauthorized personnel.	Select		Examine service provider agreement language to verify that the location of ground storage used before, during, or after the flight must be secured and inaccessible to unauthorized personnel.	Select	
k) The hand-carrying of goods is strictly prohibited.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify that the hand-carrying of goods is strictly prohibited.	Select	
4.5.3.4 Sea Freight					
a) Goods must be secured in locked or sealed containers.	Select		Examine service provider agreement language to verify that shipments made via sea freight are secured in locked or sealed containers.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Goods registered as consolidated cargo are not permitted.	Select		Examine service provider agreement language to verify that all transports between the vendor location and the destination location are required to be nonstop whenever possible.	Select	
c) Sea-freight service must be bonded.	Select		Examine service provider agreement language to verify that only container shipment is used.	Select	
d) The vendor must use container shipment.	Select		Examine service provider agreement language to verify that the vendor arranges delivery to and pick-up from dockside immediately.	Select	
e) The sea shipping container must be locked while in the vendor's shipping area using a tamper-evident, high-security locking mechanism.	Select		Examine service provider agreement language to verify that the sea freight service is required to be bonded.	Select	
f) The container transport vehicle must not carry any signs or logos that would indicate it belongs to the card vendor.	Select		Examine service provider agreement language to verify that goods registered as consolidated cargo are not permitted.	Select	
g) An accompanying escort vehicle must be used in conjunction with the container transport vehicle. This vehicle must not also be used as a card transport vehicle.	Select		Examine service provider agreement language to verify that the hand-carrying of goods is strictly prohibited.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
h) The shipping container transport vehicle used between the vendor facility and the port facility must be under dual control at all times (a driver accompanied by a guard) and never left unattended during transfer until the container enters a customs or other controlled environment at the dock yard—both sending and receiving.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify the shipping container transport vehicle is under dual control at all times (a driver accompanied by a guard) and never left unattended during the transfer until the container enters a customs or other controlled environment at the dock yard.	Select	
i) The transport between the vendor location and the port facility must be nonstop—both sending and receiving—i.e., non-emergency stops are not permitted.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify that transport between the vendor location and the port facility terminal is nonstop - both sending and receiving.	Select	
j) A direct route sea transport is required whenever possible.	Select		Examine service provider agreement language to verify that all sea transports are required to be nonstop whenever possible.	Select	
k) The container transport vehicle must be equipped with a communication device that enables two-way contact with the security controller.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify the container transport vehicle is equipped with a communication device that enables two-way contact with the security controller.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
l) The container transport vehicle location and transport status must be monitored during transport by a controller who is able to take action should the vehicle deviate from its expected route or an alarm is activated.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify the container transport vehicle location and transport status are monitored during transport by a controller who is able to take action should the vehicle deviate from its expected route or an alarm is activated.	Select	
m) The sea shipping container must be fitted with a GPS monitoring system that provides real-time tracking of the container location.	Select		Examine service provider agreement language to verify the sea shipping container is fitted with a GPS monitoring system that provides real-time tracking of the container.	Select	
n) The tracking system must provide real-time alerts in the event exception conditions are detected that affect container integrity including door opening, lighting changes, internal motion, and impacts.	Select		Examine service provider agreement language to verify the sea shipping container tracking system provides real-time alerts in the event exception conditions are detected that affect container integrity including door opening, lighting changes, internal motion, and impacts.	Select	
o) If intermediate stops are made during sea transport, the vendor must ensure the integrity of the shipment remains intact.	Select		Examine service provider agreement language to verify that the integrity of the shipment remains intact if intermediate stops are made during sea transport.	Select	
p) A representative of the vendor must be present if the contents of the shipping container must be inspected by customs.	Select		Examine service provider agreement language to verify that a representative of the vendor is present if the contents of the shipping container must be inspected by customs.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
q) After inspection, the shipping container must be resealed with a new tamper-evident, high-security locking mechanism.	Select		Examine service provider agreement language to verify that after inspection, the shipping container is resealed with a new tamper-evident, high-security locking mechanism.	Select	
r) On arrival at the destination port facility, the container must be collected as soon as possible and delivered to the final destination address.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify that upon arrival at the destination port facility, the container is collected as soon as possible and delivered to the final destination address.	Select	
s) The locked shipping container must be delivered to an issuer or certified vendor facility prior to opening and further distribution of the card shipment.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify that the locked shipping container is delivered to an issuer or certified vendor facility prior to opening and further distribution of the card shipment.	Select	
t) The hand-carry of goods is strictly prohibited.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify that the hand-carrying of goods is strictly prohibited.	Select	
4.5.3.5 Rail Freight					
a) Goods must be secured in locked or sealed containers.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify that shipments made via rail freight are secured in locked or sealed containers.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Goods registered as consolidated cargo are not permitted.	Select		. Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify that goods registered as consolidated cargo are not permitted.	Select	
c) The rail shipping container must be locked while in the vendor's shipping area using a tamper-evident, high-security locking mechanism.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify the rail shipping container is locked while in the vendor's shipping area using a tamper-evident, high-security locking mechanism.	Select	
d) The container transport vehicle must not carry any signs or logos that would indicate it belongs to the card vendor.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify the container transport vehicle does not carry any signs or logos indicating it belongs to a card vendor.	Select	
e) An accompanying escort vehicle must be used in conjunction with the container transport vehicle. This vehicle must not also be used as a card transport vehicle.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement if outsourced, to verify that an accompanying escort vehicle is used. This vehicle is not to also be used as a card transport vehicle.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) The shipping container transport vehicle used between the vendor facility and the rail facility must be under dual control at all times (a driver accompanied by a guard) and never left unattended during transfer until the container enters a customs or other controlled environment at the rail yard—both sending and receiving.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify the shipping container transport vehicle is under dual control at all times (a driver accompanied by a guard) and never left unattended during the transfer until the container enters a customs or other controlled environment at the rail yard.	Select	
g) The transport between the vendor location and the rail facility must be nonstop - both sending and receiving—i.e., non-emergency stops are not permitted.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify that transport between the vendor location and the rail facility terminal is nonstop - both sending and receiving.	Select	
h) A direct route rail transport is required whenever possible.	Select		Examine service provider agreement language to verify that all rail transports are required to be nonstop whenever possible.	Select	
i) The container transport vehicle must be equipped with a communication device that enables two-way contact with the security controller.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify the container transport vehicle is equipped with a communication device that enables two-way contact with the security controller.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
j) The container transport vehicle location and transport status must be monitored during transport by a controller who is able to take action should the vehicle deviate from its expected route or an alarm is activated.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify the container transport vehicle location and transport status are monitored during transport by a controller who is able to take action should the vehicle deviate from its expected route or an alarm is activated.	Select	
k) The rail shipping container must be fitted with a GPS monitoring system that provides real-time tracking of the container location.	Select		Examine service provider agreement language to verify the rail shipping container is fitted with a GPS monitoring system that provides real-time tracking of the container.	Select	
l) The tracking system must provide real-time alerts in the event exception conditions are detected that affect container integrity including door opening, lighting changes, internal motion, and impacts.	Select		Examine service provider agreement language to verify the rail shipping container tracking system provides real-time alerts in the event exception conditions are detected that affect container integrity including door opening, lighting changes, internal motion, and impacts.	Select	
m) If intermediate stops are made during rail transport, the vendor must ensure the integrity of the shipment remains intact.	Select		Examine service provider agreement language to verify that the integrity of the shipment remains intact if intermediate stops are made during rail transport.	Select	
n) A representative of the vendor must be present if the contents of the shipping container must be inspected by customs.	Select		Examine service provider agreement language to verify that a representative of the vendor is present if the contents of the shipping container must be inspected by customs.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
o) After inspection, the shipping container must be resealed with a new tamper-evident, high-security locking mechanism.	Select		Examine service provider agreement language to verify that after inspection, the shipping container is resealed with a new tamper-evident, high-security locking mechanism.	Select	
p) On arrival at the destination rail terminal, the container must be collected as soon as possible and delivered to the final destination address.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify that upon arrival at the destination rail terminal, the container is collected as soon as possible and delivered to the final destination address.	Select	
q) The locked shipping container must be delivered to an issuer or certified vendor facility prior to opening and further distribution of the card shipment.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify that the locked shipping container is delivered to an issuer or certified vendor facility prior to opening and further distribution of the card shipment.	Select	
r) The hand-carry of goods on rail freight solutions is strictly prohibited.	Select		Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify that hand-carry of goods on rail freight solutions is strictly prohibited.	Select	
4.6 Shipping and Receiving					
The vendor must not release card products or components unless the following minimum shipping requirements are met. The vendor must:					
a) Have access to the names and signatures of individuals who are authorized to collect and deliver shipments.	Select		Examine policies and procedures to verify that the vendor has the names and signatures of individuals who are authorized to collect and deliver shipments.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Verify the identity of personnel arriving to collect or deliver shipments.	Select		Examine policies and procedures to verify that the vendor confirms the identity of personnel arriving to collect or deliver shipments.	Select	
c) Confirm the identity with the signature list.	Select		Examine policies and procedures to verify that the vendor confirms the identity of individuals with the signature list.	Select	
d) Place the cartons on a pallet in such a manner that the sides of the carton showing the batch code are visible.	Select		Examine policies and procedures to verify that the vendor places the cartons on a pallet in such a manner that the sides of the carton showing the batch code are visible.	Select	
e) Record the name and signature of individual collecting or delivering the shipment.	Select		Examine policies and procedures to verify that the vendor records the name and signature of individuals collecting or delivering the shipment.	Select	
4.6.1 Procedures for Transportation and Receipt					
The vendor must implement the following procedures:					
a) Before release of the consignment, a pre-arranged method of identification between the vendor and destination party must be established to verify the authority and identity of the carrier to receive shipment.	Select		Examine shipping activity logs to verify establishment of a pre-arranged method of identification between the vendor and destination party to verify the authority and identity of the carrier to receive the shipment before release of the consignment.	Select	
b) At each point where custody and possession of the consignment changes from one entity or agent to another, the consignment must be inspected to confirm the integrity of all locks and seals.	Select		Examine shipping activity logs to verify that the consignment is inspected to confirm the integrity of all locks and seals at each point where custody and possession of the consignment changes from one entity to another.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) A written receipt must be completed under dual control at each point of transfer, confirming the integrity of the consignment.	Select		Examine shipping activity logs to verify that a written receipt is completed under dual control at each point of transfer, confirming the integrity of consignment.	Select	
d) If there is evidence that a container has been tampered with, is missing, or is not received as scheduled at its final destination, the requirements for loss or theft of card products (Section 3.11) must be followed, and there must be no further movement of the shipment without notification to the issuer and VPA.	Select		Examine shipping activity logs to verify that—in situations where evidence exists that a container has been tampered with, is missing, or is not received as scheduled at its final destination—the requirements for loss or theft of card products are followed and that no further movement of the shipment is made without notification to the issuer and VPA.	Select	
e) Obtain positive confirmation of receipt of shipment.	Select		Examine shipping activity logs to verify that positive confirmation of receipt of shipment is obtained by the vendor.	Select	
4.6.2 Receipt and Return of Card Components					
a) All card components must be delivered and returned by secure transport.	Select		Examine policies and procedures to verify that all card components subject to return are delivered by secure transport.	Select	
b) The consignment must be received under dual control.	Select		Examine shipping activity logs to verify that the consignments of returned card components are received under dual control.	Select	
c) Whilst under dual control, the consignment must be inventoried and handled as defined in ”Audit Controls” (Section 3.7).	Select		Examine shipping activity logs to verify that the consignment of returned card components is inventoried and handled under dual control as defined in “Audit Controls” (Section 3.7).	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Documentation of the shipment must be maintained for 24 months and must include: • Item description • Sequential identification numbers (if applicable) • Reel numbers (if applicable) • Total quantity returned • Recipient name and signatures • Destination or origination address • Shipping or receipt date and time	Select		Examine shipping activity logs to verify that documentation of the shipments is maintained for 24 months and includes: • Item description • Sequential identification numbers (if applicable) • Reel numbers (if applicable) • Total quantity returned • Recipient name and signatures • Destination or origination address • Shipping or receipt date and time	Select	
e) Prior to shipment, the vendor must ensure that the names and signatures of the authorized recipients are recorded.	Select		Examine shipping activity logs to verify that the names and signatures of the authorized recipients of returned card components are recorded prior to shipment.	Select	
f) At shipment, the vendor must verify the authorized signatures prior to transfer.	Select		Examine shipping activity logs to verify that the authorized signatures are verified prior to transfer at shipment.	Select	
4.7 Establishing Responsibility for Loss					
a) The transfer of shipment responsibility occurs at the point at which the vendor has delivered cards according to the contract between the issuer and the approved vendor.	Select		Examine a sample of agreements with issuers to verify that they contain language indicating that the transfer of shipment responsibility occurs at the point at which the vendor has delivered cards.	Select	

Section 5: PIN Printing and Packaging of Non-personalized Prepaid Cards

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
The following requirements apply only for non-personalized, prepaid cards. All other preceding requirements apply unless explicitly superseded in this section. *The PIN-printing system may be a single, integrated device with multiple components (e.g., control system, HSM, and printer) or a system of separate components with dedicated functionality, connected via cables.* *Prepaid cards may be packaged, shipped, and mailed together with their PINs, provided the following requirements are fulfilled:*					
5.1. The vendor must obtain written authorization from the issuer for packaging, shipping, or mailing the card and PIN together. This authorization must include confirmation that:	Select		Examine policies/procedures to verify they require written authorization from the issuer for packaging, shipping, or mailing the card and PIN together to include confirmation that: • Cards will not be activated or loaded with a stored value until they have reached their destination, and • The issuer accepts all risk inherent in shipping or mailing cards and PINs together. Examine a sample of written authorizations from issuers to verify that procedures are followed.	Select	
a) Cards will not be activated or loaded with a stored value until they have reached their destination, and	Select			Select	
b) The issuer accepts all risk inherent in shipping or mailing cards and PINs together.	Select			Select	
5.2 The vendor must ensure that an appropriate officer of the issuer has signed the authorization letter and must maintain a copy of the letter in its files until the card expiry date.	Select		Examine a sample of authorization letters to verify that: • An appropriate officer of the issuer has signed the authorization letter. • A copy of the letter is maintained in its files until the card expiry date.	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
5.3 A card production staff member who is involved in PIN printing must not be involved in the card personalization process or the packaging of the card with the PIN process. An audit trail must be created and maintained as evidence that this separation has been enforced.	Select		Examine policies/procedures to verify: • Card production staff involved in PIN printing are not allowed to be involved in the card personalization process or the packaging of the card with the PIN process. • An audit trail ensuring separation of duties regarding PIN printing and card personalization is maintained. Examine physical access-control system access lists for authorized individuals provided entry into the PIN-printing area and compare with those authorized to enter personalization areas. Observe process to verify that restricted access is being enforced for the PIN-printing area.	Select	
5.4 The matching of a card with a pre-printed PIN mailer—e.g., affixing the card to a carrier on which the PIN has already been printed, or placing the PIN mailer and card into one package—must be performed in the personalization HSA or in a separate HSA that meets the physical and logical requirements for a personalization HSA.	Select		Observe that all activity surrounding the matching of the card with a pre-printed PIN mailer is being handled either in the personalization HSA, or in a separate HSA that meets the physical and logical requirements for a personalization HSA.	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
5.5 Clear-text PINs must never be available on any system on the personalization network.	Select		Examine documentation to verify that clear-text PINs are never to be available on any system on the personalization network. Interview the network administrator to have them validate that clear-text PINs must never be available on any system on the personalization network. Observe DB tables containing PIN data retrieved by the network administrator to verify PINs are not in clear text.	Select	
5.6 PIN-printing systems must be either on a network physically separate from the personalization network or on a logically separated subnet dedicated for PIN printing, which is protected by a dedicated firewall.	Select		Examine network diagrams to verify that PIN-printing systems are either on: • A network physically separate from the personalization network, or • A logically separated subnet dedicated for PIN printing, which is protected by a dedicated firewall. Examine firewall rules to verify the aforementioned.	Select	
5.7 Keys used for encrypting PINs must meet the key-management requirements defined in the *PCI Card Production and Provisioning Logical Security Requirements* document.	Select		Addressed in review conducted under the *PCI Card Production and Provisioning Logical Security Requirements.*	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
5.8 PINs must be deleted from the PIN-printing system immediately after printing using a secure erasure tool that prevents recovery of the PIN using forensic techniques or off-the-shelf recovery software.	Select		Examine documentation to identify the controls in place to verify that PINs are deleted from the PIN-printing system immediately after use via: • A secure erasure tool that prevents recovery of the PIN using forensic techniques, or • Off-the-shelf recovery software. • Interview the PIN production manager to verify secure erasure of PINs after printing. Observe PIN-printing process and verify that PINs are securely erased immediately after printing.	Select	
5.9 The clear-text PIN must only be available for the minimum time required for printing and must not be stored.	Select		Examine documentation to verify that clear-text PINs are not stored. Observe PIN-printing process and verify that clear-text PINs are only available for minimum time required for printing and are not stored in clear text.	Select	
5.10 If the clear-text PIN is available outside the printer at any time—e.g., in the memory of the controlling system or PC—the entire PIN-printing system (including the HSM) must:					
a) Be in a dedicated PIN-printing room as defined in the Section 2.3.5.4 of this document, "PIN Mailer Production Room"; and	Select		Examine architecture documentation to verify that the PIN-printing room is in a dedicated room as defined in Section 2.3.5.4. Interview the owner of the PIN-printing process to verify whether clear-text PINs are available outside of the printer and to identify locations.	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Only be made operational after physical review of the cabling has been performed and it is confirmed that there is no evidence of tampering.	Select		Observe cabling to confirm no evidence of tampering. Observe how it is secured above ceiling or below flooring and the procedure for gaining access to cabling.	Select	
c) Additionally, the PIN must be concealed in tamper-evident packaging immediately after printing.	Select		Observe the process for how the PIN is concealed in tamper-evident packaging immediately after printing.	Select	
5.11 If the clear-text PIN is only available inside the single, integrated device—i.e., the HSM, controller, printer, and all cabling that carries the PIN are secured inside a single, integrated device—PIN printing may take place in any of the following places:					
a) The personalization HSA	Select		Examine documentation to verify that clear-text PINs only exist within a single integrated device. Observe that this occurs within the personalization HSA; or	Select	
b) A dedicated PIN printing room within the personalization HSA	Select		Observe that that the activity occurs in a room dedicated to only PIN printing; or	Select	
c) A separate HSA that meets the physical and logical requirements for a personalization HSA	Select		Observe the separate HSA to verify set-up of the separate HSA meets the physical and logical requirements for a personalization HSA.	Select	
d) Additionally, all of the following requirements must be fulfilled:	Select		Examine policies/procedures to verify that each of the following is required:	Select	
e) The printer must be locked under dual control before the print job starts and any PINs are decrypted.	Select		Observe the PIN-printing process to verify the printer is locked under dual controls before the print job starts and any PINs are decrypted.	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) The HSM in the printer must be under dual control at all times.	Select		Observe that the HSM is handled under dual control at all times.	Select	
g) The print job must only be started after a physical review of the chassis and cabling has been performed and it is confirmed that there is no evidence of tampering.	Select		Observe the PIN process to verify that a physical review of the chassis and cabling has been performed, and there is no evidence of tampering.	Select	
h) The clear-text PIN must only be available inside a securely locked and covered area of the machine for the minimum time required for printing and must not be stored.	Select		Observe the PIN process to verify that clear-text PINs are only available inside a securely locked and covered area of the machine, for the minimum time required printing, and are never stored. Interview the owner of the PIN-printing process to validate that no storage of the clear-text PINs is allowed.	Select	
i) The printed PIN must not be visible from outside the machine at any time—i.e., the machine must be covered to prevent observation and the covers must be locked in place with dual-control locks.	Select		Observe the PIN-printing process to verify that: • No visibility of the PIN is possible from outside the machine. • The covers on the machine are locked in place with dual control locks.	Select	
j) The PIN must be concealed in tamper-evident packaging immediately after printing and before leaving the secured confines of the printer.	Select		Observe the PIN-printing process to verify that the PIN is concealed in tamper-evident packaging: • Immediately after printing, and • Before leaving the secured confines of the printer.	Select	

Appendix B: Logical Security Requirements – CCTV and Access Control System Administration

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
B.1 User Management					
The vendor must:					
a) Ensure that procedures are documented and followed by security personnel responsible for granting access to the CCTV and access-control systems.	Select		Examine procedures for granting access to the CCTV system and access-control systems to verify existence. Interview security personnel responsible for the adding or removing of authorized users on the CCTV system and access-control systems to verify adherence to procedures.	Select	
b) Restrict approval and level of access to staff with a documented business need before access is granted. At a minimum, documented approvals must be retained while the account is active.	Select		Examine a sample of access grants and compare the positions of those granted access to the CCTV and access-control systems to verify access is appropriately restricted.	Select	
c) Restrict systems access by unique user ID to only those individuals who have a business need.	Select		Examine documentation to verify there is a list of roles that need system access together with a legitimate business need for each role to have such access. Interview administrator to verify that system access is restricted to only those unique user IDs who have a business need.	Select	

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Only grant individuals the minimum level of access sufficient to perform their duties.	Select		Examine documentation and verify that the access is restricted based on least privileges necessary to perform job responsibilities. Interview administrator to verify that individual access is based the minimum level of access sufficient to perform their duties.	Select	
e) Make certain that systems authentication requires at least the use of a unique ID and password.	Select		Examine documentation to make certain that ID and password for system authentication is unique. Observe logon to system to verify that—at a minimum—authentication requires the use of an ID and password.	Select	
f) Restrict administrative access to the minimum number of individuals required for management of the system.	Select		Interview administrator to determine names of people with administrative access. Interview management of systems to determine if the number of people with administrative access is the minimum number of individuals required for management of the system.	Select	
g) Ensure security guards do not have administrative access.	Select		Examine names of people with administrative access and cross reference with names of security guards to verify the guard names do not have administrative access.	Select	
h) Prevent remote administrative access from outside the facility, except as used in conjunction with an approved SOC.	Select		Examine configurations for remote access technologies to verify that remote access sessions are not enabled, except as used in conjunction with an approved SOC.	Select	

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
i) Ensure that group, shared, and generic accounts and passwords are disabled wherever the system supports unique values.	Select		Examine documentation to verify that group, shared, and generic accounts and passwords are disabled wherever the system supports unique values.	Select	
j) Ensure that where generic administrative accounts cannot be disabled, these accounts are used only when unique administrator sign-on credentials are not possible and only in an emergency.	Select		Examine documentation to determine if generic administrative accounts are enabled. If generic administrative accounts are enabled, examine documentation to verify that such accounts are used only: • When unique administrator sign-on credentials are not possible, and • In an emergency.	Select	
k) Ensure that when generic administrative accounts are used, the password is managed under dual control where no individual has access to the full password. Each component of the password must comply with the password control requirements in the next section except for password length where an exception condition exists.	Select		Examine documentation to verify that when generic administrative accounts are used: • The password is managed under dual control where no individual has access to the full password; and • Each component of the password complies with the password control requirements in the next section.	Select	
l) Validate all system access at least quarterly.	Select		Examine documentation to verify that (at least quarterly) all system access is reviewed. Examine a sample of system access reviews to verify they system access is validated at least quarterly.	Select	

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
m) Revalidate card production staff to any systems upon a change of duties.	Select		Examine a sample of personnel who have changed duties to verify that card production staff access review of relevant systems was conducted after their change in duties.	Select	
n) Ensure that access controls enforce segregation of duties.	Select		Examine documentation to verify that access controls enforce segregation of duties.	Select	
o) Strictly limit privileged or administrative access and ensure such access is approved by both the user's manager and the physical security manager.	Select		Examine documentation to verify that all privileged or administrative access is approved by both the user's manager and the physical security manager.	Select	
p) Establish management oversight of privileged access to ensure compliance with segregation of duties.	Select		Interview management to validate that there is oversight of privileged access to ensure compliance with segregation of duties.	Select	
q) Ensure that all privileged administrative access is logged and reviewed weekly.	Select		Examine a sample of system logs to verify that privileged administrative access is logged and reviewed at least weekly. Interview management to verify that review of logs is performed at least weekly.	Select	
B.2 Password Control					
B.2.1 General					
The vendor must:					
a) Implement a policy and detailed procedures relating to the generation, use, renewal, and distribution of passwords.	Select		Examine policies/procedures to verify coverage of the generation, use, renewal, and distribution of passwords. Interview management to verify that procedures relating to the generation, use, renewal, and distribution of passwords are followed.	Select	

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Implement procedures for handling lost, forgotten, and compromised passwords.	Select		Examine polices/procedures to verify that there is a procedure relating to handling lost, forgotten, and compromised passwords. Interview management to verify that procedures relating to handling lost, forgotten, and compromised passwords are followed.	Select	
c) Distribute password procedures and policies to all users who have access to cardholder data, or any system used as part of the personalization process.	Select		Examine password polices/procedures to verify existence and evidence that they have been distributed to all users who have access to cardholder data, or any system used as part of the personalization process.	Select	
d) Ensure that only users with administrative privileges can administer other users' passwords.	Select		Observe process to administer other users' passwords. Observe a sample of non-administrative users to verify that they do not have the ability to administer other users' passwords	Select	
e) Not store passwords in clear text.	Select		Observe data tables containing passwords and verify (on screen) that none of the entries are in clear text.	Select	
f) Change all default passwords.	Select		Observe system administrator log onto the system and validate that all default passwords have been changed.	Select	
B.2.2 Characteristics and Usage					
The vendor must ensure that:					
a) Systems are configured so that newly issued and reset passwords are set to a unique value for each user.	Select		Examine system configuration settings to verify that password parameters are set to require that newly issued and reset passwords are set to a unique value for each user.	Select	

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Newly issued passwords are changed on first use.	Select		Examine system configuration settings to verify that newly issued passwords are changed on first use.	Select	
c) "First use" passwords expire if not used within 24 hours of distribution.	Select		Examine system configuration settings to verify that "first use" passwords expire if not used within 24 hours of distribution.	Select	
d) Systems enforce password lengths of at least 12 characters or an equivalent strength.	Select		Examine system configuration settings to verify that systems enforce password lengths of at least 12 characters.	Select	
e) Passwords consist of a combination of at least three of the following: • Upper-case letters • Lower-case letters • Numbers • Special characters	Select		Examine system configuration settings to verify that password configuration parameters consist of a combination of at least three of the following: • Upper-case letters • Lower-case letters • Numbers • Special characters	Select	
f) Passwords are not the same as the user ID.	Select		Examine system configuration settings to verify that systems enforce that passwords are not allowed to the same as the user ID.	Select	
g) Passwords are not displayed during entry.	Select		Observe a sample of user logons to validate that passwords are not displayed in clear text during entry.	Select	
h) Passwords are encrypted during transmission and rendered unreadable when stored.	Select		Examine documentation to verify that passwords are encrypted during transmission and rendered unreadable when stored. Examine a sample of password data repositories to verify the password field is rendered unreadable (that is, not stored in plaintext).	Select	

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
i) Passwords have a maximum life not to exceed 90 days and a minimum life of at least one day.	Select		Examine system configuration settings to verify that passwords have a maximum life not to exceed 90 days and a minimum life of at least one day.	Select	
j) When updating passwords, the system prevents users from using a password that is the same as one of their previous four passwords.	Select		Examine system configuration settings to verify that when updating passwords, the system prevents users from using a password that is the same as one of their previous four passwords.	Select	
k) The user's identity is verified prior to resetting a user password.	Select		Examine polices/procedures for password resets to identify the process for validating the user identity prior to reset. Observe security personnel to verify that, if a user requests a reset of an authentication credential by phone, e-mail, web, or other non-face-to-face method, the user's identity is verified before the authentication credential is modified.	Select	
B.3 Session Locking					
a) The vendor must enforce the locking of an inactive session within a maximum of 15 minutes. If the system does not permit session locking, the user must be logged off after the period of inactivity.	Select		Examine system configuration settings, including those for remote access, to verify that system/session idle time-out features have been set to 15 minutes or less, either through session locking or, if unsupported, through logging off.	Select	
B.4 Account Locking					
a) Accounts that have been inactive for a specified period (with a maximum of 90 days) must be removed from the system.	Select		Examine a sample of user accounts to verify that any inactive accounts over 90 days old are either removed or disabled.	Select	

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Systems must enforce the locking of a user account after a maximum of six unsuccessful authentication attempts.	Select		Examine system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts.	Select	
c) Locked accounts must only be unlocked by the security administrator. Alternatively, user accounts may be unlocked via automated password reset mechanisms. Challenge questions with answers that only the individual user would know must be used. These questions must be designed such that the answers are not information that is available elsewhere in the organization, such as in the Human Resources Department.	Select		Examine documentation to validate that locked accounts must only be unlocked by the security administrator or via an automated password reset mechanism. Examine documentation where systems utilize unlocking via automated password reset mechanisms and validate the following: • Challenge questions with answers that only the individual user would know must be used. • The questions are designed such that the answers are not information that is available elsewhere in the organization, such as in the Human Resources Department. Examine a sample of password resets to verify that the above procedures are followed.	Select	
d) A user's account must be locked immediately upon that user leaving the vendor's employment until it is removed.	Select		Examine documentation to validate that a user's account must be locked immediately upon that user's leaving the vendor's employment until it is removed. Examine a sample of user departures to verify that the user's account was immediately locked upon the termination of employment from the vendor.	Select	

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) A user's account must be locked immediately if that user's password is known or suspected of being compromised.	Select		Examine documentation to validate that a user's account must be locked immediately if that user's password is known or suspected of being compromised.	Select	
f) The user account logs including but not limited to the following must be reviewed at least twice each month for suspect lock-out activity: • Remote access • Database • Application • OS	Select		Examine documentation to validate that account logs are reviewed at least twice each month for suspect lock-out activity—e.g., invalid logon attempts—for each of the following: • Remote access • Database • Application • OS	Select	

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
B.5 Anti-virus Software or Programs					
The vendor must:					
a) Define, document, and follow procedures to demonstrate: • Identification of security alerts—e.g., subscribing to security alerts such as Microsoft and the Computer Emergency Response Team (CERT) • Identification of system component updates that affect the supportability and stability of operating systems, software drivers, and firmware components • Inventory of current systems in the environment including information about installed software components and about running services	Select		Examine anti-virus policies/procedures to verify that the following are defined and that corresponding procedures exist for each: • Identification of security alerts—e.g., subscribing to security alerts such as Microsoft and the Computer Emergency Response Team (CERT) • Identification of system component updates that affect the supportability and stability of operating systems, software drivers, and firmware components • Inventory of current systems in the environment including information about installed software components and about running services	Select	
b) Deploy anti-virus software on all systems potentially affected by malicious software—e.g., personal computers and servers.	Select		Examine a sample of system components including all operating system types commonly affected by malicious software, and verify that anti-virus software is deployed if applicable anti-virus technology exists.	Select	

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Ensure that all anti-virus programs detect, remove, and protect against all known types of malicious software.	Select		Examine vendor documentation and examine anti-virus configurations to verify that anti-virus programs: • Detect all known types of malicious software; • Remove all known types of malicious software; and • Protect against all known types of malicious software. *Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits.*	Select	
d) Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	Select		Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date. Examine anti-virus configurations, including the master installation of the software to verify anti-virus mechanisms are: • Configured to perform automatic updates, and • Configured to perform periodic scans. Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that: • The anti-virus software and definitions are current. • Periodic scans are performed. Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that anti-virus software log generation is enabled.	Select	

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) Check for anti-virus updates at least daily and install updates in a manner consistent with patch management. Documentation must exist for why any updates were not installed.	Select		Examine patch management documentation to verify that: • Anti-virus is updated at least daily. • Updates are installed in a manner consistent with patch management guidelines. • A process exists to document why any updates were not made. Interview the system administrator to verify that anti-virus updates are applied at least daily, and updates are installed in a manner consistent with patch management.	Select	
B.6. Configuration and Patch Management					
The vendor must:					
a) Implement a documented procedure to determine whether applicable patches and updates have become available.	Select		Examine documentation related to patch management to verify: • Processes are defined for determining whether patches are applicable to systems; and • Updates are available for installation. Interview the system administrator to verify that procedures are implemented to determine whether applicable patches and updates have become available.	Select	

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Make certain a process is implemented to identify and evaluate newly discovered security vulnerabilities and security patches from software vendors.	Select		Examine documentation related to patch management to verify processes are defined for: • Identifying and evaluating newly discovered security vulnerabilities, and • Identifying and evaluating security patches from software vendors. Interview the system administrator to verify that procedures are implemented to identify and evaluate newly discovered security vulnerabilities and security patches from software vendors.	Select	
c) Ensure that secure configuration standards are established for all system components.	Select		Examine documentation to verify that secure configuration standards are established for all system components. Interview the system administrator to verify that a secure configuration standard exists and that there is a documented configuration standard for all system components.	Select	
d) Ensure that the configuration standards include system hardening by removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	Select		Examine the organization's system configuration standards for all types of system components and verify that the standard addresses: • The removing of all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	Select	

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) Ensure that the configuration of all system components associated with data transmission, storage, and personalization are validated against the authorized configuration monthly.	Select		Examine documentation to verify that there is a process in place to validate security configurations monthly for ACS and CCTV systems against the authorized configuration. Examine a sample of the ACS and CCTV systems to verify that the security configuration file has been validated within the past month against the authorized configuration.	Select	
f) Evaluate and install the latest security-relevant patches for all system components within 30 days of their release (if they pass validation tests).	Select		Examine documentation related to patch management to verify processes are defined for: • Evaluating and installing the latest security-relevant patches for all system components within 30 days of their release (if they pass validation tests). Examine a sample of recently implemented security relevant patches to verify they were: • Tested, • Approved for install, and • Applied within a 30-day cycle of their release.	Select	
g) Verify the integrity and quality of the patches before application, including source authenticity.	Select		Examine documentation related to patch management to verify processes are defined for: • Verifying the integrity and quality of the patches before application, including source authenticity.	Select	

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
h) Make a backup of the system being changed before applying any patches.	Select		Examine a sample of recently implemented security relevant patches to verify they were applied after first having the relevant system backed-up prior to the patch being applied.	Select	
i) Implement critical patches to all Internet-facing system components within seven business days of release. When this is not possible the CISO, security manager, and IT director must clearly record that they understand that a critical patch is required and authorize its implementation within a maximum of 30 business days.	Select		Examine documentation related to patch management to verify processes are defined for: • Implementing critical patches to all Internet-facing system components within seven business days of release. • Documenting exceptions for when this is not possible. • The exceptions process, which includes the CISO, IT security manager, and IT director documenting that they understand that a critical patch is required and authorize its implementation within a maximum of 30 business days. Examine a sample of recent critical patches to verify that they were either applied within seven business days or the CISO, IT security manager, and IT director documented that they understand that a critical patch was required and authorized its implementation within a maximum of 30 business days.	Select	

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
j) Ensure that emergency hardware and software implementations comply with the procedures and validation requirements established for emergency implementations.	Select		Examine documentation to verify procedures and validation requirements are established for emergency hardware and software implementations. Examine a sample of recent emergency installs and validate that the existing change-management audit trail demonstrates compliance with the procedures and validation requirements established for emergency implementations.	Select	
k) Ensure that emergency hardware and software implementations follow the configuration and patch management requirements in this section.	Select		Examine a sample of recent emergency hardware and software implementations to verify that they follow the configuration and patch management requirements in this section (B.6, "Configuration and Patch Management").	Select	
B.7 Audit Logs					
The vendor must:					
a) Ensure that audit logs exist for the CCTV and access-control systems This includes operating system logs, security software logs or product logs and application logs containing security events.	Select		Examine a sample of audit logs to verify they exist for the CCTV and access-control systems and they include: • Operating system logs, • Security software logs or • Product logs and • Application logs containing security events	Select	

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Ensure that audit logs include at least the following components: • User identification • Type of event • Valid date and time stamp • Success or failure indication • Origination of the event • Identity or name of the affected data, system component, or resources • Access to audit logs • Changes in access privileges	Select		Examine a sample of audit logs and verify that they include at least the following components: • User identification • Type of event • Valid date and time stamp • Success or failure indication • Origination of the event • Identity or name of the affected data, system component, or resources • Access to audit logs • Changes in access privileges	Select	
c) Ensure that procedures are documented and followed for audit log review and reporting of unusual activity. Log reviews may be automated or manual and must occur at least monthly.	Select		Examine documentation to validate that procedures exist, they are documented, and they are followed for: • Audit log review and • Reporting of unusual activity; and • Log reviews are either automated or manual; and • Reviews occur on a frequency that is at least monthly.	Select	
d) Verify at least once a month that all systems are meeting log requirements.	Select		Examine documentation to verify that at least once a month all systems are meeting log requirements as defined in this section (B.7, “Audit Logs”).	Select	

Appendix B Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) Ensure that logs are backed up daily, secured, and retained for at least one year. Logs must be accessible for at least three months online and one year offline.	Select		Examine documentation to verify that audit logs are backed up daily, secured, and retained for at least one year. Verify that the logs are accessible for at least three months online and one year offline. Examine a sample of logs to verify that they are: • Backed up daily, secured, and retained for at least one year • Accessible for at least three months online and one year offline	Select	
f) Protect and maintain the integrity of the audit logs from any form of modification.	Select		Examine documentation to verify audit logs are protected from unauthorized modifications via access-control mechanisms, physical segregation, network segregation, encryption, or hashing.	Select	
g) Implement a security-incident and event-logging framework for its organization.	Select		Examine documentation to verify that security-incident and event-logging are implemented within the organization.	Select	