Payment Card Industry (PCI)

# Card Production and Provisioning Physical Security

## Requirements and Test Procedures

**Version 3.0.1**

June 2022

# Document Changes

| Date | Version | Description |
|---|---|---|
| December 2012 | 1.x | RFC version |
| May 2013 | 1.0 | Initial Release |
| March 2015 | 1.1 | Enhancements for clarification |
| July 2016 | 2.x | RFC version |
| January 2017 | 2.0 | Addition of Mobile Provisioning and other changes. See Summary of Changes from v1.1 to v2. |
| January 2022 | 3.0 | Renumbered requirements from 2 through 6 to 1 through 5. Added Appendix C-Security Operations Center. See Summary of Changes from v2.0 to v3.0. |
| June 2022 | 3.0.1 | Errata |

# Contents

# Overview

## Scope

The *PCI Card Production and Provisioning Physical Security Requirements and Test Procedures* manual is a comprehensive source of information for entities involved in card production and provisioning, which may include manufacturers, personalizers, pre-personalizers, chip embedders, data-preparation, and fulfillment. The contents of this manual specify the physical security requirements and procedures that entities must follow before, during, and after the processes listed below. Also included are the related test procedures by which Payment Brand Assessors will assess compliance.

- Card Manufacturing
- Chip embedding
- Personalization
- Storage
- Packaging
- Mailing
- Shipping or delivery
- Fulfillment

In addition to the card production activities above this document defines the physical security requirements and test procedures for entities that:

- Perform cloud-based or secure element (SE) provisioning services;
- Manage over-the-air (OTA) personalization, lifecycle management, and preparation of personalization data; or
- Manage associated cryptographic keys.

It does not apply to providers who are only performing the distribution of secure elements.

Card production and provisioning entities management should review and recommend enhancements to the security procedures used by any contracted remote monitoring organization.

Appendix A, "Applicability of Requirements," makes further refinement at the requirement level for physical cards and mobile provisioning.

Although this document frequently states "vendor," the specific applicability of these requirements is up to the individual payment brands; and the payment brand(s) of interest should be contacted for the applicability of these requirements to any card production or provisioning activity.

Requirements for logical security for personalization are not included in this manual, but can be found in a separate document, *Payment Card Industry (PCI) Card Production and Provisioning – Logical Security Requirements and Test Procedures.*

***Note:*** *All additional logical actions for vendors involved in personalization activities are detailed in the Logical Security Requirements document.*

Entities may adopt additional security controls as they deem appropriate, provided they are in addition to and enhance the procedures set forth in this manual.

## Laws and Regulations

In addition to the physical security requirements contained in this document, there will almost certainly be relevant regional and national laws and regulations, including consumer protection acts, labor agreements, health and safety regulations, etc. It is the responsibility of each individual organization

independently to ensure that it obeys all local laws and regulations. Adherence to the requirements in this document does not imply compliance with local laws and regulations.

If any of the requirements contained in this manual conflict with country, state, or local laws, the country, state, or local law will apply.

## Loss Prevention

Vendors are responsible for preventing any unexplained product losses. Vendors are liable for any unexplained loss, theft, deterioration, or destruction of card products or components that may occur while such products are in the vendor's facility. Vendors are required to carry liability insurance covering all the risks stated above, taking into consideration the plant location, physical conditions and security of the plant, the number and duties of the card production staff, and the nature and volume of the contracted work.

## Limitations

The individual Participating Payment Brands are responsible for defining and managing compliance programs associated with these requirements. Contact the Participating Payment Brand(s) of interest for any additional criteria.

# Section 1: Roles and Responsibilities

## 1.1 Card Production Staff

| Requirement | Test Procedure |
|---|---|
| *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<br>b) Physical security manager<br>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.<br>d) Card production supervisor is any card production staff that fulfills a supervisory role of other staff. | Interview personnel to verify that the following roles are filled by vendor employees:<br>a) Senior management and corporate officers<br>b) Physical security manager<br>c) Any qualified individual accessible on-site acting as the physical security manager during any operational period of a facility<br>d) Card production staff that fulfills a supervisory role of other staff.<br>Examine the relevant appointment information for these positions. |
| ***1.1.2 Pre-employment Documentation and Background Checks***<br>*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<br>b) Part-time employees<br>c) Temporary employees, consultants, and contractors<br>d) Guards (internal or external) | Examine the pre-employment documentation for a sample of each category to verify it includes application documentation and a background check. |

## 1.1 Card Production Staff

| Requirement | Test Procedure |
|---|---|
| ***1.1.3 Applicant/Personnel 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.<br>b) This information must be available for the inspector during site security reviews. | 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.<br>Examine a sample of documentation from personnel whose contract of employment has been terminated within the last 18 months. |
| ***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:<br>• Details of any "alias" or any other names<br>• List of their previous addresses or residences for the last seven years<br>• Previous employers for the last seven years<br>• Applicants must satisfactorily explain gaps in employment. | Examine a sample of employment applications to verify that they have the minimum information required. |
| 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: | |
| i. Gathered as part of the hiring process:<br>– Background check results<br>– Verification of aliases (when applicable)<br>– List of previous employers and referral follow-up results<br>– Education history<br>– Social security number or appropriate national identification number<br>– Signed document confirming that the individual has read and understands the vendor's security policies and procedures<br>– Fingerprints and results of search against national and regional criminal records | Examine the personnel files of a sample of individuals to verify that they contain the minimum required documentation during their hiring process. |

## 1.1 Card Production Staff

| Requirement | Test Procedure |
|---|---|
| ii. Gathered as part of the hiring process and periodically thereafter:<br>– Current photograph, updated at least every three years<br>– Record of any arrests or convictions, updated annually<br>– Annual credit checks | 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:<br>• Current photograph, updated at least every three years<br>• Record of any arrests or convictions, updated annually<br>• Annual credit checks |
| c) These files must be available to the security inspectors during site reviews. | See above. |
| **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. | a) 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. |
| ***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. | 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.<br>b) Examine a sample of documentation to verify that the security manager is notified in writing prior to an employee's job change taking effect. |
| b) The physical security manager must adapt the access control to restricted areas within one business day. | 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.<br>Examine documentation or logs of a sample of such access-control changes were appropriately made. |
| c) Where necessary, all combinations and other applicable access codes known to or utilized by the individual are changed. | 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. |

## 1.1 Card Production Staff

| Requirement | Test Procedure |
|---|---|
| **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. | 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.<br><br>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. |
| 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. | 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. |
| c) Upon termination effective date of any personnel the physical security manager or designated representative must:<br>• Deactivate all access rights.<br>• Recover the photo ID badge.<br>• Change all applicable vault combinations and other applicable access codes known to or utilized by individual.<br>• Recover all company property used in association with card production or provisioning.<br>• Verify completion of the individual's termination checklist activities in Section 1.1.5.3, below. | 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:<br>• Deactivate all access rights.<br>• Recover the photo ID badge.<br>• Change all applicable vault combinations and other applicable access codes known to or utilized by individual.<br>• Recover all company property used in association with card production or provisioning.<br>• Verify completion of the individual's termination checklist activities in Section 1.1.5.3, below. |
| **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. | Examine documentation for a sample of terminated individual evidencing that such individual's computer user IDs and passwords have been disabled or removed. |
| b) Retrieve all software programs and documentation distributed to the individual. | Examine documentation for a sample of terminated individuals evidencing that all software programs and documentation distributed to such individuals have been retrieved. |
| c) Disable the individual's access to computer data and applications. | Examine documentation for a sample of terminated individuals evidencing that all such individuals' access to computer data and applications have been disabled. |

## 1.1 Card Production Staff

| Requirement | Test Procedure |
|---|---|
| d) Retrieve all company keys, badges, and company photo identification distributed to the individual. | 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. |
| e) Change all applicable vault combinations and other applicable access codes known to or utilized by the individual. | 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. |
| ***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. | 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. |
| 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. | 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:<br>• Have a signed employment agreement; and<br>• The agreement stipulates that the card production staff complies with company policies and rules. |
| c) Providing a copy of vendor's internal security manual to all card production staff and security personnel.<br>The security manual must include the following sections:<br>• Administration<br>• HSAs<br>• Security requirements and guidelines<br>• Procedures that card production staff must follow while working in the secure facility<br>• Specific requirements as they pertain to the cloud-based provisioning platforms and systems | Examine policies and procedures to verify that a copy of the internal security manual is provided to all card production staff and security personnel.<br>Examine the security manual to verify that it contains the minimum sections and related content required. |

## 1.1 Card Production Staff

| Requirement | Test Procedure |
|---|---|
| d) Evidence of positive affirmation by the card production staff of receipt and understanding of responsibilities and obligations under the security policy. | 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. |
| e) Ensuring that vendor staff security training incorporates the obligation for card production staff to report any observed breaches of established security procedure. | 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. |
| 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. | Examine a sample of documentation to verify the training occurred as stipulated. |
| g) Displaying information concerning security at key locations within the vendor facility via posters, notices, or electronic medium—e.g., monitors. | Observe key locations within the vendor facility to verify that information concerning security is displayed. |
| 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. | 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. |
| ***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<br>b) Physical security manager<br>c) Card production staff authorized to receive or sign for any card components | 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:<br>• Senior management and corporate officers<br>• Physical security manager<br>• Card production staff authorized to receive or sign for any card components |

## 1.2 Guards

| Requirement | Test Procedure |
|---|---|
| ***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. | 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. |
| 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. | 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. |
| **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. | 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. |
| b) Guards must not have access to:<br>• HSAs<br>• Personnel records<br>• Physical master keys that provide access to card production or provisioning areas<br>• Audit logs | Examine policies and procedures to verify that guards are not permitted access to the restricted areas and assets identified.<br>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, any restricted areas, or the assets identified. |
| c) Guards must be prevented from modifying or altering the internal configuration settings on access system controls, intrusion alarm system, closed circuit television (CCTV). | Interview system administrator(s) to verify the guards cannot modify or alter internal configuration settings on access system controls, intrusion alarm system, closed circuit television (CCTV).<br>Examine a sample of access permission settings to verify guards cannot modify or alter internal configuration settings on access system controls, intrusion alarm system, closed circuit television (CCTV). |

## 1.2 Guards

| Requirement | Test Procedure |
|---|---|
| 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. | 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.<br>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. |
| ***1.2.2 Role and Responsibilities***<br>*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. | 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. |
| b) It maintains a clear segregation of duties and independence between the production staff and the guards. | Interview guards and production staff to confirm that they have a clear segregation of duties and independence from the production staff. |
| c) Any time activities are performed in the HSA, the security control room is always occupied by at least one guard. | Interview guards to confirm that at least one guard occupies the security control room any time activities are performed in the HSA.<br>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. |
| ***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 | • Guard's responsibilities, procedures, and activities by position |
| b) Vendor's security policies | • Vendor's security policies |

## 1.2 Guards

| Requirement | Test Procedure |
|---|---|
| c) Interaction between production process management, contracted guard or monitoring services, the police, and other emergency services | • Interaction between production process management, contracted guard or monitoring services, the police, and other emergency services |
| d) Access control at all entry and exit points of the facility, by date and time of activation | • Access control at all entry and exit points of the facility, by date and time of activation |
| e) External resource response activities | • External resource response activities |
| f) CCTV monitoring and video or digital recordings | • CCTV monitoring and video or digital recordings |
| g) Administration of access credentials and photo ID badges | • Administration of access credentials and photo ID badges |
| 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) | • 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) |
| i) Company policy concerning card production staff, consultant, and visitor access to the facility (both exterior and interior) | • Company policy concerning card production staff, consultant, and visitor access to the facility (both exterior and interior) |
| j) Property removal | • Property removal |
| k) Shipping and receiving | • Shipping and receiving |
| l) Alarm activation procedures | • Alarm activation procedures |
| m) Response to alarms, including notification to law enforcement in cases of unauthorized access to the facility | • Response to alarms, including notification to law enforcement in cases of unauthorized access to the facility |
| n) Daily activity and immediate incident report | • Daily activity and immediate incident report |
| o) Potential threats—such as burglary or theft—to the facility's external or internal security | • Potential threats—such as burglary or theft—to the facility's external or internal security |

## 1.2 Guards

| Requirement | Test Procedure |
|---|---|
| p) Handling of emergencies including but not limited to:<br>• Fire<br>• Earthquakes<br>• Severe weather<br>• Direct assault by armed felons<br>• Bomb threats<br>• Civil disturbances<br>• Building evacuation<br>• Ransom demands<br>• Hostages<br>• Kidnapping | • Handling of emergencies including but not limited to:<br>– Fire<br>– Earthquakes<br>– Severe weather<br>– Direct assault by armed felons<br>– Bomb threats<br>– Civil disturbances<br>– Building evacuation<br>– Ransom demands<br>– Hostages<br>– Kidnapping |
| **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. | Examine documentation that evidences signed acknowledgement by guards that they have read and fully understand the contents of the security procedures manual. |
| **1.2.3.3 Security Procedures Manual Maintenance** | |
| a) Procedures must be reviewed, validated and if necessary, updated annually. | Examine documentation to verify updates occur annually as necessary. |
| ***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. | 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.<br>Examine records evidencing the guards received the training at least annually. |
| 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. | 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. |

## 1.3 Visitors

| Requirement | Test Procedure |
|---|---|
| a) Procedures for how visitors are managed at the vendor facility must be documented and followed. | Examine the security procedures manual to verify it contains procedures for how visitors are managed at the vendor facility.<br>Observe live visitor handling processes to confirm that the procedures are followed. |
| b) All visitors to the facility must be registered ahead of their arrival. | Examine a sample of registration documentation to verify that all visitors are registered ahead of their arrival. |
| c) The registration must include name and company they represent. | Examine a sample of registration documentation to verify that registration entries contain the visitor's name and the company they represent. |
| 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. | Examine a sample of documentation evidencing approval by both the physical security manager and the production manager for visitors that required access to the HSA or cloud-based provisioning environment. |
| e) Any unsolicited visitors must be turned away. | Examine CCTV recordings or interview guards to verify that unsolicited visitors are turned away. |
| f) An authorized card production staff member must accompany all visitors at all times while they are in the facility. | Interview the physical security manager to confirm that all visitors are accompanied by an authorized card production staff member at all times while they are in the facility.<br>Observe the CCTV for previous visitors to determine that they were escorted by an authorized card production staff member at all times the visitors were in the facility.<br>Examine documentation to verify procedures require that all visitors must be accompanied by authorized card production staff at all times while within the facility. |
| g) Visitors must enter through the reception area. | Observe live visitor entry processes to verify that all visitors are required to enter through the reception area. |
| ***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:<br>• Confirmation of previously agreed appointment<br>• Verification of identification against an official, government-issued picture ID | Examine documentation for registration of visitors entering the facility to verify the procedures include the procedures listed below.<br>Examine a sample of documentation to verify that it contains evidence of the following:<br>• Confirmation of previously agreed appointment<br>• Verification of identification against an official, government-issued picture ID |

## 1.3 Visitors

| Requirement | Test Procedure |
|---|---|
| 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. | 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. |
| c) All logs must be protected from modification. | Examine the visitor logs to verify that they have protection from modification. |
| d) The following information must be recorded in the logbook:<br>• Name of the visitor, printed and signed<br>• Number of the official ID document(s) presented and the date and place of issue<br>• Company the visitor represents (if any)<br>• Name of the person being visited or in charge of the visitor<br>• Purpose of the visit<br>• Visitor badge number<br>• Date and time of arrival and departure<br>• Signature of the card production staff member initially assigned to escort the visitor | Examine the visitor logs to verify that the entries contain the minimum required information. |
| e) The vendor must retain visitors' registration records for at least 90 days. | Examine the visitor logs to verify entries go back at least 90 days. |
| ***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. | 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.<br>Examine documentation to verify the vendor makes visitors aware of vendor security and confidentiality requirements. |

## 1.3 Visitors

| Requirement | Test Procedure |
|---|---|
| ***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. | 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. |
| 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. | 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. |
| 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:<br>• The visitor must be instructed on its proper use.<br>• 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.<br>• Visitors must use their access card in the card readers to the room into which they enter.<br>• Badging to track access must be used wherever feasible. | 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:<br>• The visitor is instructed on its proper use.<br>• 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.<br>• The visitor must use their access card in the card readers to the room into which they enter.<br>Badging to track visitor access is used wherever feasible. |
| d) Unissued visitor access badges must be securely stored. | Observe the location where unissued visitor access badges are stored to verify that it is a secure location. |
| e) Any un-badged access must be recorded in a log. Logs may be electronic and/or manual. | Examine a sample of visitor logs for entries of any un-badged visitor access to verify existence—e.g., vault or server room access. |
| 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. | 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. |

## 1.4 External Service Providers

| Requirement | Test Procedure |
|---|---|
| ***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. | Examine the security manual to verify that procedures are documented for how third parties are managed at the vendor facility.<br>Interview personnel to verify that the procedures are followed. |
| 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. | 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. |
| 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. | 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.<br>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.<br>Interview the physical security manager or senior management to confirm that they approve any exceptions to this requirement in writing. |
| d) An authorized card production staff member accompanies all external service providers at all times while they are in the HSA(s). | 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).<br>Examine a sample of CCTV footage to verify that procedures are followed. |
| e) All external service providers that require access to HSAs to service equipment have adequate liability insurance. | 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. |
| f) External service providers' staff requiring access to restricted or HSAs follow the visitor-registration procedures. | 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.<br>Examine documentation for a specific external service provider to verify that staff requiring access to restricted areas or HSAs follow the visitor-registration procedures. |

| 1.5 Vendor's Agents | |
|---|---|
| **Requirement** | **Test Procedure** |
| ***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:<br>• Agent's name, address, and telephone numbers<br>• Agent's role or responsibility | 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.<br>Examine a sample of registration documentation to verify it contains the following information:<br>• Agent's name, address, and telephone numbers<br>• Agent's role or responsibility |
| b) The vendor must inform the VPA whenever the agent relationship is changed or terminated. | 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. |
| c) Agents of the vendor are not permitted to be in the possession of a card(s), card components, or card personalization data. | 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.<br>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. |

# Section 2: Facilities

## 2.1 External Structure

| Requirement | Test Procedure |
|---|---|
| ***2.1.1 External Construction*** | |
| a) Procedures for security controls implemented at the vendor facility must be documented and followed. | Examine policy and procedures to verify security controls exist.<br>Interview a sample of personnel to verify they are aware of the security controls policies and procedures and they are followed. |
| 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. | 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.<br>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. |
| 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. | Examine settings of door contacts—electrical or magnetic—to verify they are permanently alarmed and are connected to the security control-room panels.<br>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. |
| 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. | Examine security policy and procedures to verify security controls are in place when door alarms are disabled.<br>Examine security controls to verify procedures are in place for delivery of access key(s) when repair/maintenance staff access technical machinery or equipment.<br>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. |
| e) The vendor must keep a log of the disabling of the alarm and the key exchange, describing at least:<br>• Date<br>• Time<br>• Person(s) needing access<br>• Purpose of the access | Examine a sample of the logs for the activities of disabling the alarm and key exchange.<br>Logs must describe at the minimum:<br>• Date<br>• Time<br>• Person(s) needing access<br>• Purpose of the access |

## 2.1 External Structure

| Requirement | Test Procedure |
|---|---|
| ***2.1.2 Exterior Entrances and Exits*** | |
| All non-emergency exterior entrances and exits to the facility must be: | |
| a) Contact-alarm monitored | Observe the exterior entrances and exits to verify they are contact-alarm monitored. |
| b) Locked or electronically controlled at all times | Observe that all exterior entrances and exits are locked and are controlled at all times. |
| c) Reinforced, where applicable, to resist intrusion—e.g., steel or equivalent construction that meets local fire and safety codes. | 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. |
| d) Fitted with an access-control device—i.e., card reader or biometric—that automatically activates the locking mechanism | 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. |
| e) Fitted with a mantrap or interlocking configuration to prevent staff "piggybacking" or tailgating (excluding emergency exits) | 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). |
| ***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. | 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. |
| 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. | 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. |
| c) HSA windows must be non-openable. | Observe to determine that all external HSA windows are non-openable. |
| ***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. | Observe vendor facility to verify any devices—e.g., carriers, waste containers, and tools—are not against the facility's external wall. |

## 2.2 External Security

| Requirement | Test Procedure |
|---|---|
| a) The vendor facility must be located in an area serviced by public law enforcement and fire protection services in a timely manner. | 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. |
| b) The facility must be secured with an intrusion alarm system as defined in Section 2.4.1, "Alarm Systems." | 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." |
| 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. | 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.<br>Observe that the alarm system is equipped with an auxiliary power or battery backup system with capabilities for ensuring operation. |
| d) All systems must notify the vendor in real time in the event the backup system is invoked. | Examine documentation to verify all systems are to notify the vendor in real time in the event backup systems are invoked.<br>Examine a sample of documentation—e.g., logs—to verify vendors are notified in real time in the event backup systems are invoked. |
| 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. | 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. |
| f) Alarms on external doors must be tested every three months. | Examine a sample of evidentiary matter to verify external doors alarms have been tested every three months. |
| ***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." | Interview personnel to verify that emergency exits are monitored 24 hours a day.<br>Observe via opening each emergency exit door to verify that:<br>• Exits are fitted with local audible alarms and a sign is displayed indicating "emergency exit door with alarm."<br>• Doors are fitted with an automatic closer to ensure self-latching of the door after being opened.<br>• Doors are contact-alarm monitored. |
| b) Emergency exit doors must be fitted with an automatic closer to ensure self-latching of the door after being opened. | |
| c) Emergency exit doors must be contact alarm monitored. | |

## 2.2 External Security

| Requirement | Test Procedure |
|---|---|
| d) These doors must be used only in the event of an emergency and not used for any other purpose. | Examine documents to verify emergency doors are used only in the event of an emergency.<br>Interview personnel to verify that emergency doors are used only in the event of an emergency and not used for any other purpose. |
| 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. | Examine logs to verify security controls are in place for monitoring emergency exits based upon the aforementioned tests. |
| 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. | 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.<br>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. |
| g) Emergency exit doors must not be capable of being opened from the outside. | Observe all emergency exit doors to verify they cannot be opened from the outside.<br>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.). |
| h) Emergency exits must not lead to a higher security area. | Observe that all emergency exits do not lead to a higher security area. |
| ***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. | 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. |
| b) The vendor must check all exterior lights monthly and must maintain a record for 24 months. | Examine a sample of vendor logs to determine that all exterior lights are checked monthly and a record is maintained for 24 months. |
| ***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. | 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. |

## 2.2 External Security

| Requirement | Test Procedure |
|---|---|
| b) All access points into the building from the roof must be locked or otherwise controlled from the inside. | Observe to verify all access points into the building from the roof are locked or otherwise controlled from the inside. |
| c) All access points must have magnetic contacts or contact sensors both of which must have monitored access. | Observe to verify all access points into the building from the roof have magnetic contacts or contact sensors, both of which have monitored access. |
| 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. | 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. |
| ***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. | 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. |
| b) Cameras must be monitored in the security control room during operational hours. | Interview personnel to verify that cameras are monitored in the security control room during operational hours.<br>Observe to verify that cameras are monitored in the security control room during operational hours. |
| ***2.2.5 Signage*** | |
| a) Signage on the exterior of the building must neither indicate nor imply that the vendor processes card products. | Observe that signage on the exterior of the building neither indicates nor implies that the vendor processes card products. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| ***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. | 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. |
| b) The reception area must be within a mantrap.<br>*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.* | Observe that the reception area for visitors is contained within a mantrap. |
| 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. | 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. |
| d) Visitors must be visually inspected in this area to confirm their identity and issued with identification badges before being admitted into the facility. | 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.<br>Interview personnel to validate visitors are visually inspected in the reception area and:<br>• Their identity is confirmed.<br>• They are issued identification badges before being admitted into the facility. |
| 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. | Examine documents to verify procedures are in place describing the process by which visitors are granted access to the facility and they stipulate that:<br>• Only authorized staff can bring visitors into the facility<br>• The list is maintained at the reception area.<br>• Only people on the list are allowed to bring visitors into the facility.<br>Examine evidence to verify that only authorized staff have been allowed to bring visitors into the facility. |
| 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. | 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.<br>Observe to verify visitor(s) wear an ID badge at all times while inside the facility. |
| g) The electronic control points for operating this system must be located at the receptionist's desk or in the security control room. | 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. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| 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. | 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:<br>• Reinforced, and<br>• 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. |
| 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. | Examine evidence that personnel working in these areas have at a minimum:<br>• A telephone<br>• A duress button that activates a silent alarm at a remote, central monitoring service or police station. |
| 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. | 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. |
| 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. | 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.<br>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. |
| 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. | Observe to verify that card production staff are entering the facility through the main entrance area or through an employee-only entrance.<br>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. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| ***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. | Examine policy and procedures to verify that the room is staffed at all times while activity occurs in the HSA.<br>Interview personnel to verify that the room is staffed at all times while activity occurs in the HSA.<br>Observe random CCTV recordings of the security control room when activity occurs in the HSA.<br>Examine access-control logs to verify the SCR was not left unoccupied. |
| 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. | Observe the location of the security control room to verify that it is located outside of the HSA and cloud-based provisioning environment. |
| c) Build the security control room of concrete block or other material offering similar resistance, if not part of the facility. | 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. |
| d) Protect the room by an internal motion detector. | Observe the security control room to determine it is protected by an internal motion detector. |
| 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. | 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.<br>Examine a sample of logs to verify all accesses and exits are being recorded.<br>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. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| 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). | 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). |
| 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). | Examine system configuration and interview personnel or observe a demonstration to verify the systems works as described:<br>• An alarm is generated if movement is detected inside the room when the software counter is zero (nobody registered in the room).<br>• 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).<br>• 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). |
| 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). | See g) above. |
| 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. | Observe to verify that the door is fitted with an automatic closing device.<br>Observe to verify that when the door is opened for more than 30 seconds an automatically activated alarm sounds.<br>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.<br>Examine evidence, if applicable, of how procedural controls are used for person-by-person access. |
| j) Ensure that each individual entering or exiting completes the full cycle of badging in and badging out. | Observe the process to validate each individual entering or exiting to verify the full cycle of badging in and badging out is followed.<br>Examine a sample of logs to verify that each individual entering or exiting completed the full cycle of badging in and badging out. |
| k) Equip the security control room with two independent means of communication. | Observe that the security control room is equipped with two independent means of communication. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| 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. | 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.<br>Observe that the access-control monitor displays the access transactions on a real-time basis.<br>Observe the guards cross-check the access-control records with the CCTV images. |
| m) Train guards in the security control room in the effective use of the access-control system and CCTV system facility. | Examine training documents to verify inclusion of training for the effective use of the access-control system and CCTV system facility.<br>Examine training activity logs to verify all guards have gone through training. |
| n) Ensure that a security guard is assigned to watch real-time CCTV images on the monitors. | 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. |
| 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. | 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.<br>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. |
| p) Equip any other external-facing windows with bullet-resistant glass and mirror filming sufficient to prevent any observation from outside the building. | 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.<br>Examine documentation to validate the bullet-resistance of any other external-facing windows. |
| 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. | 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. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| 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. | 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.<br>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. |
| s) Ensure that security room windows are non-openable. | Observe to verify that security control room windows are non-openable. |
| t) Ensure that when the room is used for reception control, the conditions outlined in Section 2.3.1, “Reception,” apply. | 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.<br>Interview personnel to verify procedures are following when the room is used for reception control. |
| 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. | Observe that the CCTV and access-control servers are in the security control room or a room with equivalent security.<br>Observe that the servers are not in the HSA. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| ***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:<br>• Card manufacturing<br>• Chip embedding<br>• Personalization<br>• Storage<br>• Packaging<br>• Mailing<br>• Shipping or delivery<br>• Fulfillment<br>• HCE and SE mobile provisioning | Examine documentation to verify that the activities listed below only occur within the HSA.<br>Observe to verify that the activities listed below, at a minimum, take place within the HSA and only within the HSA.<br>Interview personnel to verify the activities listed below only occur within the HSA.<br>• Card manufacturing<br>• Chip embedding<br>• Personalization<br>• Storage<br>• Packaging<br>• Mailing<br>• Shipping or delivery<br>• Fulfillment<br>• HCE and SE mobile provisioning |
| b) Card production staff may only bring items related to card production and provisioning activity into the HSA. | 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.<br>Observe that card production staff are only allowed to bring items related to card production and provisioning activity into the HSA.<br>Interview personnel to verify that card production staff are only allowed to bring items related to card production and provisioning activity into the HSA. |
| 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. | Examine documentation of HSA design to verify that if the facility performs multiple production activities, they are performed in separate areas within the HSA.<br>Observe to verify that if the facility performs multiple production activities, they are performed in separate areas within the HSA.<br>Interview personnel to verify that if the facility performs multiple production activities, they are performed in separate areas within the HSA. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| d) With the exception of mobile provisioning, if multiple HSAs are within the same building, they must be contiguous. | Examine documentation to verify that if multiple HSAs are within the same building, they are contiguous, with the exception of mobile provisioning.<br>Observe to verify that if multiple HSAs exist within the same building, they are contiguous, with the except of mobile provisioning. |
| e) Equipment that is purely associated with test activities is not allowed in the HSA. | Interview personnel to verify equipment that is associated with test activities is not allowed in the HSA.<br>Observe that equipment associated with test activities is not allowed in the HSA. |
| 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. | 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.<br>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. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| ***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. | Examine policy and procedures to verify that access controls to the HSA are in place.<br>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.<br>Observe that access to the HSA is restricted to authorized persons through an access-control system, working on a strict person-by-person basis. |
| b) Access-control systems must:<br>• Always be connected to the computer that monitors and logs all staff and visitor movements.<br>• Prevent personnel from piggybacking.<br>• Enforce person-by-person access.<br>• Implement anti-pass-back mechanisms.<br>• 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. | Examine access-control systems documentation to verify that they:<br>• Are always connected to the computer that monitors and logs all staff and visitor movements.<br>• Prevent personnel from piggybacking.<br>• Enforce person-by-person access.<br>• Implement anti-pass-back mechanisms.<br>• 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.<br>Observe access-control systems to verify that they:<br>• Are always connected to the computer that monitors and logs all staff and visitor movements.<br>• Prevent personnel from piggybacking.<br>• Enforce person-by-person access.<br>• Implement anti-pass-back mechanisms.<br>• 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. |
| c) The vendor must program the software access-control system, whereby access is on a person-by-person basis and restricted to authorized personnel. | 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. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| d) The access-control system must activate the alarm system each time the last person leaves the HSA. | Examine access-control system settings to verify the access-control system will activate an alarm system each time the last person leaves the HSA.<br>Examine a sample of logs to verify that the access-control system activated the alarm system each time the last person left the HSA. |
| 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. | 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.<br>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). |
| 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. | 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.<br>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). |
| 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. | Examine documentation policy and procedures to verify that:<br>• The alarm is a local sound alarm;<br>• Notification (silent and/or audible alarm) occurs within the security control room; and<br>• After working hours, a simultaneous alarm to the local external security company or local police occurs.<br>Observe that the warning is a local sound alarm and notification (silent and/or audible alarm) occurs within the security control room. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| 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. | Examine documentation to validate what is allowed and not allowed in the HSA. This includes but not limited to:<br>• 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.<br>• No personal food or beverages are allowed.<br>• Medical items such as medications and tissues are acceptable if in clear containers that can be examined.<br>Interview personnel to verify policy is being followed.<br>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 exiting the HSA. |
| 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. | 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.<br>Observe to verify that the access-control server is not located in the HSA. |
| **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. | Observe to verify that access is enforced by the use of an air lock, single sluice, or security turnstile.<br>Examine security settings to verify that access controls are activated by logical means, ensuring strict compliance with the person-by-person mandate.<br>Observe via demonstration the person-by-person access control, by attempting for two personnel to cross the control point together. |
| b) Activation of the access device must be controlled by a card reader that enforces an anti-pass-back function. | Examine settings to verify activation of the access device is controlled by a card reader that enforces an anti-pass-back function.<br>Observe via demonstration that activation of the access device is controlled by a card reader that enforces an anti-pass-back function. |
| c) The card readers must be permanently connected to a computer that centralizes the logging of any card reader activation. | Observe to verify the card readers are permanently connected to a computer that centralizes the logging of any card reader activation.<br>Examine a sample of logs to verify the computer is the centralized mechanism that is logging all card reader activations. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| d) The status of the access must change only when the person has successfully completed the access cycle. | Examine access-control settings to verify that the status of access changes only when the person has successfully completed the access cycle.<br>Examine a sample of logs to verify the status of access changes only when the person has successfully completed the access cycle. |
| **2.3.4.3 Transfer of Physical 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. | 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.<br>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. |
| 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. | Observe that a goods-tools trap or similar mechanism is used to transfer physical materials between different HSAs. |
| **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. | Examine documentation to verify bullet-resistant—e.g., UL 752—glass or iron bars protects all windows in HSAs.<br>Observe that bullet-resistant glass or iron bars are used to protect all windows in HSAs. |
| 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. | 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.<br>***Note:*** *See Annex A for further clarification.* |
| 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. | 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.<br>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. |
| d) All access points—e.g., electrical conduits, opening windows, and ventilation shafts—in HSAs must have physical barriers. | Examine documentation to verify that all access points—e.g., electrical conduits, opening windows, and ventilation shafts—in/to the HSAs have physical barriers.<br>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. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| 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. | 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.<br>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. |
| f) The entire HSA must be covered by CCTV as defined in Section 2.4.5, "Closed Circuit Television (CCTV)." | Examine security-control documentation to verify the HSA has CCTV coverage as defined in Section 2.4.5, "Closed Circuit Television (CCTV)."<br>Observe to verify the HSA is covered by CCTV as defined in Section 2.4.5, "Closed Circuit Television (CCTV)." |
| 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. | Examine access-control system settings to validate audible alarms sound if the door or gate remains open for more than 30 seconds.<br>Observe that all doors and gates to these areas are contact monitored and fitted with automatic closing or locking devices.<br>Examine a sample of logs to verify the audible alarms are sounded if the door or gate remains open for more than 30 seconds. |
| 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. | 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.<br>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. |
| i) Doors must not open directly to the building's exterior unless they are alarmed emergency exit doors. | Observe to verify that doors do not open directly to the building's exterior unless they are alarmed emergency exit doors. |
| 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." | Observe emergency exits to verify they:<br>• Are fitted with local audible alarms.<br>• Display a sign indicating "emergency exit door with alarm."<br>• Are monitored 24 hours a day. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| **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. | Observe via demonstration the access-control system by requesting that one authorized person authenticates to the access reader:<br>• If the door opens, does a "single occupancy" alarm sound within a 60-second period?<br>• If the door does not open, verify that it opens after two authorized authentications have been presented. |
| ***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. | Examine HSA documentation to verify separate rooms within the HSA meet all of the HSA requirements with the exception of person-by-person access.<br>Observe that separate rooms within the HSA meet the HSA requirements with the exception of person-by-person access. |
| b) Toilet rooms are prohibited except where required by local law. Where used, the entry/exit way must be camera-monitored. | Examine documentation to verify that toilets, if present, are required by local law.<br>Observe to determine that, if present, the toilet room's entry/exit ways are camera-monitored. |
| 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. | 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. |
| 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. | 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. |
| **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. | Observe to verify that the pre-press process is performed in a separate room within the HSA. |
| b) The pre-press room is where the vendor produces or stores film, plates, or electronic media. | Observe to verify that the pre-press room is the location where the vendor stores film, plates, or electronic media. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| **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. | Observe the WIP storage room to verify it is segregated from production and is protected by at a minimum by wire mesh. |
| 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). | 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). |
| 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. | 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. |
| 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). | 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).<br>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). |
| e) CCTV surveillance is mandatory and must cover the entire area, ensuring that there are no blind spots. | Observe CCTV surveillance camera video to determine that coverage exists for the entire area, ensuring that there are no blind spots. |
| **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. | 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. |
| 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. | Examine documentation to verify that destruction by a third party takes place in the loading bay using portable/mobile equipment.<br>Examine a sample of video logs to verify all requirements for a destruction room are met for this temporary usage.<br>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. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| **2.3.5.4 PIN Mailer Production Room** | |
| a) PIN mailer production must be performed in a separate room within the HSA. | Observe to verify that PIN mailer production is performed in a separate room within the HSA. |
| 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. | 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.<br>Interview personnel to determine procedures are followed as stated. |
| 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. | Examine procedures to verify that personnel involved in personalization are never involved in PIN printing of the associated cards.<br>Interview personnel involved in personalization to verify they are never involved in PIN printing of the associated cards. |
| 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. | Examine documentation to verify PIN mailer procedures exist.<br>Examine a sample of PIN mailers to verify:<br>• PIN mailers are printed in such a way that the plaintext PIN cannot be observed until the envelope is opened.<br>• The envelope displays the minimum data necessary to deliver the PIN mailer to the correct customer.<br>• PIN mailers are tamper-evident so that it is highly likely that accidental or fraudulent opening will be obvious to the customer. |
| e) PIN mailers must be mailed as defined in Section 4.5, “Delivery.” | Examine a sample of logs to verify PIN mailers are mailed as defined in Section 4.5, “Delivery.”<br>Observe to verify that PIN mailers are mailed as defined in Section 4.5, “Delivery.” |
| f) No activity other than PIN mailer production may take place in the room. | Interview personal to verify that no activity other than PIN mailer production takes place in the room.<br>Observe to verify that no activity other than PIN mailer production takes place in the room. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| g) All re-runs of jobs to print PINs must be pre-approved in writing by management. | Examine policy and procedures to verify that re-runs of jobs to print PINs are pre-approved in writing by management.<br>Examine a sample of logs to verify that re-runs of jobs to print PINs are pre-approved in writing by management. |
| h) Reports and PIN mailers must not display printed PIN data in the clear. | Examine a sample of Reports and PIN mailers to verify that printed PIN data is not displayed in the clear. |
| i) PIN mailers must not contain the associated cardholder account number. | Examine a sample of PIN mailers to verify that they do not contain the associated cardholder account number. |
| j) PIN mailers must be stored in the vault or the PIN printing room prior to shipment. | Interview personnel to validate that PIN mailers are stored in the vault or the PIN printing room prior to shipment.<br>Observe that PIN mailers are stored in the vault or the PIN printing room prior to shipment. |
| k) All waste material from the PIN-printing process must be destroyed as defined in Section 3, "Production Procedures and Audit Trails." | 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."<br>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."<br>Observe that all waste material from the PIN-printing process is destroyed as defined in Section 3, "Production Procedures and Audit Trails." |
| **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. | Observe to verify server processing, key management, and data preparation are performed in a separate room within the personalization HSA. |
| 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.<br>*For example, in a traditional card vendor environment this could be:*<br>• *A separate rack in a server room, or*<br>• *In a provisioning-only entity, housed in a separate room or cage in a data center.* | Observe the location where cloud-based provisioning network components are located to verify the servers, firewalls, and HSMs are:<br>• 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<br>• In a provisioning-only entity, housed in a separate room or cage in a data center. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| 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. | 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. |
| 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. | Observe that internal CCTV cameras:<br>• Are installed to cover the access to the key-management and server room.<br>• Provide an overview of the room.<br>• Are positioned in such a manner to not allow observation of keystroke entry or the monitoring of the screen. |
| 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. | Examine CCTV camera settings to verify configurations of the cameras do not have zoom or scanning functionality. |
| **2.3.5.6 Vault**<br>*The vault is the primary security area in the vendor facility.* | |
| a) The following must be stored in the vault:<br>• Cards awaiting personalization<br>• Security components<br>• Materials awaiting destruction<br>• Samples and test cards prior to distribution and after return<br>• Any card that is personalized with production data<br>• If the facility is closed, personalized cards that will not be shipped within the same working day<br>• Products awaiting return to the supplier | d) Examine documentation to verify the following, at a minimum, are to be stored in the vault:<br>• Cards awaiting personalization<br>• Security components<br>• Materials awaiting destruction<br>• Samples and test cards prior to distribution and after return<br>• Any card that is personalized with production data<br>• If the facility is closed, personalized cards that will not be shipped within the same working day<br>• Products awaiting return to the supplier<br>Observe the contents of the vault to verify that the aforementioned are stored in the vault. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| 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.<br><br>***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.* | 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).<br><br>Observe the vault to verify the design is constructed as required. |
| i. An outside wall of the building must not be used as a wall of the vault. | Observe to verify that an outside wall of the building is not used as a wall of the vault. |
| 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. | 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.<br><br>Examine evidence to verify that any small (dead) space between the vault and the outside wall is constantly monitored for intrusion. |
| iii. No windows are permitted. | Observe to verify that no windows are in the vault. |
| 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. | Observe access to the vault to verify the following exist to protect access to the vault:<br>• 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<br>• Access to the vault is only through vault doors and gates configured with intruder-detection devices. |
| 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. | Observe to verify the protection of the vault includes but is not limited to:<br>• 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.<br>• 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. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| 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. | Examine procedures to verify opening and closing of the main vault door is always under dual control.<br>Examine a sample of logs to verify opening and closing the main vault door is always under dual control.<br>Observe the opening and closing of the main vault door to verify it is under dual control. |
| 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. | Observe (if the vault door is required to remain open during production hours) to verify:<br>• An inner grille is used<br>• 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.<br>• The inner grille meets the same access-control criteria as other rooms within the HSA. |
| 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. | Observe that the vault door or the inner grille are equipped with:<br>• An automatic closing device<br>• An automatically activated simultaneous sound alarm that will be heard locally and in the security control room, if opened for more than 60 seconds.<br>Observe sample documents—e.g., logs—to verify the existing controls are in place. |
| 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. | Examine documentation to verify emergency exit doors from the vault to the HSA:<br>• Meet the strength requirements for a vault door.<br>• Have alarms.<br>• Are not capable of being opened from outside.<br>Observe to verify emergency exit doors meet the requirements in place. |
| g) Card components being taken in or out must be recorded in a vault log and confirmed by at least two card production staff. | 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.<br>Interview personnel to verify procedures are followed. |
| 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. | 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. |

## 2.3 Internal Structure and Processes

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

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| ***2.3.6 Other Areas*** | |
| **2.3.6.1 Goods-tools Traps**<br>*Goods-tools trap configuration options are as follows:* | |
| a) One-room configuration:<br>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.<br>In this configuration, the goods-tools trap must be operated as follows:<br>• The movement detector is deactivated when someone swipes the access card in the card reader.<br>• The person opens the door, introduces the package, and closes the door.<br>• 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.<br>• 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. | Observe good tools trap configuration:<br>• If a one room configuration is used, perform test procedures for Requirement a).<br>• If a two-room configuration is used, perform the test procedures for Requirement b) below.<br>Observe the room configuration to verify the goods-tools trap one-room is configured and operated as follows:<br>• 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.<br>• Movement detector is deactivated when someone swipes the access card in the card reader.<br>• The person opens the door, introduces the package, and closes the door.<br>• Movement detector is reactivated automatically, so any person inside the goods-tools trap is detected.<br>• If someone is detected, the cycle cannot be completed, and the other goods-tools trap door cannot be opened to take the package back.<br>• 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. |
| b) Two-room configuration:<br>• In this configuration, the goods-tools trap is composed of two consecutive rooms, similar to the classical shipping and delivery room configuration.<br>• Security requirements, protection devices, and access procedures are the same as for the standard shipping and delivering area configuration, as defined below. | Observe to verify it is configured and operated as follows:<br>• Goods-tools trap is composed of two consecutive rooms, similar to the classical shipping and delivery room configuration.<br>• Security requirements, protection devices, and access procedures are the same as for the standard shipping and delivering area configuration, as defined below. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| **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.<br>***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.* | Observe to verify the shipping and delivery areas (loading/unloading) of card components to have at a minimum:<br>• At least two consecutive enclosed rooms and three doors (external, intermediate, and inner), and<br>• Minimization of physical contact between the individuals collecting or delivering materials and the shipment/delivery card production staff. |
| 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. | 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. |
| c) An intercom communications system must be contained in this area to allow identification of incoming drivers. | Observe to verify that an intercom communications system is operational in this area to allow identification of incoming drivers. |
| 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. | Observe to verify that one of the rooms in the shipping area:<br>• Contains a solution to allow the exchange of control documents without coming into contact with external personnel; and<br>• Allows communication with and visual identification of external personnel. |
| 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. | 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.<br>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. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| 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. | 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.<br>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.<br>Interview a sample of guards and other personnel to verify that procedures are followed. |
| 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. | 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.<br>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.<br>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. |
| 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. | 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.<br>Examine either a logical (software) or a physical (alarm report book) log of such events to validate a record is kept for at least two years. |
| 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. | 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.<br>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. |

## 2.3 Internal Structure and Processes

| Requirement | Test Procedure |
|---|---|
| j) The vendor must install at least:<br>• One external CCTV camera covering the external shipping and delivery area door and its environment<br>• Two CCTV cameras inside the outer room covering all sides of the vehicle<br>• One CCTV camera inside the inner room covering the shipping and delivery operations | Observe to verify the CCTV cameras from the security control room have been installed to cover at a minimum:<br>• One external CCTV camera covering the external shipping and delivery area door and its environment<br>• Two CCTV cameras inside the outer room covering all sides of the vehicle<br>• One CCTV camera inside the inner room covering the shipping and delivery operations |
| 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. | 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. |
| 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. | 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. |

## 2.4 Internal Security

| Requirement | Test Procedure |
|---|---|
| ***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. | 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. |
| 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. | 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.<br>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. |
| c) The system must notify the vendor in real time in the event the backup system is invoked. | 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.<br>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.<br>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. |
| 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. | Examine alarm policy and procedures to verify at a minimum:<br>• 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.<br>• The alarm deactivation process allows for the generation of a fast, silent alarm in case of threat.<br>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.<br>Interview personnel to verify the alarm deactivation process allows for the generation of a fast, silent alarm in case of threat. |

## 2.4 Internal Security

| Requirement | Test Procedure |
|---|---|
| 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. | 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.<br>Interview personnel to verify they are knowledgeable of and able to execute the procedure. |
| ii. Alarm activation and deactivation codes must be known only by guards or security team members authorized to use them. | Interview personnel to verify alarm activation and deactivation codes are known only by the guards or security team members authorized to use them.<br>Examine documentation to verify alarm activation and deactivation codes are known only by the card production staff authorized to use them. |
| iii. Codes must be deactivated upon termination of any guards or security team members with knowledge of the code. | Interview personnel to verify alarm activation and deactivation codes are deactivated upon termination of any staff with knowledge of the code.<br>Examine documentation to verify alarm activation and deactivation codes are deactivated upon termination of any staff with knowledge of the code. |
| 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. | 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.<br>Interview guards and card production staff to verify they know the procedures in case of an alarm system activation.<br>Examine a sample of training materials to verify guards and card production staff know the procedures in case of an alarm system activation. |
| 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. | 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.<br>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.<br>Observe a demonstration of someone badging in and badging out, but not actually egressing the restricted area to verify the detection works. |

## 2.4 Internal Security

| Requirement | Test Procedure |
|---|---|
| ***2.4.2 Access-Control System Administration*** | |
| **2.4.2.1 Identification Badges** | |
| a) Procedures must be documented and followed for managing identification (ID) badges. | Examine badging administration documentation to verify procedures are defined for managing ID badges.<br>Examine a sample of logs to verify procedures are followed in managing ID badges. |
| 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. | Examine documented procedures to verify the vendor issues a photo identification badge to each card production staff member and consultant.<br>Examine a sample of logs to verify badge issuance to card production staff and consultants. |
| 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. | 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. |
| d) Access credentials (which may be the ID badge) must be programmed only for the access required based on job function. | 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.<br>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.<br>Interview personnel to verify access is required based on job function. |
| **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. | 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.<br>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.<br>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. |
| b) Personnel must display their ID badges at all times while in the facility. | Observe that personnel display their ID badges at all times while in the facility. |

## 2.4 Internal Security

| Requirement | Test Procedure |
|---|---|
| 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. | Examine documentation to verify policies and procedures address but are not limited to:<br>• Card production staff and consultants are responsible for securing their ID badge from loss or theft.<br>• If an individual determines his/her ID badge has been lost or misplaced, they must notify the physical security manager immediately.<br>Interview personnel to verify they have knowledge to report any lost/stolen or broken badges to the physical security manager immediately.<br>Examine sample reports to verify lost/stolen or broken badges have been reported to the security manager. |
| 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. | 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. |
| **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. | Examine the unassigned badge inventory log to verify completeness. |
| b) Ensure dual control exists for badge access and distribution to individuals. | Examine procedures to validate a process is in place to have dual control for badge access and distribution to individuals.<br>Examine a sample of logs to verify dual control for badge access and assignments. |
| c) Ensure ID badges are retrieved from terminated individuals prior to their departure from the facility. | Examine procedures to validate a process is in place to retrieve ID badges from terminated individuals prior to their departure from the facility.<br>Examine a sample of terminated personnel documentation to verify ID badges were retrieved from each terminated individual prior to their departure from the facility. |
| d) Ensure all access rights are immediately deactivated. | Examine procedures to validate a process is in place to deactivate all access rights immediately on a departure of an individual.<br>Examine a sample of terminated personnel documentation to verify all access rights were immediately deactivated. |

## 2.4 Internal Security

| Requirement | Test Procedure |
|---|---|
| e) Maintain precise documentation accounting for all lost badges. | Examine documentation to verify a process is in place to maintain documentation to account for all lost badges.<br>Examine a sample of documentation to verify existence of an audit trail of all lost badges. |
| ***2.4.3 Access-Control System*** | |
| a) The vendor must document, follow, and maintain procedures for access-control system administration. | Examine policy and procedures to verify access-control system administration is documented and maintained.<br>Interview personnel to verify personnel follow the procedures for access-control system administration. |
| 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. | 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.<br>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. |
| c) Contingency plans must exist for securing card components in the event of an outage greater than 48 hours. | Examine contingency plans to verify procedures exist to secure card components in the event of an outage greater than 48 hours.<br>Interview personnel to verify procedures are known and followed for securing card components in the event of an outage greater than 48 hours. |
| 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. | 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.<br>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. |

## 2.4 Internal Security

| Requirement | Test Procedure |
|---|---|
| **2.4.3.1 Activity Reports** | |
| a) All procedures for access control must be documented and kept current. | Examine documentation to verify access-control procedures exist and are current.<br>Interview the access-control system administrator to validate access documents are current. |
| b) The access-control system must log sufficient information to produce the daily card activity reports detailed below:<br>• Card reader<br>• Card reader status<br>• Card identification<br>• Date and time of access<br>• Access attempts results<br>• Unauthorized attempts<br>• Anti-pass-back violation and corrective actions taken<br>• Access-control system changes describing:<br>– The date and time of the change,<br>– The reasons for the change, and<br>– The person who made the change. | Examine a sample of access-control system logs to verify they contain the following information at a minimum:<br>• Card reader<br>• Card reader status<br>• Card identification<br>• Date and time of access<br>• Access attempts results<br>• Unauthorized attempts<br>• Anti-pass-back violation and corrective actions taken<br>• Access-control system changes describing:<br>– The date and time of the change,<br>– The reasons for the change, and<br>– The person who made the change. |
| c) The physical security manager must review these reports weekly. | Examine evidence that the physical security manager is reviewing reports weekly. |
| d) The access-control system audit trail must be maintained for at least three months. | Examine access-control system setting to verify that audit trails are enabled and are kept for three months.<br>Examine a sample of reports to verify the access-control system audit trail is maintained for at least three months. |

## 2.4 Internal Security

| Requirement | Test Procedure |
|---|---|
| **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. | Examine access-control system documentation to validate each access-control system administrator uses his or her own user ID and password.<br>Interview personnel to verify that each access-control system administrator uses his or her own user ID and password. |
| b) Passwords are changed at least every 90 days. | Examine documentation to verify procedures are in place that passwords are changed at least every 90 days.<br>Examine a sample of system configurations to verify passwords required to be changed at least every 90 days.<br>Interview personnel to verify that passwords are changed at least every 90 days. |
| c) User IDs and passwords are assigned to the physical security manager and authorized personnel, who must be employees. | Examine documentation to verify that user IDs and passwords are assigned to the physical security manager and authorized personnel<br>Interview personnel to verify that access-control system administrators are vendor employees.<br>Examine a sample of logs to verify user IDs and passwords are assigned to the physical security manager and authorized personnel. |
| 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. | 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.<br>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. |
| e) At the end of each session, the individual who initiated the session must log off the system. | 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. |

## 2.4 Internal Security

| Requirement | Test Procedure |
|---|---|
| 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. | 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.<br>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.<br>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. |
| g) Access-control systems are physically and logically isolated on a dedicated network from the main office network. | Interview personnel to verify that the access-control systems are physically and logically isolated on a dedicated network from the main office network. |
| **2.4.3.3 Remote-access Controls** | |
| a) Offsite access to the access-control system is not permitted. | Examine documentation to verify that the remote-access requirements listed below are met where system administration is performed remotely.<br>Examine a sample of reports to verify system administrators follow requirements for remote access as stipulated below.<br>Examine documentation to verify vendor facilities not subject to logical security audits have a written statement that requirements are being met.<br>Interview personnel to verify that the following remote-access requirements are met where system administration is performed remotely:<br>• Offsite access to the access-control system is not permitted.<br>• Access-control system data must be backed up on a weekly basis.<br>• Access-control systems administration must be performed from within the security control room.<br>• 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.<br>• In addition, the access-control system must meet the logical security requirements in Appendix B. |
| b) Access-control system data must be backed up on a weekly basis. | |
| c) Access-control systems administration must be performed from within the security control room. | |
| 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. | |
| e) In addition, the access-control system must meet the logical security requirements in Appendix B. | |

## 2.4 Internal Security

| Requirement | Test Procedure |
|---|---|
| ***2.4.4 Duress Buttons*** | |
| **2.4.4.1 Location** | |
| Duress buttons must be located in the following areas: | |
| a) Reception | Observe that duress buttons are located in the following areas:<br>• Reception<br>• Security control room<br>• The vault<br>• Shipping and delivery area<br>• Every card production staff entrance |
| b) Security control room | |
| c) The vault | |
| d) Shipping and delivery area | |
| e) Every card production staff entrance | |
| **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. | 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:<br>• A warning or emergency signal is sent to an on-site security control room.<br>• A remote central monitoring station, or the local police station.<br>• The anticipated initial response—i.e., event verification—is within two minutes. |
| 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:<br>• Time and date when the duress button was activated<br>• Time taken by the remote central monitoring service to respond<br>• Time taken by the police or other help to respond/arrive on site<br>• Chronology of all related activities, including names of personnel involved<br>• Reason for activating alarm | 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.<br>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:<br>• Time and date when the duress button was activated<br>• Time taken by the remote central monitoring service to respond<br>• Time taken by the police or other help to respond/arrive on site<br>• Chronology of all related activities, including names of personnel involved<br>• Reason for activating alarm |

## 2.4 Internal Security

| Requirement | Test Procedure |
|---|---|
| **2.4.4.3 Testing** | |
| a) All duress buttons must be tested, and the results documented on a quarterly basis. | Examine a sample of logs to verify quarterly tests are performed on all duress buttons and that the results are documented. |
| ***2.4.5 Locks and Keys*** | |
| **2.4.5.1 Key Receipt and Return**<br>*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. | Examine documentation to verify that key-management procedures exist and are followed.<br>Interview personnel to verify that key-management procedures are known and are followed.<br>Examine sample documents to validate key-management procedures are followed. |
| 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. | Examine procedures for issuance of keys and the requirement that they be entrusted to authorized personnel.<br>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. |
| c) All unissued keys, master keys, and duplicate keys must be maintained under dual control in a safe or secure cabinet. | Examine policy and procedures that all unissued keys, master keys, and duplicate keys are maintained under dual control in a safe or secure cabinet.<br>Interview personnel to verify unissued keys, master keys, and duplicate keys are maintained under dual control.<br>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. |
| d) Any transfer of responsibility between the staff issuing the key and the key recipient must be recorded in a specific key logbook. | 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.<br>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. |

## 2.4 Internal Security

| Requirement | Test Procedure |
|---|---|
| **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:<br>• Key identification number<br>• Date and time the key is issued (transfer of responsibility)<br>• Name and signature of the card production staff member issuing the key<br>• Name and signature of the authorized recipient<br>• Date and time the key is returned (transfer of responsibility)<br>• Name and signature of the authorized individual returning the key<br>• Name and signature of the card production staff member receiving the key | Examine documentation to verify procedures require the key logbook to contain the information listed below at a minimum.<br>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:<br>• Key identification number<br>• Date and time the key is issued (transfer of responsibility)<br>• Name and signature of the card production staff member issuing the key<br>• Name and signature of the authorized recipient<br>• Date and time the key is returned (transfer of responsibility)<br>• Name and signature of the authorized individual returning the key<br>• Name and signature of the card production staff member receiving the key |
| 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. | 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.<br>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. |
| c) For keys that allow access to sensitive materials, the physical security manager must conduct a quarterly review of:<br>• The key logbook<br>• The list of card production staff authorized to hold keys<br>• The locks each key operates | 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.<br>• The key logbook<br>• The list of card production staff authorized to hold keys<br>• The locks each key operates<br>Examine evidence that for keys that allow access to sensitive materials, the physical security manager performed a quarterly review of:<br>• The key logbook<br>• The list of card production staff authorized to hold keys<br>• The locks each key operates |

## 2.4 Internal Security

| Requirement | Test Procedure |
|---|---|
| d) The physical security manager must sign and date each of the key-control documents, attesting that the review process was completed. | Examine documentation to verify a process is in place for the physical security manager to, at a minimum:<br>• Sign and date each of the key-control documents; and<br>• Attest that the review process was completed.<br>Examine a sample of records to verify the physical security manager performed the key-control process as noted above. |
| **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. | 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.<br>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. |
| **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. | 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.<br>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. |
| ***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. | Examine documentation to verify CCTV procedures are documented.<br>Interview personnel to verify they are aware of and follow the CCTV procedures.<br>Examine a sample of documents to verify CCTV media are managed per the policy. |

## 2.4 Internal Security

| Requirement | Test Procedure |
|---|---|
| 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. | 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.<br>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.<br>Interview security personnel and examine evidence to verify that:<br>• Cameras are tested and monitors checked at least monthly to confirm clarity of images.<br>• Records of such testing are retained for a minimum of two years. |
| 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. | 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.<br>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<br>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. |
| 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. | 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. |
| e) The recording system must be able to replay any recorded sequence without stopping the normal recording operation. | Observe a sample of CCTV media to verify the recording system is able to replay any recorded sequence without stopping the normal recording operation. |
| f) CCTV cameras in server rooms and PIN-mailer rooms must not contain (or must have disabled) zoom or scanning functionality. | Examine CCTV camera settings located in server rooms and PIN-mailer rooms to verify zoom or scanning functionality are disabled.<br>Observe that CCTV cameras in server rooms and PIN-mailer rooms do not contain (or have disabled) zoom or scanning functionality. |

## 2.4 Internal Security

| Requirement | Test Procedure |
|---|---|
| **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. | Examine each monitor, camera, and digital recorder settings and documentation to verify that camera recordings provide the following at a minimum:<br>• Four (4) picture frames per second on motion or four (4) picture frames per second permanently; and<br>• Clear images on the monitor without being out-of-focus, blurred, washed out, or excessively darkened. |
| 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. | Examine CCTV camera settings and documentation to verify that camera recordings—e.g., via motion activation—provide a minimum of the requirements listed below.<br>Observe a demonstration (including dark periods) to verify the CCTV that camera recordings—e.g., via motion activation—provide a minimum of:<br>• Recording to capture any motion at least five seconds before and after the detected motion.<br>• 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. |
| c) CCTV monitors and recorders must be located in an area that is restricted from unauthorized personnel. | Observe that CCTV monitors and recorders are in a location restricted from unauthorized personnel. |
| d) CCTV cameras must be connected at all times to:<br>• Monitors located in the control room<br>• An alarm system that will generate an alarm if the CCTV is disrupted<br>• An active image-recording device | Observe that CCTV cameras are connected (via a list of known cameras) and active at all times to but not limited to:<br>• Monitors located in the control room<br>• An alarm system that will generate an alarm if the CCTV is disrupted<br>• An active image-recording device |
| **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. | 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. |
| 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. | 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. |
| c) Each internal CCTV camera and recording system must be equipped with an automatic recording capability in case of an alarm event. | 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. |

## 2.4 Internal Security

| Requirement | Test Procedure |
|---|---|
| **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. | Examine documentation and a sample of archived video to verify CCTV images are:<br>• Kept for at least 90 days;<br>• Backed up daily; and that<br>• Both primary and backup copies exist for a minimum of 90 days. |
| 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. | Examine documentation to verify backup recording and storage requirements exist.<br>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.<br>Interview personnel to verify that segregation of duties exists between the users and the system administrators. |
| **2.4.6.5 System Administration** | |
| a) The CCTV system must meet the logical security requirements in Appendix B. | See Appendix B. |

## 2.4 Internal Security

| Requirement | Test Procedure |
|---|---|
| ***2.4.7 Security Device Inspections*** | |
| *See Appendix B: "Logical Security Requirements – CCTV and Access-Control System Administration" for CCTV system criteria.* | |
| **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:<br>• Alarm system<br>• Access-control system<br>• Window and door contacts<br>• Glass-break detectors<br>• Emergency door alarms<br>• Passive infrared detectors<br>• Microwave sensors<br>• CCTV monitors<br>• CCTV image recorders | Examine documentation to verify inspections on all security devices and hardware were performed at least semi-annually and include but were not limited to:<br>• Alarm system<br>• Access-control system<br>• Window and door contacts<br>• Glass-break detectors<br>• Emergency door alarms<br>• Passive infrared detectors<br>• Microwave sensors<br>• CCTV monitors<br>• CCTV image recorders |
| b) Inspections must be carried out by an external organization qualified to perform such functions. | Examine sample documents to verify security inspections are performed by a qualified external organization. |
| 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. | 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. |
| **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. | 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.<br>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. |
| b) Evidence (logs) must be retained for this testing for at least 18 months. | Examine evidence (logs) to verify battery test logs have been retained for at least 18 months. |

## 2.5 Vendor Security Contingency Plan

| Requirement | Test Procedure |
|---|---|
| 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. | 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.<br><br>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. |

## 2.6 Decommissioning Plan

| Requirement | Test Procedure |
|---|---|
| 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. | 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. |
| 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. | Examine procedures to verify the process identifies and secures all of the following but not limited to:<br>• Data storage<br>• Card design materials<br>• Cards<br>• Card components<br>• Physical keys<br>• Cryptographic keys<br>• Hardware utilized for production activities |
| 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. | Examine the vendor's policy and procedures to verify they include the disposition expectations for each identified item. |

# Section 3: Production Procedures and Audit Trails

## 3.1 Order Limitations

| Requirement | Test Procedure |
|---|---|
| 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. | Examine the documented procedures in place when vendor starts production of card products or component runs regarding specific orders.<br>Examine a sample of signed work orders to verify:<br>• The order is signed by representative of the payment brand, issuer, or issuer's authorized agent.<br>• The completed work order matches the corresponding inventory of card products or components. |
| b) The vendor must only produce sufficient cards to meet the quantity specified on the order. | Examine documentation to verify procedures are in place to ensure the vendor only produces sufficient cards to meet the quantity specified on the order.<br>Examine a sample of work orders to production run totals to verify procedures are followed. |
| c) If a function normally associated with card production or provisioning is subcontracted, the vendor must obtain authorization from the VPA and the issuer. | Interview production management to determine whether any functions associated with card production or provisioning are subcontracted.<br>Examine documentation to identify what card-production/provisioning functions are subcontracted.<br>Examine a sample of completed documentation to verify the vendor received authorization from the VPA and the issuer. |
| d) The information on the reverse of the cards must always identify the vendor that produces the card. | 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. |

## 3.2 Card Design Approvals

| Requirement | Test Procedure |
|---|---|
| ***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. | Examine the various card-design approval processes to verify that payment brand reviews are appropriately understood and documented by the design team.<br>Examine documentation with vendor to verify that all mandated approvals have been received and are on file to be reviewed upon request. |
| ***3.2.2 Approval Response*** | |
| a) The vendor must proceed with card manufacturing only after the submission has been approved. | Interview production management to verify what controls are in place to verify vendor only starts a manufacturing run after approvals have been received.<br>Examine a sample of artwork approval timeframes compared with production runs to verify approval has occurred prior to production. |

## 3.3 Samples

| Requirement | Test Procedure |
|---|---|
| ***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 | Examine a sample of order documentation to verify all payment brand job-approval records have been retained. |
| b) A sample of the partially processed product or component | Examine a sample of production run retentions to verify they include partially processed products or components. |
| c) A portion of a printed sheet | Examine a sample of production run retentions to verify they each include a portion of a printed sheet. |
| d) Documentation indicating the source, quantities, and the distribution of each product received from an external company | Examine a sample of production run retentions to verify they include documentation of each product received from an external company. |
| e) All samples visually voided and functionally inoperable | Examine a sample of production run retentions to verify their inoperability and void markings. |
| ***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. | 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.<br>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. |

## 3.4 Origination Materials and Printing Plates – Access and Inventory

| Requirement | Test Procedure |
|---|---|
| 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. | Examine policies/procedures to verify restricted access exists where film, plates, or electronic media are produced.<br>Observe that restricted access is in place for any room or area that includes the film, plates, or electronic media.<br>Examine a sample of physical access-control logs to verify that authorized personnel are only allowed within these areas. |
| 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. | Interview personnel to verify that it is required that two persons are involved in the transfer.<br>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. |
| c) The audit sheet must contain at least the following:<br>• Signature of the pre-press staff delivering or collecting the printing films<br>• Job number identification and description of item(s) to be transferred<br>• Signature of the card printing staff collecting or delivering the printing films<br>• Quantity of item(s) transferred (number of films, front and reverse)<br>• Date and time of transfer | Examine a sample of completed audit sheets to verify proper completion to include:<br>• Signature of the pre-press staff delivering or collecting the printing films<br>• Job number identification and description of item(s) to be transferred<br>• Signature of the card printing staff collecting or delivering the printing films<br>• Quantity of item(s) transferred (number of films, front and reverse)<br>• Date and time of transfer |
| d) The vendor must inventory the films, printing plates, and duplicates including a record of plates issued from and returned to the printing department. | 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. |
| e) The vendor must audit this inventory quarterly. | Examine documentation to verify the vendor conducts audits on a quarterly basis. |
| f) The vendor must keep films and printing plates locked under dual control when not in use. | 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. |
| g) Materials maintained must be limited to the final approved version of the last production run of a particular card type. | Examine what materials are in place within the production area.<br>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. |

## 3.4 Origination Materials and Printing Plates – Access and Inventory

| Requirement | Test Procedure |
|---|---|
| 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. | Examine destruction logbook on final use for films and printing plates and verify that two persons are simultaneously signing the destruction log. |
| 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. | Examine documentation and verify security controls are in place such that all discrepancies are documented and immediately reported to management.<br>Examine a sample of documentation to verify that any loss or theft is reported to the VPA within 24 hours of discovery. |

## 3.5 Core Sheets and Partially Finished Cards

| Requirement | Test Procedure |
|---|---|
| ***3.5.1 Core Sheets*** | |
| **3.5.1.1 Access** | |
| a) Access to unbundled core sheets must be restricted at all times. | Observe to verify unbundled core sheets are under restricted access at all times. |
| b) Core sheets must be allocated for production use under a materials/production regimen. | Observe the material/production regimen for allocation of core sheets for production runs to verify existence. |
| **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. | Examine documentation to verify that the WIP storage room is utilized for storage longer than one week.<br>Observe storage controls in place by vendor for both partially and fully printed sheets. |

## 3.5 Core Sheets and Partially Finished Cards

| Requirement | Test Procedure |
|---|---|
| b) Audit or accountability forms for core sheets must provide the following information for every order processed:<br>• Good sheets<br>• Rejected sheets<br>• Set-up sheets<br>• Quality control sheets<br>• Unused core sheets | Examine a sample of orders processed and validate that audit or accountability forms for core sheets contain:<br>• Good sheets<br>• Rejected sheets<br>• Set-up sheets<br>• Quality control sheets<br>• Unused core sheets |
| 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. | 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. |
| 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. | 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.<br>Observe production control system to verify that there is an accurate sheet count recorded. |
| 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. | 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. |
| ***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. | Observe to verify cards stored outside the vault are stored in secure, locked containers in the HSA under dual controls.<br>Examine procedures for use of the WIP area to verify that partially finished cards are stored properly in the HSA. |

## 3.6 Ordering Proprietary Components

| Requirement | Test Procedure |
|---|---|
| a) The vendor must obtain proprietary components—e.g., signature panels, holographic materials, special dies—only from authorized suppliers. | Examine documentation to determine what supplier the vendor is receiving proprietary components from, and whether they are authorized suppliers. |
| 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. | 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. |

## 3.7 Audit Controls – Production

| Requirement | Test Procedure |
|---|---|
| ***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. | Examine policies/procedures to verify audit controls and an audit trail are in place for each job/batch and production step.<br>Examine a complete job run to verify procedures are followed. |
| b) All card products and components—both good and rejected, including samples—must be counted and reconciled prior to any transfer of responsibility. | 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. |

## 3.7 Audit Controls – Production

| Requirement | Test Procedure |
|---|---|
| c) An effective audit trail is comprised of a series of audit logs that must contain but are not limited to the following information:<br>• Description of the component or card product(s) being transferred<br>• Name and signature of the individual releasing the component or card product(s)<br>• Name and signature of the individual receiving the component or card product(s)<br>• Number of components or card products transferred<br>• Number of components used<br>• Number returned to vault or WIP storage<br>• Number rejected or damaged<br>• Number to be destroyed<br>• Date and time of transfer<br>• Name and signature of supervisor<br>• Signatures of persons inventorying components | Examine a sample of audit logs used during a production runs to verify that they contain:<br>• Description of the component or card product(s) being transferred<br>• Name and signature of the individual releasing the component or card product(s)<br>• Name and signature of the individual receiving the component or card product(s)<br>• Number of components or card products transferred<br>• Number of components used<br>• Number returned to vault or WIP storage<br>• Number rejected or damaged<br>• Number to be destroyed<br>• Date and time of transfer<br>• Name and signature of supervisor<br>• Signatures of persons inventorying components |
| 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. | Observe production run to verify the security controls in place include a dual count of cards after each step of the production run. |
| 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. | 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.<br>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. |
| 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. | Examine a sample of documentation to verify:<br>• Accurate and complete inventory of materials is completed.<br>• Audit trails of the past 24 months are maintained by the vendor and available for inspection. |
| 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. | Examine documentation to verify that originals or copies of both the purchase order and invoice for procured materials are being maintained. |

## 3.7 Audit Controls – Production

| Requirement | Test Procedure |
|---|---|
| h) The vendor must conduct inventory counts to ensure that invoices are correct and that they comply with the purchase order. | Examine a sample of inventory counts to verify accuracy of the invoices related to the purchase orders. |
| 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. | Observe the processing of card products to verify that:<br>• The process includes only the minimum number of boxes or sleeves required be opened at one time.<br>• The contents of partially used boxes or sleeves are verified against the inventory control documents.<br>• Any partially used boxes or sleeves are fully used before additional boxes or sleeves are opened<br>• The number of cards in partially used boxes and sleeves are verified.<br>• Each box or sleeve is rewrapped and sealed before being stored in the vault |
| j) Card components must be received and initially inventoried against the supplier's shipping documentation under dual control. | 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. |
| k) A physical count of the boxes containing the card components must be completed at delivery to confirm accuracy of the shipper's documents. | 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. |
| 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. | Examine a sample of transfer documentation to validate:<br>• An authorized card production staff member signs for the component stock received by the vendor.<br>• The person delivering the stock also signs the transfer documentation. |
| m) Card components must be transferred to the vault immediately. | Observe or review the process in place to verify immediate storage of card components into the vault. |
| n) The exact quantity of card components must be counted and registered in the inventory book before vault storage. | Examine the inventory book to verify accurate counts of card components are being maintained by vendor. |
| 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). | Examine the inventory book to validate that:<br>• The hologram identification number is being registered and listed.<br>• If new reels are present, the first hologram number has been listed and matches the reel stored in the vault. |

## 3.7 Audit Controls – Production

| Requirement | Test Procedure |
|---|---|
| p) The card component inventory log must include but is not limited to:<br>• The reel number or equivalent control that provides unique identification.<br>• Date of usage<br>• Customer job number<br>• Number of images or modules placed on cards<br>• Number of rejected images or modules from header and trailer scrap<br>• Number of and reason for rejected images | Examine the card component inventory log to verify that it includes at least:<br>• The reel number or equivalent control that provides unique identification<br>• Date of usage<br>• Customer job number<br>• Number of images or modules placed on cards<br>• Number of rejected images or modules from header and trailer scrap<br>• Number of and reason for rejected images |
| q) Card components must be removed from the machine and locked within a secure container when not in use. | Examine policies/procedures to verify that card components are removed from the machine and locked within a secure container when not in use.<br>Observe and verify that card components are removed from the machine and locked within a secure container when not in use. |
| r) Card components must be returned to the vault during non-production hours. | Examine policies/procedures to verify that card components are returned to the vault during non-production hours.<br>Observe and verify that card components are returned to the vault during non-production hours. |
| s) Rejected card components awaiting return for credits must be maintained under dual control. | Observe and verify that rejected cards awaiting return for credits are maintained under dual control. |
| **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. | Examine a sample of audit logs to verify that all modifications to the audit logs are being made in the authorized and designated manner. |
| b) The updated figure and the initials of the card production staff member making the changes must be placed adjacent to the incorrect figure. | Examine a sample of logs to verify that all modifications to the audit log are being made in the authorized and designated manner. |
| **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. | 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. |
| b) The review must be signed and dated as part of the log. | Examine a sample of logs and verify that it is signed and dated as required and by the proper individual. |

## 3.7 Audit Controls – Production

| Requirement | Test Procedure |
|---|---|
| c) All logs referenced in this document must be retained for a minimum of two years unless otherwise stated. | Examine a sample of logs and verify that logs are retained for a minimum of two years unless required otherwise. |
| ***3.7.2 Vault Audit Controls*** | |
| a) A log is required for items moved in or out of the vault and must contain:<br>• Name of the card issuer<br>• Type of card<br>• Number of cards originally placed in inventory<br>• Reason for transaction—e.g., job number<br>• Number of cards removed from inventory<br>• Number of cards returned to inventory<br>• Balance remaining in the vault<br>• Date and time of activity<br>• Names and signatures of the card production staff who handled the transaction | Examine the vault log to verify that at a minimum it contains:<br>• Name of the card issuer<br>• Type of card<br>• Number of cards originally placed in inventory<br>• Reason for transaction—e.g., job number<br>• Number of cards removed from inventory<br>• Number of cards returned to inventory<br>• Balance remaining in the vault<br>• Date and time of activity<br>• Names and signatures of the card production staff who handled the transaction<br>Observe items being logged in and out of the vault to verify that proper documentation is accurately completed. |
| b) Two card production staff must create a written, physical inventory of card and card components monthly. | 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. |
| c) Card production staff performing the inventory must not have knowledge of the results of the last inventory. | Interview personnel to verify controls are in place to restrict knowledge of any previous inventory. |
| d) At a minimum, the monthly inventory log must contain:<br>• Date of the review<br>• Name of the card issuer<br>• Type of card<br>• Number of cards indicated in the inventory<br>• Number of cards counted<br>• Name and signature of both card production staff who conducted the inventory | Examine a sample of monthly inventory logs and verify that they contain at a minimum:<br>• Date of the review<br>• Name of the card issuer<br>• Type of card<br>• Number of cards indicated in the inventory<br>• Number of cards counted<br>• Name and signature of both card production staff who conducted the inventory |

## 3.7 Audit Controls – Production

| Requirement | Test Procedure |
|---|---|
| e) Any discrepancies must be reported to management and resolved. | Examine procedures related to discrepancies to verify they are reported to management for resolution. |
| ***3.7.3 Personalization Audit Controls*** | |
| a) During personalization, cards and cardholder data must be handled in a secure manner to ensure accountability. | Observe personalization process and validate controls are in place that ensure a secure method of handling and accountability. |
| b) An audit control log must be maintained for each job/sub-job (batch) designating:<br>• Job number<br>• Issuer name<br>• Card type | Examine a sample of audit control logs to verify they include job number, issuer name, and card type. |
| c) For each personalization batch, include:<br>• Initial card procurement (beginning balance)<br>• Card re-makes<br>• Cards returned to inventory<br>• Spoiled cards<br>• Sample/test cards<br>• Machine/operation identification<br>• Date and time of reconciliation<br>• Operator name and signature<br>• Name and signature of an individual other than the operator, who is responsible for verifying the count | Examine a sample of a personalization batches and verify they include:<br>• Initial card procurement (beginning balance)<br>• Card re-makes<br>• Cards returned to inventory<br>• Spoiled cards<br>• Sample/test cards<br>• Machine/operation identification<br>• Date and time of reconciliation<br>• Operator name and signature<br>• Name and signature of an individual other than the operator, who is responsible for verifying the count |
| d) For accounts/envelopes, include:<br>• Number of accounts<br>• Number of card carriers printed<br>• Number of carriers wasted<br>• Number of envelopes that contain cards<br>• Operator name and signature<br>• Name and signature of an individual other than the operator, who is responsible for verifying the count | Examine a sample of a personalization batches and verify they include:<br>• Number of accounts<br>• Number of card carriers printed<br>• Number of carriers wasted<br>• Number of envelopes that contain cards<br>• Operator name and signature<br>• Name and signature of an individual other than the operator, who is responsible for verifying the count |

## 3.7 Audit Controls – Production

| Requirement | Test Procedure |
|---|---|
| e) For PIN mailers, include:<br>• Number of mailers to be printed<br>• Number of mailers actually printed<br>• Wasted mailers that have been printed<br>• Number of mailers transferred to the mailing area/room<br>• Operator name and signature<br>• Name and signature of an individual other than the operator, who is responsible for verifying the count | Examine a sample of a personalization batches and verify they include:<br>• Number of mailers to be printed<br>• Number of mailers actually printed<br>• Wasted mailers that have been printed<br>• Number of mailers transferred to the mailing area/room<br>• Operator name and signature<br>• Name and signature of an individual other than the operator, who is responsible for verifying the count |

## 3.8 Production Equipment and Card Components

| Requirement | Test Procedure |
|---|---|
| ***3.8.1 Personalization Equipment*** | |
| a) The vendor must maintain a log of personalization equipment failures, including at a minimum:<br>• Operator name<br>• Supervisor name and signature<br>• Machine description/number<br>• Job number<br>• Date<br>• Time<br>• Cause of the malfunction | Examine a sample of logs for personalization equipment failures to verify they include at a minimum:<br>• Operator name<br>• Supervisor name and signature<br>• Machine description/number<br>• Job number<br>• Date<br>• Time<br>• Cause of the malfunction |
| ***3.8.2 Indent Printing Module*** | |
| The vendor must: | |
| a) Use payment system proprietary typefaces within indent-printing modules only for payment system cards | Examine cards to verify that authorized payment system proprietary typefaces with indent-printing modules are used only for payment system cards |

## 3.8 Production Equipment and Card Components

| Requirement | Test Procedure |
|---|---|
| b) Destroy, under dual control, payment system proprietary typefaces within indent-printing modules that are no longer to be used. | 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. |
| c) Record the destruction of modules. | Examine a sample of documentation to verify that a record of this destruction is maintained. |
| ***3.8.3 Tipping Foil*** | |
| a) The vendor must shred completely used tipping foil reels containing cardholder data as follows:<br>• In-house—i.e., within the facility,<br>• Under dual control, and<br>• 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. | 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.<br>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. |
| b) Used tipping foil must be removed from the machine during non-production hours. | Examine documentation to verify it requires that tipping foil be removed during non-production hours.<br>Observe procedure of removal of tipping foil to verify it is followed by vendor. |
| c) Prior to destruction—e.g., shredding—the foil must be stored within the HSA under dual access control. | Observe security controls are in place to store tipping foil under dual control within the HSA prior to shredding. |
| d) When destroyed the results must be non-readable and non-recoverable. | Examine a sample of waste to verify proper shredding and destruction of materials is being followed. |
| e) An inventory of the number of used reels must be maintained and reconciled with the number of reels shredded. | Examine a sample of inventory logs to verify the number of used reels is maintained and reconciled with the number of reels shredded. |
| f) A log, pre-numbered and bound, of the destruction of the foil must be maintained and include at a minimum:<br>• Number of reels—partial or full. All used foil must be accounted for and destroyed.<br>• Date and time<br>• Written initials of both individuals who witnessed the destruction | Examine documentation to verify logs are maintained for the destruction of the foil and they contain at a minimum:<br>• Number of reels—partial or full. All used foil must be accounted for and destroyed.<br>• Date and time<br>• Written initials of both individuals who witnessed the destruction |

## 3.8 Production Equipment and Card Components

| Requirement | Test Procedure |
|---|---|
| ***3.8.4 Thermal Transfer Foil*** <br><br> ***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. | Examine documented processes and procedures for the handling of thermal transfer foil reels/cassettes and tracking thermal. |
| b) Records must be maintained pertaining to the reel/cassette for tracking purposes from first use through destruction. | Examine documented processes and procedures for the tracking thermal transfer foil reels/ cassettes. |
| c) The vendor must shred completely used thermal transfer foil reels/cassettes containing cardholder data as follows:<br>• In-house—i.e., within the facility,<br>• Under dual control, and<br>• 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. | 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.<br><br>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. |
| 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. . | Examine documentation to verify it requires that thermal transfer foil reels/cassettes are required to be removed during non-production hours.<br><br>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. |
| e) Thermal transfer foils must be removed from the machine under dual control. These must then be immediately:<br>• Destroyed, or<br>• 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<br>• 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. | Examine documentation to verify it requires that thermal transfer foils are removed for only the following reasons:<br>• Immediate destruction<br>• 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.<br>• 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.<br><br>Observe procedure of removal of tipping foil to verify the process. |

## 3.8 Production Equipment and Card Components

| Requirement | Test Procedure |
|---|---|
| f) Prior to destruction—e.g., shredding—the foil must be stored within the HSA under dual access control. | Observe security controls are in place to store thermal transfer foil under dual control within the HSA prior to destruction. |
| g) When destroyed the results must be non-readable and non-recoverable. | Examine a sample of waste to verify proper destruction of materials is being followed. |
| 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. | 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. |
| i) A log, pre-numbered and bound, of the destruction of the thermal transfer foil must be maintained and include at a minimum:<br>• Number of reels and/or cassettes—partial or full. All used foil must be accounted for and destroyed.<br>• Date and time<br>• Written initials of both individuals who witnessed the destruction. | Examine documentation to verify logs are maintained for the destruction of the foil and they contain at a minimum:<br>• Number of reels and/or cassettes—partial or full. All used foil must be accounted for and destroyed.<br>• Date and time<br>• Written initials of both individuals who witnessed the destruction. |

## 3.9 Returned Cards/PIN Mailers

| Requirement | Test Procedure |
|---|---|
| ***3.9.1 Receipt*** | |
| The vendor must: | |
| a) Maintain a log of all returned cards and PIN mailers. | Examine polices/procedures to verify that a log is required for all returned cards and PIN mailers.<br>Examine a sample of logs to verify procedures are followed to maintain a log of all returned cards and PIN mailers. |
| b) Store all returned cards in a secure container under dual control. | Observe that a secure container is utilized to store all returned cards under dual control. |

## 3.9 Returned Cards/PIN Mailers

| Requirement | Test Procedure |
|---|---|
| c) Either send returned cards to the issuer or destroy them as defined in Section 3.10, "Destruction and Audit Procedures." | Examine polices/procedures to verify returned cards are either sent to the issuer or destroyed according to "Destruction and Audit Procedures."<br>Interview personnel to verify procedures are known and followed. |
| d) Destroy returned PIN mailers as defined in Section 3.10 below. | Observe the method of destruction of PIN mailers to verify it is in accordance with "Destruction and Audit Procedures." |
| 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. | Interview personnel to identify third-party providers with access to PIN mailers.<br>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. |
| ***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. | 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. |
| b) The log must contain at a minimum:<br>• Date of receipt,<br>• Written initials of both card production staff counting the cards,<br>• The issuer name, and<br>• For each package:<br>– The card type<br>– The number of envelopes<br>– The number of cards | Examine a sample of logs to verify they contain at a minimum:<br>• Date of receipt,<br>• Written initials of both card production staff counting the cards,<br>• The issuer name, and<br>• For each package:<br>– The card type<br>– The number of envelopes<br>– The number of cards |

## 3.10 Destruction and Audit Procedures

| Requirement | Test Procedure |
|---|---|
| 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. | 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.<br>Observe in-house destruction process to verify all waste components are counted before being destroyed in-house and under dual control. |
| b) The following materials must be destroyed on a batch basis by shredding or grinding such that the resulting material cannot be reconstructed:<br>• Spoiled or waste card products<br>• Holographic materials<br>• Signature panels<br>• Sample and test cards<br>• Any other sensitive card component material or courier material related to any phase of the card production and personalization process | 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:<br>• Spoiled or waste card products<br>• Holographic materials<br>• Signature panels<br>• Sample and test cards<br>• Any other sensitive card component material or courier material related to any phase of the card production and personalization process |
| c) Destruction of chips, modules, or chip cards must ensure that the chip itself is destroyed. | Observe destruction process to verify that destruction of chips, modules, or chip cards ensures that the chip itself is destroyed. |
| d) An exception to the above is that holograms failing the hot-stamping process must be rendered unusable at the machine. | 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. |
| e) The material waiting to be destroyed must be stored securely, under dual control. | Observe that materials to be destroyed are stored in a secure location under dual control. |
| f) Destruction must be carried out in a separate room as defined in Section 3.10 | Observe destruction is carried out under dual control in a separate room that has restricted access and is under CCTV coverage. |

## 3.10 Destruction and Audit Procedures

| Requirement | Test Procedure |
|---|---|
| g) Proper destruction requires the following:<br>• Individuals destroying the materials must ensure that they are rendered unusable and unreadable.<br>• Two card production staff must simultaneously count and shred the material.<br>• Before leaving the room, both card production staff must ensure that all material has been destroyed and not displaced in the machinery or equipment.<br>• Card production staff must prepare, sign, and maintain a destruction document.<br>• Once the destruction process is initiated, the process must not be interrupted. | 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:<br>• Individuals destroying the materials ensure they are rendered unusable and unreadable.<br>• Two card production staff simultaneously count and shred the material.<br>• Before leaving the room, both card production staff ensure that all material has been destroyed and not displaced in the machinery or equipment.<br>• Card production staff prepare, sign, and maintain a destruction document.<br>• The destruction process, once initiated, is not interrupted. |
| h) An audit log must be created which, at a minimum, contains the following information:<br>• Signatures of the individuals presenting waste material<br>• Description of item(s) to be destroyed (such as product type, job number, and issuer name)<br>• Signatures of the persons observing or carrying out the waste destruction<br>• Quantity of item(s) to be destroyed<br>• Date and time of destruction | Examine a sample of audit logs to verify that, at a minimum, it contains the following information:<br>• Signatures of the individuals presenting waste material<br>• Description of item(s) to be destroyed (such as product type, job number, and issuer name)<br>• Signatures of the persons observing or carrying out the waste destruction<br>• Quantity of item(s) to be destroyed<br>• Date and time of destruction |

## 3.11 Lost and Stolen Reports

| Requirement | Test Procedure |
|---|---|
| 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. | Examine policies/procedures to verify that reporting of loss or theft of card products is:<br>a) Handled immediately (within 24 hours).<br>b) Reported to the VPA, the issuer, and appropriate law-enforcement agencies.<br>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. |
| b) The report must include but is not limited to:<br>• The complete and detailed chronology of events<br>• Cardholder account numbers<br>• Personal identification numbers (PINs)<br>• Printing plates<br>• Encoding or personalizing equipment<br>• Signature panels<br>• Holograms<br>• Electronic storage media<br>• Chips or any carrier containing card components<br>• The vendor's technical specification manual | Examine a sample of lost-or-stolen report logs to verify the information includes, but is not limited to:<br>• The complete and detailed chronology of events<br>• Cardholder account numbers<br>• Personal identification numbers (PINs)<br>• Printing plates<br>• Encoding or personalizing equipment<br>• Signature panels<br>• Holograms<br>• Electronic storage media<br>• Chips or any carrier containing card components<br>• The vendor's technical specification manual |

## 3.11 Lost and Stolen Reports

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

# Section 4: Packaging and Delivery Requirements

The following requirements apply to the packaging and delivery of card products and PINs.

All card shipments are shipped in accordance with the delivery methods defined in the following table:

***Note:*** *Sample cards or proofs sent to an issuer or payment brand are out of scope for this requirement.*

| | Type of Delivery | Card Volume | Destination |
|---|---|---|---|
| **Personalized Cards – Individual** | Card Mail | Individual Package | Cardholder |
| | Courier Service | Individual Package | Cardholder |
| | | Unlimited | Issuer, an approved vendor, or (with written issuer and VPA consent) to another destination |
| | Secure Transport | Unlimited | Issuer, an approved vendor, or (with written issuer[1] and VPA consent) to another destination |
| **Personalized Cards – Bulk** | Card Mailing | Not allowed | |
| | Courier Service | Unlimited | Issuer, an approved vendor, or (with written issuer[1] and VPA consent) to another destination |
| | Secure Transport | Unlimited | Issuer, an approved vendor, or (with written issuer[1] and VPA consent) to another destination |
| **Unpersonalized Cards – Bulk** | Card Mailing | Not allowed | |
| | Courier Service | Limited to 500/package/day/issuer location e.g., branch/vendor | Issuer, an approved vendor, or (with written issuer[1] and VPA consent) to another destination |
| | Secure Transport | Unlimited | Issuer, an approved vendor, or (with written issuer[1] and VPA consent) to another destination |

[1] This includes cards that have been personalized with a cardholder name or a generic identifier, or no cardholder identifier.

## 4.1 Vendor Responsibility and Shipment Documentation

| Requirement | Test Procedure |
|---|---|
| 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. | 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. |
| b) These shipments must be documented to include at least the following information:<br>• Name of the issuer<br>• Destination<br>• Date of shipment<br>• Name of courier<br>• Manifest number | Examine a sample of shipment labels to verify they contain the minimum information required:<br>• Name of the issuer<br>• Destination<br>• Date of shipment<br>• Name of courier<br>• Manifest number |
| 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. | 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. |

## 4.2 Preparation

| Requirement | Test Procedure |
|---|---|
| The vendor must: | |
| a) Count all card products under dual control. | 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. |
| b) Complete audit-control documentation before the cards are packaged. | 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. |
| c) Reconcile all counts with amount to be shipped prior to packaging. | 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. |
| d) Immediately seal containers for final packaging. | 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. |

## 4.2 Preparation

| Requirement | Test Procedure |
|---|---|
| e) Immediately investigate and resolve discrepancies. | Examine policies and procedures to verify that all discrepancies in the preparation process are immediately investigated and resolved before packaging. |

## 4.3 Packaging

| Requirement | Test Procedure |
|---|---|
| The vendor must: | |
| a) Use materials for the packaging of cards and components with sufficient strength to minimize breakage during shipment. | Observe an example to verify the use of packaging materials of sufficient strength to minimize breakage during shipment. |
| b) Use packaging that does not indicate or imply the nature of the contents. | Observe an example to verify the packaging does not indicate or imply the nature of the contents. |
| c) Use reinforced, tamper-evident, color-coded tape that is not in common use to band the containers. | Observe an example to verify the tape used for sealing the packaging is reinforced, tamper-evident, unique, and color-coded. |
| d) Use containers that are uniquely numbered and labeled. | Observe an example to verify the containers are uniquely numbered and labeled. |
| e) Record the number of containers and cards on a packing list. | Observe an example to verify that the number of containers and cards on a packing list are recorded. |
| 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$^{2.}$ | 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$^2$. |
| 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. | Observe an example to verify that each carton that contains shipments of cards has:<br>• The number of cards contained therein printed on the carton.<br>• The batch/shipment details of which it forms part. |

## 4.4 Storage before Shipment

| Requirement | Test Procedure |
|---|---|
| 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. | 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.<br>Observe the area where cards are stored for shipment to verify that:<br>• They are stored in the HSA, and<br>• Access is limited to authorized personnel.<br>Observe CCTV for an example to verify that when the facility is closed cards awaiting shipment are stored in the vault under dual control. |
| b) Packages that are opened or damaged must not be shipped until the contents are recounted and repackaged. | Examine policies/procedures for handling opened or damaged packages to verify they are not shipped until the contents are recounted and repackaged.<br>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. |

## 4.5 Delivery

| Requirement | Test Procedure |
|---|---|
| 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. | 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.<br>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. |

## 4.5 Delivery

| Requirement | Test Procedure |
|---|---|
| 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. | 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.<br>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:<br>• An issuer authorization letter exists, and<br>• 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<br>• A copy of the shipping approval from the VPA is on file, if the VPA requires it. |
| 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. | 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.<br>Interview personnel to identify logs associated with the physical movement of product associated with order numbers.<br>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.<br>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. |
| 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.* |
| ***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. | 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. |
| b) After applying postage and sealing, the envelopes must be counted under dual control and placed in locked or sealed containers or bags. | 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. |

## 4.5 Delivery

| Requirement | Test Procedure |
|---|---|
| c) The loading and transfer process must use the shipping and delivery areas as defined in Section 2.3.6, "Other Areas." | 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." |
| d) Packages containing card envelopments must be sent to the postal service, presort facility, or issuer. | Examine a sample of packages containing card envelopments to verify they are only sent to the postal service, a presort facility, or issuer. |
| 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. | 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. |
| ii. The card transport vehicle must be equipped with a communication device that enables two-way contact with the security controller. | 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. |
| iii. The contents are secured with tamper-evident straps and checked upon delivery. | Examine vendor policies and procedures to verify the contents are secured with tamper-evident straps and checked upon delivery. |
| iv. The vehicle is loaded using dual control and locked during transport. | 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. |
| v. Vehicle drivers do not have a key or access to contents. | 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. |
| vi. Two persons are in the vehicle equipped with a device to communicate with the security control room. | 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. |
| 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. | 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. |

## 4.5 Delivery

| Requirement | Test Procedure |
|---|---|
| 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. | 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.<br>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. |
| **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. | Examine policies and procedures to verify that:<br>• The inclusion of the PIN with the mailing of emergency cards is allowed only with written approval from the issuer;<br>• An appropriate officer of the card issuer is required to sign the authorization letter for emergency card replacement orders;<br>• Such letters contain acknowledgment from the issuer accepting all risk inherent in shipping cards and PINs together;<br>• Such letters confirm that the expedited process is permitted only for emergency card replacement orders; and<br>• The issuer may issue a standing letter of instruction and does not need to approve each emergency card replacement order. |
| **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. | 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. |
| b) The packaging must be the same as that used by the local mail service. | Examine a sample of mail trays to verify that their packaging is the same as that used by the local mail service. |
| c) Labels on packages sent to the postal service or presort facility must not indicate the name of the vendor or issuer. | 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. |
| d) Labels on packages sent to the issuer must not indicate the name of the vendor. | Examine a same of packages for issuers to verify that their package labeling does not indicate the name of the vendor. |
| 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. | 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. |

## 4.5 Delivery

| Requirement | Test Procedure |
|---|---|
| ***4.5.2 Courier Service*** | |
| a) The vendor must secure packages under dual control with access limited to authorized personnel. | Observe that the packages are secured under dual control with access limited to authorized personnel prior to transfer to courier service. |
| 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. | Examine policies and procedures to verify that:<br>• Only a courier service that assigns a unique tracking number for each package is used,<br>• A tracking system is in place to enable the identification of:<br>– Successful completion of delivery milestones during the delivery process from initial pick-up to final delivery.<br>– Exception conditions during the delivery process commencing with initial pick-up and ending with delivery.<br>Observe a sample of activity to verify the ability to track the package in accordance with the aforementioned. |
| 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:<br>• The type of each card<br>• The quantity per card type<br>• The job number(s)<br>• The date of shipment<br>• The date of receipt<br>• Name of receiving organization<br>• Name and signature of person receiving the cards | 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.<br>Examine a sample of manifests to verify that they contain the minimum information required. |
| d) The contents of the manifest must be reconciled with the audit trail for the job. | Examine policies and procedures to verify that the contents of the manifest are reconciled with the audit trail for each job. |

## 4.5 Delivery

| Requirement | Test Procedure |
|---|---|
| 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). | 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.<br>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. |
| f) Receipt of the shipment and count of contents must be confirmed by the recipient, immediately upon receipt under dual control. | 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.<br>Observe a sample of shipping logs to verify that upon receipt of shipment the contents are confirmed by the recipient under dual control. |
| 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. | 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.<br>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. |
| ***4.5.3 Secure Transport*** | |
| a) The vendor must confirm with the VPA whether specific requirements apply to its geographic locations. | Examine evidence of VPA guidance for whether specific requirements apply to its geographic locations. |
| 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. | 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.<br>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. |
| 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 Delivery

| Requirement | Test Procedure |
|---|---|
| **4.5.3.1 Armored Vehicle** | |
| a) This service must be carried out under dual control. | 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. |
| b) The card transport vehicle must not carry any signs or logos indicating it belongs to a card vendor. | 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. |
| 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. | 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. |
| 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. | 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. |
| **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. | 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. |
| 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. | 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. |
| 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. | 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. |
| d) The card transport vehicle must be equipped with a communication device that enables two-way contact with the security controller. | 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. |

## 4.5 Delivery

| Requirement | Test Procedure |
|---|---|
| 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. | 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. |
| **4.5.3.3 Air Freight** | |
| a) Goods must be secured in locked or sealed containers. | 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. |
| b) Goods registered as consolidated cargo are not permitted. | 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. |
| c) The card transport vehicle must not carry any signs or logos indicating it belong to a card vendor. | 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. |
| 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. | 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. |
| 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. | 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. |
| 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. | 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. |
| g) The card transport vehicle must be equipped with a communication device that enables two-way contact with the security controller. | 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. |
| h) If intermediate stops are made during air transport, the vendor must ensure the integrity of the shipment remains intact. | Examine service provider agreement language to verify that the integrity of the shipment remains intact if intermediate stops are made during air transport. |

## 4.5 Delivery

| Requirement | Test Procedure |
|---|---|
| i) An air freight facility capable of handling secure cargo must be used. | 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. |
| j) If any ground storage is required before, during, or after the flight, the location must be secured and inaccessible to unauthorized personnel. | 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. |
| k) The hand-carrying of goods is strictly prohibited. | 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. |
| **4.5.3.4 Sea Freight** | |
| a) Goods must be secured in locked or sealed containers. | 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 sea freight are secured in locked or sealed containers and that only container shipment is used. |
| b) Goods registered as consolidated cargo are not permitted. | Examine vendor policies and procedures—i.e., using internal staff—using internal staff or service provider agreement language to verify that goods registered as consolidated cargo are not permitted. |
| c) Sea-freight service must be bonded. | Examine service provider agreement language to verify that the sea freight service is required to be bonded. |
| d) The vendor must use container shipment. | Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify that only container shipment is used. |
| e) The sea shipping container must be locked while in the vendor's shipping area using a tamper-evident, high-security locking mechanism. | Examine vendor policies and procedures, if done in-house—i.e., using internal staff—or service provider agreement language to verify the sea shipping container is locked while in the vendor's shipping area using a tamper-evident, high-security locking mechanism. |
| f) The container transport vehicle must not carry any signs or logos that would indicate it belongs to the card vendor. | 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. |
| 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. | 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. |

## 4.5 Delivery

| Requirement | Test Procedure |
|---|---|
| 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. | 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. |
| 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. | 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. |
| j) A direct route sea transport is required whenever possible. | Examine service provider agreement language to verify that all sea transports are required to be nonstop whenever possible. |
| k) The container transport vehicle must be equipped with a communication device that enables two-way contact with the security controller. | 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. |
| 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. | 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. |
| m) The sea shipping container must be fitted with a GPS monitoring system that provides real-time tracking of the container location. | 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. |
| 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. | 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. |
| o) If intermediate stops are made during sea transport, the vendor must ensure the integrity of the shipment remains intact. | Examine service provider agreement language to verify that the integrity of the shipment remains intact if intermediate stops are made during sea transport. |
| p) A representative of the vendor must be present if the contents of the shipping container must be inspected by customs. | 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. |
| q) After inspection, the shipping container must be resealed with a new tamper-evident, high-security locking mechanism. | Examine service provider agreement language to verify that after inspection, the shipping container is resealed with a new tamper-evident, high-security locking mechanism. |

## 4.5 Delivery

| Requirement | Test Procedure |
|---|---|
| r) On arrival at the destination port facility, the container must be collected as soon as possible and delivered to the final destination address. | 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. |
| 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. | 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. |
| t) The hand-carry of goods is strictly prohibited. | 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. |
| **4.5.3.5 Rail Freight** | |
| a) Goods must be secured in locked or sealed containers. | 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. |
| b) Goods registered as consolidated cargo are not permitted. | . 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. |
| c) The rail shipping container must be locked while in the vendor's shipping area using a tamper-evident, high-security locking mechanism. | 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. |
| d) The container transport vehicle must not carry any signs or logos that would indicate it belongs to the card vendor. | 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. |
| 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. | 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. |
| 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. | 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. |

## 4.5 Delivery

| Requirement | Test Procedure |
|---|---|
| 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. | 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. |
| h) A direct route rail transport is required whenever possible. | Examine service provider agreement language to verify that all rail transports are required to be nonstop whenever possible. |
| i) The container transport vehicle must be equipped with a communication device that enables two-way contact with the security controller. | 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. |
| 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. | 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. |
| k) The rail shipping container must be fitted with a GPS monitoring system that provides real-time tracking of the container location. | 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. |
| 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. | 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. |
| m) If intermediate stops are made during rail transport, the vendor must ensure the integrity of the shipment remains intact. | Examine service provider agreement language to verify that the integrity of the shipment remains intact if intermediate stops are made during rail transport. |
| n) A representative of the vendor must be present if the contents of the shipping container must be inspected by customs. | 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. |
| o) After inspection, the shipping container must be resealed with a new tamper-evident, high-security locking mechanism. | Examine service provider agreement language to verify that after inspection, the shipping container is resealed with a new tamper-evident, high-security locking mechanism. |
| p) On arrival at the destination rail terminal, the container must be collected as soon as possible and delivered to the final destination address. | 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. |

## 4.5 Delivery

| Requirement | Test Procedure |
|---|---|
| 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. | 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. |
| r) The hand-carry of goods on rail freight solutions is strictly prohibited. | 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. |

## 4.6 Shipping and Receiving

| Requirement | Test Procedure |
|---|---|
| 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. | Examine policies and procedures to verify that the vendor has the names and signatures of individuals who are authorized to collect and deliver shipments. |
| b) Verify the identity of personnel arriving to collect or deliver shipments. | Examine policies and procedures to verify that the vendor confirms the identity of personnel arriving to collect or deliver shipments. |
| c) Confirm the identity with the signature list. | Examine policies and procedures to verify that the vendor confirms the identity of individuals with the signature list. |
| d) Place the cartons on a pallet in such a manner that the sides of the carton showing the batch code are visible. | 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. |
| e) Record the name and signature of individual collecting or delivering the shipment. | Examine policies and procedures to verify that the vendor records the name and signature of individuals collecting or delivering the shipment. |

## 4.6 Shipping and Receiving

| Requirement | Test Procedure |
|---|---|
| ***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. | 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. |
| 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. | 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. |
| c) A written receipt must be completed under dual control at each point of transfer, confirming the integrity of the consignment. | 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. |
| 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. | 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. |
| e) Obtain positive confirmation of receipt of shipment. | Examine shipping activity logs to verify that positive confirmation of receipt of shipment is obtained by the vendor. |
| ***4.6.2 Receipt and Return of Card Components*** | |
| a) All card components must be delivered and returned by secure transport. | Examine policies and procedures to verify that all card components subject to return are delivered by secure transport. |
| b) The consignment must be received under dual control. | Examine shipping activity logs to verify that the consignments of returned card components are received under dual control. |
| c) Whilst under dual control, the consignment must be inventoried and handled as defined in ”Audit Controls” (Section 3.7). | 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). |

## 4.6 Shipping and Receiving

| Requirement | Test Procedure |
|---|---|
| d) Documentation of the shipment must be maintained for 24 months and must include:<br>• Item description<br>• Sequential identification numbers (if applicable)<br>• Reel numbers (if applicable)<br>• Total quantity returned<br>• Recipient name and signatures<br>• Destination or origination address<br>• Shipping or receipt date and time | Examine shipping activity logs to verify that documentation of the shipments is maintained for 24 months and includes:<br>• Item description<br>• Sequential identification numbers (if applicable)<br>• Reel numbers (if applicable)<br>• Total quantity returned<br>• Recipient name and signatures<br>• Destination or origination address<br>• Shipping or receipt date and time |
| e) Prior to shipment, the vendor must ensure that the names and signatures of the authorized recipients are recorded. | Examine shipping activity logs to verify that the names and signatures of the authorized recipients of returned card components are recorded prior to shipment. |
| f) At shipment, the vendor must verify the authorized signatures prior to transfer. | Examine shipping activity logs to verify that the authorized signatures are verified prior to transfer at shipment. |

## 4.7 Establishing Responsibility for Loss

| Requirement | Test Procedure |
|---|---|
| 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. | 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. |

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

## 5 PIN Printing and Packaging of Non-personalized Prepaid Cards

| Requirement | Test Procedure |
|---|---|
| *The following requirements apply only for non-personalized, prepaid cards. All other preceding requirements apply unless explicitly superseded in this section.*<br>*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.*<br>*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:<br>a) Cards will not be activated or loaded with a stored value until they have reached their destination, and<br>b) The issuer accepts all risk inherent in shipping or mailing cards and PINs together. | 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:<br>• Cards will not be activated or loaded with a stored value until they have reached their destination, and<br>• The issuer accepts all risk inherent in shipping or mailing cards and PINs together.<br>Examine a sample of written authorizations from issuers to verify that procedures are followed. |
| **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. | Examine a sample of authorization letters to verify that:<br>An appropriate officer of the issuer has signed the authorization letter.<br>A copy of the letter is maintained in its files until the card expiry date. |
| **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. | Examine policies/procedures to verify:<br>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.<br>An audit trail ensuring separation of duties regarding PIN printing and card personalization is maintained.<br>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.<br>Observe process to verify that restricted access is being enforced for the PIN-printing area. |
| **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. | 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. |

## 5 PIN Printing and Packaging of Non-personalized Prepaid Cards

| Requirement | Test Procedure |
|---|---|
| **5.5** Clear-text PINs must never be available on any system on the personalization network. | Examine documentation to verify that clear-text PINs are never to be available on any system on the personalization network.<br>Interview the network administrator to have them validate that clear-text PINs must never be available on any system on the personalization network.<br>Observe DB tables containing PIN data retrieved by the network administrator to verify PINs are not in clear text. |
| **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. | Examine network diagrams to verify that PIN-printing systems are either on:<br>• A network physically separate from the personalization network, or<br>• A logically separated subnet dedicated for PIN printing, which is protected by a dedicated firewall.<br>Examine firewall rules to verify the aforementioned. |
| **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. | Addressed in review conducted under the *PCI Card Production and Provisioning Logical Security Requirements.* |
| **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. | Examine documentation to identify the controls in place to verify that PINs are deleted from the PIN-printing system immediately after use via:<br>• A secure erasure tool that prevents recovery of the PIN using forensic techniques, or<br>• Off-the-shelf recovery software.<br>• Interview the PIN production manager to verify secure erasure of PINs after printing.<br>Observe PIN-printing process and verify that PINs are securely erased immediately after printing. |
| **5.9** The clear-text PIN must only be available for the minimum time required for printing and must not be stored. | Examine documentation to verify that clear-text PINs are not stored.<br>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. |

## 5 PIN Printing and Packaging of Non-personalized Prepaid Cards

| Requirement | Test Procedure |
|---|---|
| **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 | Examine architecture documentation to verify that the PIN-printing room is in a dedicated room as defined in Section 2.3.5.4.<br>Interview the owner of the PIN-printing process to verify whether clear-text PINs are available outside of the printer and to identify locations. |
| 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. | Observe cabling to confirm no evidence of tampering.<br>Observe how it is secured above ceiling or below flooring and the procedure for gaining access to cabling. |
| c) Additionally, the PIN must be concealed in tamper-evident packaging immediately after printing. | Observe the process for how the PIN is concealed in tamper-evident packaging immediately after printing. |
| **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 | Examine documentation to verify that clear-text PINs only exist within a single integrated device.<br>Observe that this occurs within the personalization HSA; or |
| b) A dedicated PIN printing room within the personalization HSA | Observe that that the activity occurs in a room dedicated to only PIN printing; or |
| c) A separate HSA that meets the physical and logical requirements for a personalization HSA | Observe the separate HSA to verify set-up of the separate HSA meets the physical and logical requirements for a personalization HSA. |
| d) Additionally, all of the following requirements must be fulfilled: | Examine policies/procedures to verify that each of the following is required: |
| e) The printer must be locked under dual control before the print job starts and any PINs are decrypted. | Observe the PIN-printing process to verify the printer is locked under dual controls before the print job starts and any PINs are decrypted. |
| f) The HSM in the printer must be under dual control at all times. | Observe that the HSM is handled under dual control at all times. |

## 5 PIN Printing and Packaging of Non-personalized Prepaid Cards

| Requirement | Test Procedure |
|---|---|
| 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. | 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. |
| 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. | 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.<br>Interview the owner of the PIN-printing process to validate that no storage of the clear-text PINs is allowed. |
| 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. | Observe the PIN-printing process to verify that:<br>• No visibility of the PIN is possible from outside the machine.<br>• The covers on the machine are locked in place with dual control locks. |
| j) The PIN must be concealed in tamper-evident packaging immediately after printing and before leaving the secured confines of the printer. | Observe the PIN-printing process to verify that the PIN is concealed in tamper-evident packaging:<br>• Immediately after printing, and<br>• Before leaving the secured confines of the printer. |

# Appendix A: Applicability of Requirements

| Physical Security Requirements | | | | |
|---|---|---|---|---|
| **Requirement** | **Physical Cards** | **Mobile Provisioning** | | **Conditions** |
| | | **SE** | **HCE** | |
| **Section 1 - Personnel** | | | | |
| All | X | X | X | All requirements applicable |
| **Section 2 – Facilities** | | | | |
| All | X | X | X | All requirements applicable |
| **Section 3 – Production Procedures and Audit Trails** | | | | |
| 3.1 | X | X | X | Only 3.1c applies for mobile provisioning |
| 3.2 | X | | | |
| 3.3 | X | | | |
| 3.4 | X | | | |
| 3.5 | X | | | |
| 3.6 | X | | | |
| 3.7 | X | | | |
| 3.8 | X | | | |
| 3.9 | X | | | |
| 3.10 | X | | | |
| 3.11 | X | | | |
| **Section 4 – Packaging and Delivery Requirements** | | | | |
| All | X | | | All requirements applicable |
| **Section 5 – PIN Printing and Packaging of Non-personalized Prepaid Cards** | | | | |
| All | X | | | All requirements applicable |

# Appendix B: Logical Security Requirements – CCTV and Access-Control System (ACS) Administration

## B.1 User Management

| Requirement | Test Procedure |
|---|---|
| *All system components and software are managed in accordance with the following except for purpose-built appliances such as digital video recorders (DVRs). Purpose-built appliances and similar devices are generally not susceptible to malware and other vulnerabilities and frequently do not support anti-virus and/or patching. Any appliance based on an operating system such as Linux or Windows must be isolated from other networks and not use open connectivity methodologies, such as IP.*<br>*These criteria apply to all systems commonly impacted by malicious software and similar vulnerabilities, such as personal computers and servers. Additionally, all user management controls, including password controls, are implemented except where the platform does not support that degree of granularity. Regardless, controls will be implemented to the degree possible. System upgrades will include at a minimum these capabilities.* | |
| 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. | Examine procedures for granting access to the CCTV system and access-control systems to verify existence.<br>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. |
| 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. | 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. |
| c) Restrict systems access by unique user ID to only those individuals who have a business need. | 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.<br>Interview administrator to verify that system access is restricted to only those unique user IDs who have a business need. |
| d) Only grant individuals the minimum level of access sufficient to perform their duties. | Examine documentation and verify that the access is restricted based on least privileges necessary to perform job responsibilities.<br>Interview administrator to verify that individual access is based the minimum level of access sufficient to perform their duties. |
| e) Make certain that systems authentication requires at least the use of a unique ID and password. | Examine documentation to make certain that ID and password for system authentication is unique.<br>Observe logon to system to verify that—at a minimum—authentication requires the use of an ID and password. |

## B.1 User Management

| Requirement | Test Procedure |
|---|---|
| f) Restrict administrative access to the minimum number of individuals required for management of the system. | Interview administrator to determine names of people with administrative access.<br>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. |
| g) Ensure security guards do not have administrative access. | 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. |
| h) Prevent remote administrative access from outside the facility, except as used in conjunction with an approved SOC. | Examine configurations for remote access technologies to verify that remote access sessions are not enabled, except as used in conjunction with an approved SOC. |
| i) Ensure that group, shared, and generic accounts and passwords are disabled wherever the system supports unique values. | Examine documentation to verify that group, shared, and generic accounts and passwords are disabled wherever the system supports unique values. |
| 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. | Examine documentation to determine if generic administrative accounts are enabled.<br>If generic administrative accounts are enabled, examine documentation to verify that such accounts are used only:<br>• When unique administrator sign-on credentials are not possible, and<br>• In an emergency. |
| 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. | Examine documentation to verify that when generic administrative accounts are used:<br>• The password is managed under dual control where no individual has access to the full password; and<br>• Each component of the password complies with the password control requirements in the next section. |
| l) Validate all system access at least quarterly. | Examine documentation to verify that (at least quarterly) all system access is reviewed.<br>Examine a sample of system access reviews to verify they system access is validated at least quarterly. |
| m) Revalidate card production staff to any systems upon a change of duties. | 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. |
| n) Ensure that access controls enforce segregation of duties. | Examine documentation to verify that access controls enforce segregation of duties. |
| o) Strictly limit privileged or administrative access and ensure such access is approved by both the user's manager and the physical security manager. | Examine documentation to verify that all privileged or administrative access is approved by both the user's manager and the physical security manager. |

## B.1 User Management

| Requirement | Test Procedure |
|---|---|
| p) Establish management oversight of privileged access to ensure compliance with segregation of duties. | Interview management to validate that there is oversight of privileged access to ensure compliance with segregation of duties. |
| q) Ensure that all privileged administrative access is logged and reviewed weekly. | Examine a sample of system logs to verify that privileged administrative access is logged and reviewed at least weekly.<br>Interview management to verify that review of logs is performed at least weekly. |

## B.2 Password Control

| Requirement | Test Procedure |
|---|---|
| ***B.2.1 General*** | |
| The vendor must: | |
| a) Implement a policy and detailed procedures relating to the generation, use, renewal, and distribution of passwords. | Examine policies/procedures to verify coverage of the generation, use, renewal, and distribution of passwords.<br>Interview management to verify that procedures relating to the generation, use, renewal, and distribution of passwords are followed. |
| b) Implement procedures for handling lost, forgotten, and compromised passwords. | Examine polices/procedures to verify that there is a procedure relating to handling lost, forgotten, and compromised passwords.<br>Interview management to verify that procedures relating to handling lost, forgotten, and compromised passwords are followed. |
| 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. | 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. |
| d) Ensure that only users with administrative privileges can administer other users' passwords. | Observe process to administer other users' passwords.<br>Observe a sample of non-administrative users to verify that they do not have the ability to administer other users' passwords |

## B.2 Password Control

| Requirement | Test Procedure |
|---|---|
| e) Not store passwords in clear text. | Observe data tables containing passwords and verify (on screen) that none of the entries are in clear text. |
| f) Change all default passwords. | Observe system administrator log onto the system and validate that all default passwords have been changed. |
| ***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. | 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. |
| b) Newly issued passwords are changed on first use. | Examine system configuration settings to verify that newly issued passwords are changed on first use. |
| c) "First use" passwords expire if not used within 24 hours of distribution. | Examine system configuration settings to verify that "first use" passwords expire if not used within 24 hours of distribution. |
| d) Systems enforce password lengths of at least 12 characters or an equivalent strength. | Examine system configuration settings to verify that systems enforce password lengths of at least 12 characters. |
| e) Passwords consist of a combination of at least three of the following:<br>• Upper-case letters<br>• Lower-case letters<br>• Numbers<br>• Special characters | Examine system configuration settings to verify that password configuration parameters consist of a combination of at least three of the following:<br>• Upper-case letters<br>• Lower-case letters<br>• Numbers<br>• Special characters |
| f) Passwords are not the same as the user ID. | Examine system configuration settings to verify that systems enforce that passwords are not allowed to the same as the user ID. |
| g) Passwords are not displayed during entry. | Observe a sample of user logons to validate that passwords are not displayed in clear text during entry. |

## B.2 Password Control

| Requirement | Test Procedure |
|---|---|
| h) Passwords are encrypted during transmission and rendered unreadable when stored. | Examine documentation to verify that passwords are encrypted during transmission and rendered unreadable when stored.<br>Examine a sample of password data repositories to verify the password field is rendered unreadable (that is, not stored in plaintext). |
| i) Passwords have a maximum life not to exceed 90 days and a minimum life of at least one day. | 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. |
| j) When updating passwords, the system prevents users from using a password that is the same as one of their previous four passwords. | 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. |
| k) The user's identity is verified prior to resetting a user password. | Examine polices/procedures for password resets to identify the process for validating the user identity prior to reset.<br>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. |

## B.3 Session Locking

| Requirement | Test Procedure |
|---|---|
| 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. | 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. |

## B.4 Account Locking

| Requirement | Test Procedure |
|---|---|
| a) Accounts that have been inactive for a specified period (with a maximum of 90 days) must be removed from the system. | Examine a sample of user accounts to verify that any inactive accounts over 90 days old are either removed or disabled. |
| b) Systems must enforce the locking of a user account after a maximum of six unsuccessful authentication attempts. | 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. |
| 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. | Examine documentation to validate that locked accounts must only be unlocked by the security administrator or via an automated password reset mechanism.<br>Examine documentation where systems utilize unlocking via automated password reset mechanisms and validate the following:<br>• Challenge questions with answers that only the individual user would know must be used.<br>• 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.<br>Examine a sample of password resets to verify that the above procedures are followed. |
| d) A user's account must be locked immediately upon that user leaving the vendor's employment until it is removed. | 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.<br>Examine a sample of user departures to verify that the user's account was immediately locked upon the termination of employment from the vendor. |
| e) A user's account must be locked immediately if that user's password is known or suspected of being compromised. | 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. |
| 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:<br>• Remote access<br>• Database<br>• Application<br>• OS | 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:<br>• Remote access<br>• Database<br>• Application<br>• OS |

## B.5 Anti-virus Software or Programs

| Requirement | Test Procedure |
|---|---|
| The vendor must: | |
| a) Define, document, and follow procedures to demonstrate:<br>• Identification of security alerts—e.g., subscribing to security alerts such as Microsoft and the Computer Emergency Response Team (CERT)<br>• Identification of system component updates that affect the supportability and stability of operating systems, software drivers, and firmware components<br>• Inventory of current systems in the environment including information about installed software components and about running services | Examine anti-virus policies/procedures to verify that the following are defined and that corresponding procedures exist for each:<br>• Identification of security alerts—e.g., subscribing to security alerts such as Microsoft and the Computer Emergency Response Team (CERT)<br>• Identification of system component updates that affect the supportability and stability of operating systems, software drivers, and firmware components<br>• Inventory of current systems in the environment including information about installed software components and about running services |
| b) Deploy anti-virus software on all systems potentially affected by malicious software—e.g., personal computers and servers. | 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. |
| c) Ensure that all anti-virus programs detect, remove, and protect against all known types of malicious software. | Examine vendor documentation and examine anti-virus configurations to verify that anti-virus programs:<br>• Detect all known types of malicious software;<br>• Remove all known types of malicious software; and<br>• Protect against all known types of malicious software.<br>*Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits.* |

## B.5 Anti-virus Software or Programs

| Requirement | Test Procedure |
|---|---|
| d) Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs. | Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date.<br>Examine anti-virus configurations, including the master installation of the software to verify anti-virus mechanisms are:<br>• Configured to perform automatic updates, and<br>• Configured to perform periodic scans.<br>Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that:<br>• The anti-virus software and definitions are current.<br>• Periodic scans are performed.<br>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. |
| 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. | Examine patch management documentation to verify that:<br>• Anti-virus is updated at least daily.<br>• Updates are installed in a manner consistent with patch management guidelines.<br>• A process exists to document why any updates were not made.<br>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. |

## B.6 Configuration and Patch Management

| Requirement | Test Procedure |
|---|---|
| The vendor must: | |
| a) Implement a documented procedure to determine whether applicable patches and updates have become available. | Examine documentation related to patch management to verify:<br>• Processes are defined for determining whether patches are applicable to systems; and<br>• Updates are available for installation.<br>Interview the system administrator to verify that procedures are implemented to determine whether applicable patches and updates have become available. |
| b) Make certain a process is implemented to identify and evaluate newly discovered security vulnerabilities and security patches from software vendors. | Examine documentation related to patch management to verify processes are defined for:<br>• Identifying and evaluating newly discovered security vulnerabilities, and<br>• Identifying and evaluating security patches from software vendors.<br>Interview the system administrator to verify that procedures are implemented to identify and evaluate newly discovered security vulnerabilities and security patches from software vendors. |
| c) Ensure that secure configuration standards are established for all system components. | Examine documentation to verify that secure configuration standards are established for all system components.<br>Interview the system administrator to verify that a secure configuration standard exists and that there is a documented configuration standard for all system components. |
| 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. | Examine the organization's system configuration standards for all types of system components and verify that the standard addresses:<br>• The removing of all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. |
| e) Ensure that the configuration of the ACS and CCTV systems is validated against the authorized configuration monthly. | 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.<br>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. |

## B.6 Configuration and Patch Management

| Requirement | Test Procedure |
|---|---|
| f) Evaluate and install the latest security-relevant patches for all system components within 30 days of their release (if they pass validation tests). | Examine documentation related to patch management to verify processes are defined for:<br>• Evaluating and installing the latest security-relevant patches for all system components within 30 days of their release (if they pass validation tests).<br>Examine a sample of recently implemented security relevant patches to verify they were:<br>• Tested,<br>• Approved for install, and<br>• Applied within a 30-day cycle of their release. |
| g) Verify the integrity and quality of the patches before application, including source authenticity. | Examine documentation related to patch management to verify processes are defined for:<br>• Verifying the integrity and quality of the patches before application, including source authenticity. |
| h) Make a backup of the system being changed before applying any patches. | 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. |
| i) Implement critical patches to all Internet-facing system components within seven business days of release. When this is not possible the CISO, IT 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. | Examine documentation related to patch management to verify processes are defined for:<br>• Implementing critical patches to all Internet-facing system components within seven business days of release.<br>• Documenting exceptions for when this is not possible.<br>• 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.<br>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. |
| j) Ensure that emergency hardware and software implementations comply with the procedures and validation requirements established for emergency implementations. | Examine documentation to verify procedures and validation requirements are established for emergency hardware and software implementations.<br>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. |
| k) Ensure that emergency hardware and software implementations follow the configuration and patch management requirements in this section. | 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”). |

## B.7 Audit Logs

| Requirement | Test Procedure |
|---|---|
| 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. | Examine a sample of audit logs to verify they exist for the CCTV and access-control systems and they include:<br>• Operating system logs,<br>• Security software logs or<br>• Product logs and<br>• Application logs containing security events |
| b) Ensure that audit logs include at least the following components:<br>• User identification<br>• Type of event<br>• Valid date and time stamp<br>• Success or failure indication<br>• Origination of the event<br>• Identity or name of the affected data, system component, or resources<br>• Access to audit logs<br>• Changes in access privileges | Examine a sample of audit logs and verify that they include at least the following components:<br>• User identification<br>• Type of event<br>• Valid date and time stamp<br>• Success or failure indication<br>• Origination of the event<br>• Identity or name of the affected data, system component, or resources<br>• Access to audit logs<br>• Changes in access privileges |
| 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. | Examine documentation to validate that procedures exist, they are documented, and they are followed for:<br>• Audit log review and<br>• Reporting of unusual activity; and<br>• Log reviews are either automated or manual; and<br>• Reviews occur on a frequency that is at least monthly. |
| d) Verify at least once a month that all systems are meeting log requirements. | 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”). |

## B.7 Audit Logs

| Requirement | Test Procedure |
|---|---|
| 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. | 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.<br>Examine a sample of logs to verify that they are:<br>• Backed up daily, secured, and retained for at least one year<br>• Accessible for at least three months online and one year offline |
| f) Protect and maintain the integrity of the audit logs from any form of modification. | Examine documentation to verify audit logs are protected from unauthorized modifications via access-control mechanisms, physical segregation, network segregation, encryption, or hashing. |
| g) Implement a security-incident and event-logging framework for its organization. | Examine documentation to verify that security-incident and event-logging are implemented within the organization. |

# Appendix C: Security Operations Center

A Security Operations Center (SOC) is a permanent security configuration that controls Security Management Systems and maintains a high level of protection for buildings, assets, access, and staff. The SOC is optional and when implemented provides a centralized location to monitor, manage, and administer the CCTV, Access Control, and Alarm Systems for multiple facilities. A vendor may implement one or more SOCs such that each SOC provides security services for multiple (2 or more) facilities. When a SOC is present, it is located at a card production facility that is approved by the Vendor Program Administrator (VPA) for card production activities, and the SOC is expected to only monitor card production facilities that are either VPA-approved or are seeking VPA approval. These facilities are owned and operated by the card vendor who operates the SOC.

When a SOC controls the security activities of multiple facilities, a local Security Control Room (SCR) is maintained at each facility for backup purposes in the event the SOC loses connectivity or otherwise becomes non-operational. Therefore, a local SCR is present at each facility managed by a SOC except for the facility at which the SOC is located where it is optional. The local SCR contains fully functional security control systems, but the day-to-day operations are performed by the SOC. Security guards that would normally perform SCR activities and other security functions that do not require a physical presence at the local facility may perform these activities from the SOC. When a SOC is temporarily not operational, local guards and predefined staff members at the affected facilities are expected to perform all tasks necessary to ensure continuous compliance with the security standard.

The SOC security requirements in this section duplicate many of the requirements already contained in other sections of PCI Card Production and Provisioning Security Requirements. This is intentional as a SOC is only evaluated against the security requirements in Appendix C and the rest of the card production facility is assessed against the balance of the requirements. A card production facility that uses a SOC for security services is assessed for compliance with all physical and logical security requirements except where an exception is explicitly permitted for when a SOC is implemented. The SOC must be VPA-approved before becoming operational and is included in the scope of the annual assessment performed by a qualified CPSA.

## C.1 General Requirements

| Requirement | Test Procedure |
|---|---|
| a) Only activities related to SOC and SCR operations shall occur within the SOC perimeter.<br>***Note:*** *SCR activities are not required to occur within the SOC environment.* | Observe to verify that only activities related to SOC and SCR operations occur within the SOC perimeter.<br>Interview personnel to verify that only activities related to SOC and SCR operations occur within the SOC perimeter. |
| b) SOCs must only monitor facilities that are owned and operated by the card vendor who operates the SOC. | Examine documentation to verify that facilities monitored are owned and operated by the card vendor who operates the SOC.<br>Interview personnel to verify that the SOC only monitors facilities that are owned and operated by the card vendor who operates the SOC. |
| c) SOCs must only monitor card production facilities that are either VPA-approved or are seeking VPA approval. | Examine documentation to identify which vendor facilities are VPA-approved and list them for VPA review. |
| d) There must be a shared, common spoken language between all SOCs and managed vendor facilities that all SOC personnel and security responders—i.e., local onsite staff—can use to communicate. | Examine applicable policies and procedures to verify that a shared common spoken language exists between all SOCs and managed vendor facilities.<br>Interview a sample of personnel to verify they can speak the language. |
| e) Upon initiation of communication from a SOC, a trained member of the security organization—e.g., security manager, CISO, security responder—must respond within two minutes when required to intervene in an active event. | Examine policies and procedures to verify that a trained member of the security organization must respond within two minutes when required to intervene in an active event. |
| f) Security responders must be onsite whenever a managed vendor facility is operational. These personnel must be trained to the same level as security guards, as defined in this document. | Examine applicable policies and procedures to verify that security responders must be onsite whenever a managed vendor facility is operational and that they must be trained to the same level as security guards as defined in this document.<br>Interview a sample of security responders to verify that they must be onsite whenever a managed vendor facility is operational and that they are trained to the same level as security guards. |

## C.1 General Requirements

| Requirement | Test Procedure |
|---|---|
| g) The SOC personnel must be aware of who to contact whenever a facility is operational. This information must be readily available at all times for the SOC personnel. This includes but not limited to:<br>• Production manager<br>• Local security manager<br>• CISO<br>• Security Responder(s)<br>This must be reviewed on a monthly basis by the Local Security Manager and provided to the SOC. The SMS must be updated with this information within 48 hours of receipt. | Examine policies and procedures to verify information is provided to SOC personnel of who contact whenever a facility is operational and that this includes:<br>• Production manager<br>• Local security manager<br>• CISO<br>• Security Responder(s)<br>Interview a sample of SOC personnel to verify their awareness of the aforementioned.<br>Examine policies and procedures to verify that the contact information is reviewed on a monthly basis by the Local Security Manager and provided to the SOC.<br>Examine policies and procedures to verify the security management system is updated within 48 hours of receipt of this information. |
| h) All staff that have access to a managed vendor facility must be able to contact the SOC. | Interview a sample of staff with access to a managed vendor facility to verify they have the ability to contact the SOC |
| The vendor must: | |
| i) Document security controls that protect security system data and the SOC network. | Examine policies and procedures to verify that security controls for protecting security system data and the SOC network exists. |
| j) Ensure that any system used in the SOC process is only used to perform its intended function—i.e., monitor and control SOC process activities and/or provide administration activities. | Interview SOC personnel to verify that systems used in the SOC process are only used to perform intended functions. |
| k) Change supplier provided default parameters prior to or during installation in the SOC environment. | Examine documentation to verify that supplier provided default parameters are changed prior to or during installation into the SOC environment. |
| l) Synchronize clocks on all systems-associated SOC networks with an external time source based on International Atomic Time or Universal Time Coordinated (UTC). | Examine documentation to verify that all systems-associated SOC network clocks are synchronized with an external time source based on International Atomic Time or Universal Time Coordinated (UTC). |
| m) Restrict and secure access to security system files at all times. | Examine access controls to security system files to verify access is restricted to only authorized personnel. |

## C.2 Physical Construction

| Requirement | Test Procedure |
|---|---|
| *To ensure that the SOC can provide effective management of a managed vendor facility, the SOC has a resilient infrastructure—i.e., its physical location, structural requirements, equipment within the SOC, and layout.* | |
| ***C.2.1 SOC location*** | |
| The vendor must ensure the SOC: | |
| a) Is located at a VPA-approved facility. | Observe that the SOC is located in a VPA-approved facility |
| b) Is outside of the high security area (HSA) of the facility and the cloud-based provisioning environment and is segregated from the Security Control Room (SCR), either in a separate room, or a fully segregated room within the SCR, or a stand-alone building. | Observe the location of the SOC to verify that it is located outside of the HSA and cloud-based provisioning environment and is segregated from the SCR either in a separate room or a fully segregated room within the SCR, or a stand-alone building. |
| c) Is in a building with low risk of fire, explosion, flooding, vandalism, and exposure hazards from other buildings, and the vendor has performed an analysis to demonstrate that mitigation. The building must be protected against the effects of lightning strikes. | Examine the vendor's analysis to verify the mitigations have been identified.<br>Observe the building housing the SOC to verify it is located in a building that has a low risk of fire, explosion, flooding, vandalism, and exposure hazards from other buildings and the mitigations identified have been implemented.<br>Observe that the building has protections against the effects of lightning strikes. |
| ***C.2.2 Structural requirements*** | |
| The vendor must ensure that: | |
| a) The perimeter walls of the SOC must be concrete or of a similar construction of equivalent resistance. | Examine documentation for the design of the SOC perimeter walls to verify they are constructed of concrete or a similar construction of equivalent resistance.<br>Observe the perimeter walls to verify the design is constructed as stated above. |
| b) Doors, frames, locks, and door closers fitted with ACS must all be of reasonable quality and strength to be effective. | Observe the doors, frames, locks, and door closers fitted with ACS to verify the construction are of reasonable quality and strength to be effective |
| c) Fail-secure doors must be used that will not release in the event of emergency egress or power failure—i.e., the default state is the door stays locked. | Observe that fail-secure doors are used for the SOC that do not release in the event of emergency egress or power failure. |

## C.2 Physical Construction

| Requirement | Test Procedure |
|---|---|
| d) A Hostile Vehicle Mitigation (HVM) risk assessment must be performed to ensure the risk of a vehicle penetrating the SOC is mitigated. Controls to be considered in the risk assessment are:<br>• Location of the SOC in relation to distance from vehicular access points.<br>• Walls existing between the SOC and the road.<br>• Installation of HVM Barriers.<br>The vendor must ensure the following:<br>• All risks identified that could result in a breach of the SOC are remediated.<br>• Assessment is reviewed on an annual basis. | Examine documentation of the HVM risk assessment to verify controls mitigating the risk of a vehicle penetrating the SOC have been considered.<br>Examine evidence that the assessment is reviewed on an annual basis.<br>Interview a local security manager to verify that all risks identified that could result in a breach of the SOC are remediated and that the assessment is reviewed on an annual basis. |
| e) All external windows are to be physically secure from external attack—e.g., non-opening, bullet-resistant, or equipped with metal bars. Windows will be mirrored or use material such as opaque film to prevent sight into buildings. | 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 and are mirrored or use material such as opaque film to prevent sight into buildings. |
| f) External lighting is used to assist in protecting the SOC in conjunction with the CCTV to protect the perimeter. | Observe CCTV footage to verify that external lighting assists in protecting the SOC perimeter in conjunction with CCTV. |
| g) Entrance to the SOC must be via an access-controlled mantrap. | Observe that the entrance to the SOC is controlled via an access-controlled mantrap. |
| h) Entrance to the SOC must be fitted with an intercom. | Observe that the entrance to the SOC is fitted with an intercom. |
| i) CCTV must cover all areas of the SOC, as well as its entrances and exits, as defined in Section 2.4.5, "Closed Circuit Television (CCTV)." | Examine security-control documentation to verify the SOC has CCTV coverage as defined in Section 2.4.5, "Closed Circuit Television (CCTV)."<br>Observe to verify the SOC is covered by CCTV as defined in Section 2.4.5, "Closed Circuit Television (CCTV)." |
| j) The SOC 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, as well as full coverage of the walls, ceiling, and floor. | Examine documentation to verify the SOC 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.<br>Observe access to the SOC to verify the intruder-detection devices are installed as documented. |

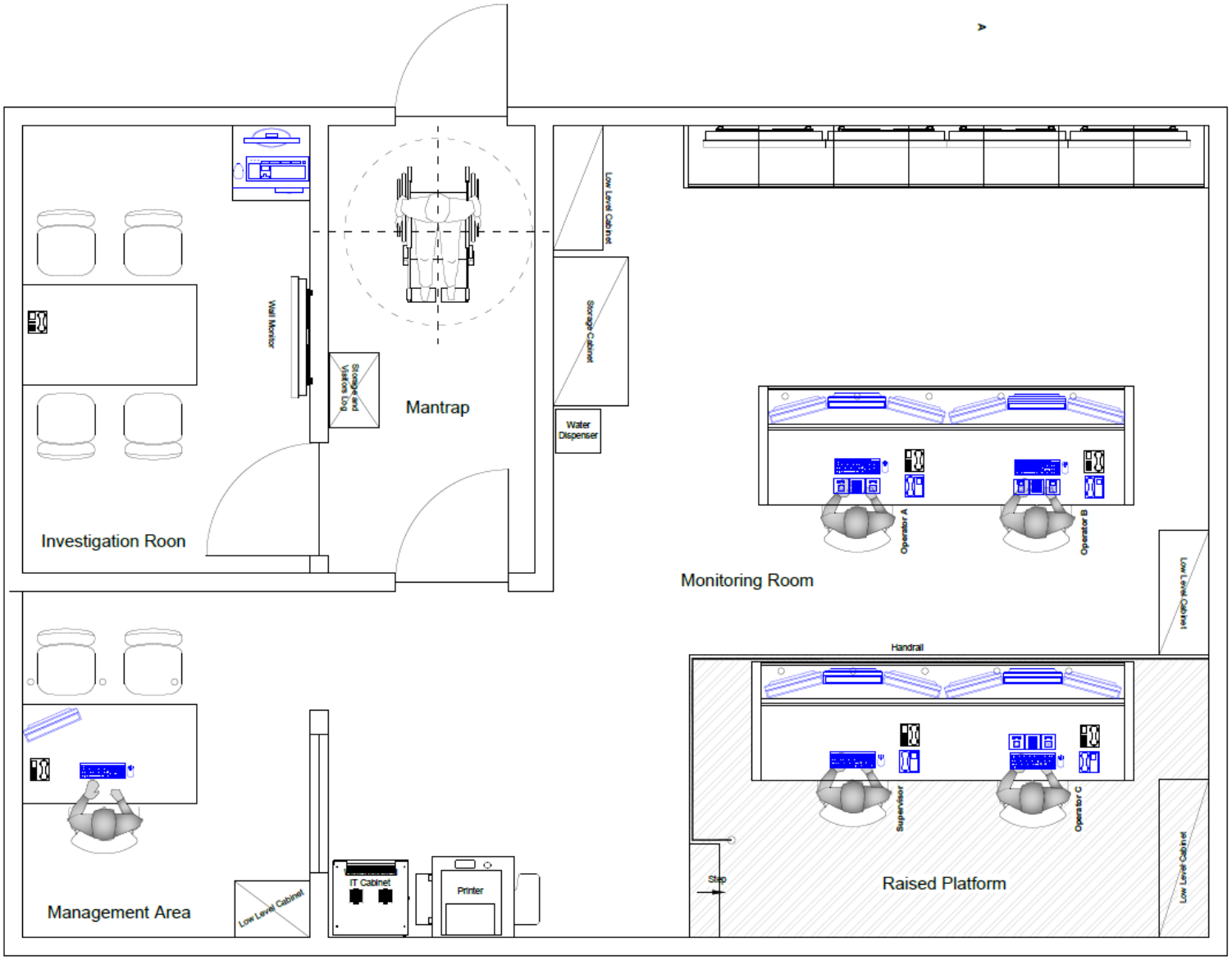
## C.2 Physical Construction

| Requirement | Test Procedure |
|---|---|
| k) The SOC is protected by internal motion detectors that must be activated in zones whenever no authorized staff are known to be present. | Observe the SOC and all separate rooms within the SOC to verify they are protected by internal motion detectors that must be activated in zones when no staff are present.<br><br>Observe via inspection that every zone 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). |
| ***C.2.3 Equipment within the SOC***<br><br>*The SOC has the equipment that is sufficient to adequately monitor the sites that that are under SOC control, with the capability to expand if and when required. The number of operators and workstations needed will be determined by the time required to manage all events from the sights monitored by the SOC.* | |
| At a minimum, each SOC must have: | |
| a) Sufficient operator workstations and monitors to address the following:<br>• Displaying at a minimum:<br>– Event management<br>– Standard operating procedures<br>– CCTV<br>• Ability from a single console to achieve single-point control of systems | Observe to verify that the SOC has sufficient operator workstations, to address the following:<br>• Displaying at a minimum:<br>– Event management<br>– Standard operating procedures<br>– CCTV<br>• Ability from a single console to achieve single-point control of systems |
| b) Two independent forms of communication | Observe to verify that the SOC has sufficient operator workstations to address two independent forms of communication. |
| c) Duress alarm buttons | Observe to verify that the SOC has sufficient operator workstations to address duress alarm buttons. |
| d) An intrusion alarm panel for management of the SOC alarm system, and investigation of events. The alarm system must automatically arm and disarm based on the authorized occupancy of the room. For example, zero occupancy auto-arms the system and occupancy of one or greater auto-disarms the system. | Observe to verify that the SOC has an intruder alarm panel for management of the SOC alarm system, and investigation of events.<br><br>Examine documentation to verify that the alarm system automatically arms and disarms based on the authorized occupancy of the room. |
| e) A security video wall to allow a collaborative environment and for background topics to view international news channels, incidents, events. The monitor wall must be sufficient for any SOC operator to observe. | Observe to verify that the SOC has a security video wall with sufficient monitors to allow a collaborative environment and for background topics. |

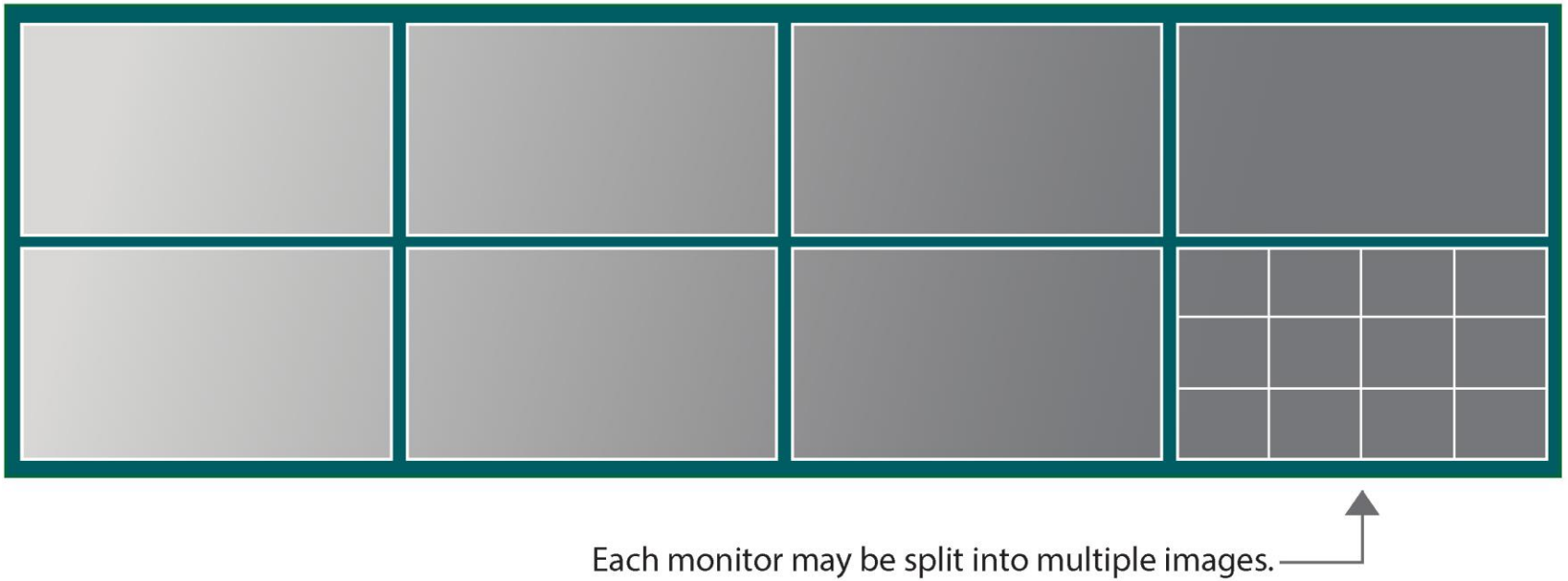
## C.2 Physical Construction

| Requirement | Test Procedure |
|---|---|
| ***C.2.4 Layout of the SOC***<br>*The SOC is configured with the equipment and personnel necessary to effectively monitor the activities and control access at remote facilities.*<br>*There are at a minimum three main areas as shown in the examples below.*<br>**Mantrap Entrance**<br>*The mantrap controls access to the SOC and minimizes disruption to critical business activities.*<br>**Monitoring room**<br>*The main purpose of the monitoring room is to provide a well-managed, ergonomic area for SOC operators to effectively manage all security system events across the managed vendor facilities. The monitoring room will:*<br>• *Provide effective access control and monitoring of PCI CPP regulated areas.*<br>• *Provide resilience and redundancy of critical SMS.*<br>• *Initiate appropriate and timely security response to incidents.*<br>• *Oversee security responses until resolved and provide post-incident reporting.*<br>**Investigation room**<br>*There is dedicated investigations room, separate from the SOC monitoring room.*<br>*Without disturbing the day-to-day operations, the purpose of this area is to:*<br>• *Provide a quiet area to concentrate on high-level event management.*<br>• *Host third parties as part of an investigation.*<br>• *Host third parties for the purpose of auditing.* | |
| The SOC must have: | |
| a) A mantrap entrance to prevent staff “piggybacking” or tailgating (excluding emergency exits). | Observe entrances and exits to determine whether they are fitted with a mantrap to prevent staff “piggybacking” or tailgating (excluding emergency exits). |
| b) A monitoring room, where event monitoring is conducted. | Observe that the SOC has an event monitoring room. |
| c) An investigation room for more in-depth reviews, demonstrations, or audits of the system, without disturbing the monitoring room. | Observe that the SOC has an investigation room that can be used without disturbing the monitoring room. |

**SOC Layout Example**



**Video Wall Example**



## C.3 Security Management System

| Requirement | Test Procedure |
|---|---|
| *A Security Management System (SMS) needs to be created by integrating all the managed vendor facility security systems together to form a centralized operational and management system. The SMS is to be designed to provide real-time information and events to the SOC. For example, an active event, such as a perimeter alarm, will generate an alarm in the SOC. A graphical map will then display the location of the alarm, and the most relevant camera images will appear on the workstation monitors. This will quickly provide the SOC operator with all the information required to investigate potential incidents and initiate appropriate responses.* | |
| ***C.3.1 SMS Provisions*** | |
| The SMS must provide: | Observe to verify that the SMS provides for: |
| a) Visual verification of alarms when possible, to identify nuisance alarms or to initiate an appropriate and balanced response to an actual incident. | • Visual verification of alarms to identify nuisance alarms or to initiate a response to an actual incident. |
| b) Events must be monitored using a video wall in combination with SOC operator workstations. | • Events are monitored using a video wall in combination with SOC operator workstations. |
| c) Single graphical user interface (GUI) to allow the global estate, sites and buildings to be fully monitored. | • Single graphical user interface (GUI) to allow the global estate, sites and buildings to be fully monitored. |
| d) Display pertinent information displayed to aid SOC monitoring and allow a quicker response to incidents. | • Pertinent information displayed to aid SOC monitoring and allow a quicker response to incidents. |
| e) Collection of system data for reports and to provide intelligence to the security management. | • Collection of system data for reports and to provide intelligence to the security management. |
| f) Secure connection to third-party databases to allow for single sourcing of data to reduce errors. | • Secure connection to third-party databases to allow for single sourcing of data to reduce errors. |
| ***C.3.2 System baseline requirements*** | |
| a) The SMS must: | Examine documentation to verify the SMS: |
| i. Allow for real-time event monitoring. | • Allows for real-time event monitoring |
| ii. Integrate with security systems to provide pop-ups for event management. | • Integrates with security systems to provide pop-ups for event management |

## C.3 Security Management System

| Requirement | Test Procedure |
|---|---|
| iii. Support secure individual log-on with configurable user privileges, including user, operator, supervisor, and administrator. | • Supports secure individual log-on with configurable user privileges |
| iv. Provide search functions for reporting and audit purposes to include, but not limited to event logs, user transactions and alarms. | • Provides search functions for reporting and auditing, including event logs, user transactions and alarms |
| v. Allow viewing of system events when required. | • Allows viewing of system events when required. |
| b) The CCTV system must be able to:<br>• View both live and recorded CCTV footage.<br>• Automatically display live CCTV footage associated to an event.<br>• Display recorded CCTV footage that is marked at the event ready for playback. | Examine documentation to verify the CCTV system can<br>• View both live and recorded CCTV footage.<br>• Automatically display live CCTV footage associated to an event.<br>• Display recorded CCTV footage that is marked at the event ready for playback<br>Observe to verify that the aforementioned CCTV system characteristics exist. |
| c) Each SOC must have sufficient bandwidth to manage the security systems.<br>• Minimum requirements include the capability to simultaneously stream the following:<br>– Multiple CCTV feeds per SOC operator workstation.<br>– Multiple CCTV feeds per supervisor workstation.<br>– Multiple CCTV feeds per manager workstation.<br>• This must be tested on a monthly basis. | Examine documentation to verify the SOC has sufficient bandwidth to manage security systems including providing for the following minimums:<br>• Multiple CCTV feeds per SOC operator workstation.<br>• Multiple CCTV feeds per supervisor workstation.<br>• Multiple CCTV feeds per manager workstation.<br>Observe to verify that the aforementioned minimum feeds exist at each applicable workstation |
| d) Standard operating procedures must be creating for the management of all security systems events. The event log must include:<br>• Definition of action required.<br>• Person completing the action.<br>• Time and date action was completed. | Examine documentation of standard operating procedures for management of all security system events to verify their existence.<br>Examine a sample of the event log to verify that it contains the following:<br>• Definition of action required.<br>• Person completing the action.<br>• Time and date action was completed. |

## C.3 Security Management System

| Requirement | Test Procedure |
|---|---|
| ***C.3.3 Functionality*** | |
| *From the SOC Monitoring room, the SOC operators are able to manage all security system events from any site being monitored.* | |
| **C.3.3.1 Security System Events** | |
| The following events must be logged: | Examine a sample of security system event logs to verify they contain the following information at a minimum: |
| a) Unauthorized access attempts | Unauthorized access attempts |
| b) Access (successful or failed) attempts results | Access attempts results |
| c) Anti-pass-back violations | Anti-pass-back violations |
| d) Door-open-too-long alarm | Door-open-too-long alarm |
| e) Forced door | Forced door |
| f) Occupancy violations such as:<br>• Dual occupancy<br>• Occupancy greater or equal to one, with no motion detected within 15 or fewer minutes<br>• Motion detected when occupancy equals zero<br>• Motion detected inside the inner room of the loading bay when both intermediate and inner doors are closed | Occupancy violations such as:<br>• Dual occupancy<br>• Occupancy greater or equal to one, with no motion detected within 15 or fewer minutes<br>• Motion detected when occupancy equals zero<br>• Motion detected inside the inner room of the loading bay when both intermediate and inner doors are closed |
| g) Duress Alarm activation | Duress Alarm activation |
| h) 24/7 monitored intruder alarm device activation | 24/7 monitored intruder alarm device activation |
| i) Activations from managed vendor facilities where intruder alarm systems are set | Activations from managed vendor facilities where intruder alarm systems are set |
| j) Intruder alarm system not set or unset within a scheduled time | Intruder alarm system not set or unset within a scheduled time |
| k) Fire alarm activation | Fire alarm activation |
| l) Auxiliary power or battery backup system is invoked | Auxiliary power or battery backup system is invoked |
| m) CCTV involuntary or voluntary disconnection | CCTV involuntary or voluntary disconnection |

## C.3 Security Management System

| Requirement | Test Procedure |
|---|---|
| **C.3.3.2 Access Credential Management** | |
| SOC personnel can be authorized to create or update access credentials for the managed vendor facilities. The vendor must first ensure that: | |
| a) The Access Credential Management Process must include:<br>• A request for updating access credentials is made.<br>• The local security manager or other authorized personnel within each managed vendor facility approves the change.<br>• The request is sent to the SOC, and SOC personnel modify the access credential assignment under dual control.<br>• All changes to the system must be logged. | Examine policies and procedures to verify the following processes exist<br>• A request for updating access credentials is made.<br>• The local security manager or other authorized personnel within each managed vendor facility approves the change.<br>• The request is sent to the SOC, and SOC personnel modify the access credential assignment under dual control.<br>• All changes to the system are logged.<br>Examine a sample of creation and updating of access credentials to verify the aforementioned process is followed. |
| **C.3.3.3 Event Management Steps** | |
| a) An "Event matrix" must be created. The matrix must:<br>• List all possible events for each system type.<br>• For each event type, an SLA must be established. | Examine documentation to verify that an event matrix has been created that includes:<br>• Listing all possible events for each system type<br>• For each event type an SLA is established |
| b) For each identified event:<br>• The event must be registered in the security system and actioned by the SOC operator.<br>• The system must automatically bring all relevant information—e.g., event information (alarm location depicted on map), CCTV live and recorded footage, and standard operating procedures—to a selection of screens in front of the SOC operator.<br>• Documented procedures must require the SOC operator to investigate the event. | Examine security system documentation to verify:<br>• Events are registered in the security system and actioned by the SOC operator<br>• That the system automatically brings all relevant information (e.g., event information, CCTV live and recorded footage, and standard operating procedures) to a selection of screens in front of a SOC operator.<br>Examine policies and procedures to verify that SOC operators are required to investigate events.<br>Interview a SOC operator to verify the event investigation process defined above. |

## C.3 Security Management System

| Requirement | Test Procedure |
|---|---|
| c) Documented procedures must provide guidance to facilitate operator taking action to:<br>• Contain the event.<br>• Escalate as necessary.<br>• Take necessary corrective actions within prescribed time frames. | Examine documentation of standard operating procedures to verify they contain guidance for SOC operator actions required to contain events and prevent their escalation.<br>Observe that SOC operators have systems available in front of them to contain an event, including blocking access rights or alerting the local security manager.<br>Examine documentation of standard operating procedures to verify they contain guidance for SOC operators on necessary corrective actions. |
| d) The system must help generate a report by automatically pulling the relevant data into one template. | Examine a sample of medium- and high-security events to verify that the security system automatically generates a report pulling the relevant data into one template. |
| e) Documented procedures must require that all actions taken for medium- and high-security events are reviewed to ensure that the preventative actions are sufficient to prevent reoccurrence. | Examine policies and procedures of to verify that medium- and high-security events are reviewed to ensure that the preventative actions taken are sufficient to prevent reoccurrence. |

## Examples of Security System Events and Priorities

| SECURITY SYSTEM EVENTS | SERVICE LEVEL AGREEMENT (SLA) | | | | PRIORITY |
|---|---|---|---|---|---|
| | Understand the situation – after the event acceptance (seconds) | Take containments measures (seconds) | Take corrective action (seconds) | SLA time – start to finish (seconds) | |
| Invalid card (single) – Defined secure area | 15 | 60 | 45 | 120 | Low |
| Invalid card (three or more attempts) – Defined secure area | 15 | 60 | 105 | 180 | Medium |
| Invalid card – Non-secure area | 0 | 0 | 0 | 0 | N/A |
| Valid card | 0 | 0 | 0 | 0 | N/A |
| Forced door (door opened without use of a valid access credential) | 15 | 60 | 105 | 180 | High |
| Door open too long – Multiple (three or more) activations | 15 | 60 | 45 | 120 | Medium |
| Anti-passback violation | 15 | 60 | 45 | 120 | N/A |
| Motion detected when occupancy equals zero | 15 | 60 | 45 | 120 | High |
| Occupancy is one, with no second person present within 60 seconds; or multiple single occupancies within 5 minutes. | 15 | 60 | 45 | 120 | Medium |
| Camera signal loss | 15 | 240 | 45 | 300 | Medium |
| Hard-drive failure | 15 | 240 | 45 | 300 | Low |
| Multiple hard-drive failures | 15 | 240 | 45 | 300 | High |
| Camera masking | 15 | 60 | 45 | 120 | Medium |
| Duress alarm activated | 15 | 60 | 45 | 120 | Medium |
| Motion sensor activated | 15 | 60 | 45 | 120 | Medium |
| IR beam activated | 15 | 60 | 45 | 120 | Medium |
| Acoustic break glass activated | 15 | 60 | 45 | 120 | Medium |
| Shock sensor activated | 15 | 60 | 45 | 120 | Medium |
| Seismic sensor activated | 15 | 60 | 45 | 120 | Medium |

## C.3 Security Management System

### *C.3.4 Priorities*

*The system processes the events on a priority basis to allow efficient and effective management. The guideline timing below provides the first steps to contain the event and prevent it from escalating. Subsequent steps can take longer, based on other events.*

| | |
|---|---|
| a) All security system events must be addressed within the following timeframes:<br>• N/A events are simply registered without action.<br>• Low priority events must be addressed within 30 minutes.<br>• Medium priority events must be addressed within 10 minutes.<br>• High priority events must be addressed within 6 minutes. | Examine policies and procedures to verify they require that security system events are contained according to the following timeframes:<br>• N/A events are simply registered without action.<br>• Low priority events are addressed within 30 minutes.<br>• Medium priority events are addressed within 10 minutes.<br>• High priority events are addressed within 6 minutes.<br>Examine a sample of low, medium, and high priority events to verify they are addressed within the prescribed timeframes. |
| **C.3.4.1 Performance Management** | |
| a) Ongoing performance must be monitored and reported, ensuring:<br>• The event matrix is accurate and kept up to date.<br>• Events are managed correctly within the SLA's defined in the event matrix.<br>• The Corporate Security Director reports the results of SLA performance on a monthly basis to senior management.<br>• The full assessment is reviewed annually. | Examine policies and procedures to verify a process exists and is followed to ensure the event matrix is kept accurate and up to date.<br>Examine a sample of events to verify they are managed within the specifications of the SLA as defined in the event matrix.<br>Interview the Corporate Security Director to verify the CSD reports the results of SLA performance on a monthly basis to senior management.<br>Examine policies and procedures to verify the full assessment is reviewed annually. |

## C.4 SOC Personnel

| Requirement | Test Procedure |
|---|---|
| a) A corporate security director must be designated to ensure oversight and continuity between all SOCs of the vendor.<br>This position is responsible for ensuring that:<br>• The SOCs are appropriately resourced.<br>• The SOCs fulfil their responsibility for the remote monitoring and administration of all managed vendor facilities.<br>• The corporate security director must report to senior management the status and performance of the SOCs on a quarterly basis. | Examine applicable policies and procedures to verify that a senior manager has been designated as corporate security director to ensure oversight and continuity between all SOCs of the vendor.<br>Interview the corporate security director to determine their understanding of their roles and responsibilities, which include:<br>• The SOCs are appropriately resourced.<br>• The SOCs fulfil their responsibility for the remote monitoring and administration of all managed vendor facilities.<br>• Reporting to senior management the status and performance of the SOCs on a quarterly basis. |
| b) The corporate security director must be an employee of the vendor. | Examine employment documentation to verify employment and position. |
| c) A CISO must be designated to be responsible for all security matters related to the SOC. | Examine applicable policies and procedures to verify that a senior manager has been designated as CISO responsible for all security matters related to the SOC.<br>Interview the CISO to determine their understanding of their roles and responsibilities. |
| d) The CISO must be an employee of the vendor. | Examine employment documentation to verify employment and position. |
| e) A dedicated supervisor must be working in a SOC whenever the SOCs are operational. The supervisor's role is:<br>• Coordinating incident management responses.<br>• Functioning as the initial point of escalation of security events for the SOCs. | Examine applicable policies and procedures to verify that individuals have been designated as dedicated supervisors to work in the SOC whenever the SOCs are operational.<br>Interview at least one dedicated supervisor to determine his or her understanding of roles and responsibilities which include:<br>• Coordinating incident management responses.<br>• Functioning as the Initial point of escalation of security events for the SOCs. |
| f) The dedicated supervisors must be employees of the vendor. | Examine employment documentation to verify employment and position. |
| g) Each SOC must be manned by the appropriate number of SOC operators according to Section C.2.3.3, "Event Management Steps." At a minimum, there must always be one SOC operator per operational SOC location. | Examine applicable policies and procedures to verify that each SOC must be manned by the appropriate number of SOC operators according to Section C.2.3.3, "Event Management Steps." At a minimum, there must always be one SOC operator per operational SOC location.<br>Observe the SOC at the facility under review to verify that the number of SOC operators is in accordance with Section C.2.3.3, "Event Management Steps". |

## C.4 SOC Personnel

| Requirement | Test Procedure |
|---|---|
| h) Supervisors and SOC operators are not permitted to perform any functions normally associated with the production of card products or card components. They must not have access to:<br>• HSAs<br>• Physical Master Keys that provide access to card production or provision environments<br>• Any restricted areas where the vendor processes, stores, or ships or receives card products and card components | Examine applicable policies and procedures to verify that supervisors and SOC operators are not permitted to perform any functions normally associated with the production of card products or card components including access to:<br>• HSAs<br>• Physical Master Keys that provide access to card production or provision environments<br>• Any restricted areas where the vendor processes, stores, or ships or receives card products and card components<br>Interview a sample of supervisors and SOC operators to determine their understanding of their roles and responsibilities which DO NOT include access to:<br>• HSAs<br>• Physical Master Keys that provide access to card production or provision environments<br>• Any restricted areas where the vendor processes, stores, or ships or receives card products and card components. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| ***C.5.1 Communication between SOC and Managed Vendor Facilities*** | |
| Communication between SOC and managed vendor facilities must use HTTPS connections (to ensure security of communication is maintained while firewalls ensure specific flows for inbound/outbound traffic. These connections must: | |
| a) Use authorized locations and equipment to be defined and managed accordingly. | Examine policies and procedures to verify that only authorized locations and equipment are used. |
| b) Use strong cryptography and security protocols to safeguard security system data during transmission over open, public networks, including the following:<br>• Only trusted keys and certificates are accepted.<br>• The protocol in use only supports secure versions or configurations.<br>• The encryption strength is appropriate for the encryption methodology in use. | Examine documentation and system settings to verify that only strong cryptography and security protocols as defined in PCI DSS are used for transmission of security system data over open, public networks. This includes:<br>• Only trusted keys and certificates are accepted.<br>• The protocol in use only supports secure versions or configurations.<br>• The encryption strength is appropriate for the encryption methodology in use. |

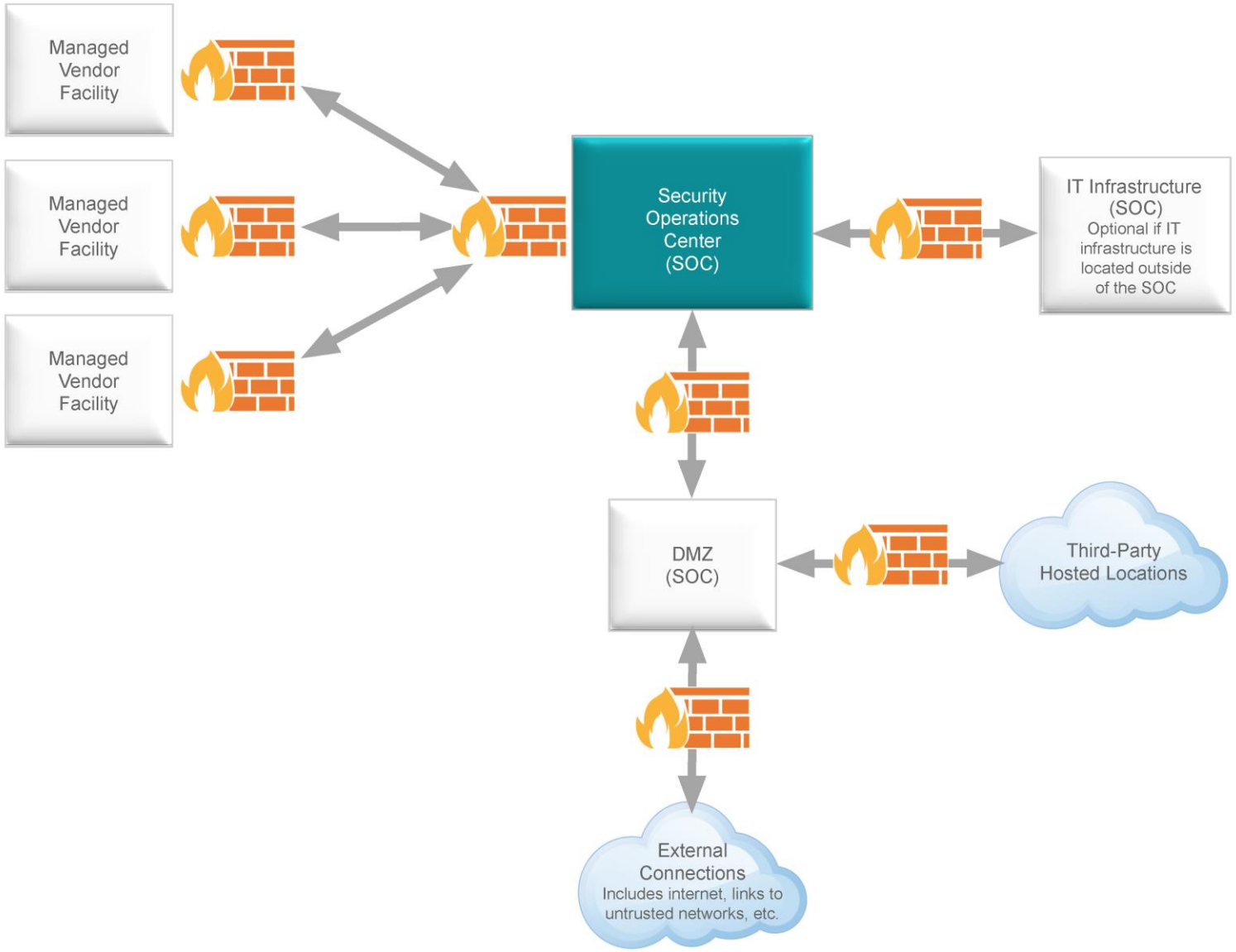
## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| ***C.5.2 Network Security*** | |
| *Access-control information, CCTV images, and any other data used in connection with remote administration of a card facility are encrypted during transmission over public networks, because it is easy and common for a malicious individual to intercept and/or divert data while in transit.*<br>*Secure transmission of security system data requires using trusted keys/certificates, a secure protocol for transport, and proper encryption strength to encrypt security system data. Connection requests from systems that do not support the required encryption strength and would result in an insecure connection should not be accepted.*<br>*Note that some protocol implementations (such as SSL, SSH v1.0, and TLS 1.0 or 1.1) have known vulnerabilities that an attacker can use to gain control of the affected system. Whichever security protocol is used, ensure it is configured to use only secure versions and configurations to prevent use of an insecure connection—e.g., using only trusted certificates and supporting strong encryption, not weaker, insecure protocols or methods.*<br>*Verifying that certificates are trusted—e.g., have not expired and are issued from a trusted source—helps ensure the integrity of the secure connection.*<br>*Generally, the web page URL should begin with "HTTPS" and/or the web browser with a padlock icon displayed somewhere in the window. Many TLS certificate vendors also provide a highly visible verification seal—sometimes referred to as a "security seal," "secure site seal," or "secure trust seal"—which may provide the ability to click on the seal to reveal information about the website.*<br>*Refer to industry standards and best practices for information on strong cryptography and secure protocols—e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.*<br>***Note:** SSL/early TLS is not considered strong cryptography and may not be used as a security control.* | |
| **C.5.2.1 General Requirements** | |
| The vendor must: | |
| a) Maintain a current network topology diagram that includes all system components on the network. The diagram must clearly define the boundaries of all networks. | Examine network topology diagram to verify it exists, clearly defines the boundaries for all networks, and includes all system components related to the SOC. |
| b) Ensure the network topology diagram is reviewed, updated as appropriate, and verified at least once each year and whenever the network configuration is changed. | Interview network administration personnel to verify the policy and procedures require topology review and update upon making changes to the network and at least annually.<br>Examine evidence that the network topology diagram was reviewed and updated when the network configuration was changed and at least within the last 12 months if there were no changes. |
| c) Ensure that the CISO accepts, by formal signature, the security implications of the current network topology. | Examine evidence that the CISO has accepted the security implications of the current network topology and that the document includes his or her formal signature. |
| d) Document the flow of security system data within the environment from the receipt/generation to end of its lifecycle. | Examine the data-flow diagram of security system data within the environment from the receipt/generation to end of its lifecycle.<br>Interview the IT manager to verify the diagram(s) are kept current and updated as needed. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| e) Ensure that the SMS is on dedicated network(s) independent of the back office—e.g., accounting, human resources, etc.—and Internet-connected networks. | Examine documentation to verify that the SMS is on dedicated network(s) independent of the back office. |
| f) Put controls in place to restrict, prevent, and detect unauthorized access to the security system networks. | Examine policies and procedures to verify that access to the security system networks is restricted, and unauthorized access is prevented and detected.<br>Examine a sample of access rules to verify that access to the security system networks is restricted, and unauthorized access is prevented and detected. |
| g) Be able to immediately assess the impact if any of its critical connecting points are compromised. | Examine documented incident response procedures to verify processes are in place that allow for immediate assessment of the impact of any compromise of critical connecting points |
| h) Control at all times the physical connection points leading into the security system network. | Observe physical connection points leading into the security system network to verify they are controlled at all times. |
| i) Prevent data from being tampered with or monitored by protecting the network cabling associated with security system data movement. | Observe a sample of security system network cabling to verify that access is restricted, the cabling is protected, and safeguards are in place to avoid tampering. |
| j) Ensure a process is in place for updates and patches and identification of their criticality, as detailed in Section C.6.14, "Configuration and Patch Management." | Examine documented procedures to verify they include a process for updates and patches that includes identification of their criticality as delineated in the Section C.6.14, "Configuration and Patch Management." |
| k) Have the capability to detect, isolate, and correct abnormal operations within the SMS network endpoints on a real-time basis, 24/7. | Interview personnel to verify that system-monitoring assets are functional and utilized.<br>Examine evidence to verify that abnormal operations on SMS network endpoints can be:<br>• Detected,<br>• Isolated, and<br>• Corrected<br>on a real-time and 24/7 basis. |

**SOC Topology Example**



## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| ***C.5.3 Network Devices*** | |
| *The requirements in this section apply to all hardware—e.g., routers, controllers, firewalls, storage devices—that comprises the security system networks.* | |
| The vendor must: | |
| a) Document the process to authorize all changes to network devices and protocols. | Examine policies and procedures to verify a process is in place to authorize all changes to network devices and protocols prior to implementation.<br>Examine a sample of change-management logs for network devices and protocols to verify the changes are authorized. |
| b) Document the current network device configuration settings, rules set and justification for each device. | Examine a sample of network device documentation to verify configuration settings, rulesets, and their justifications are documented.<br>Interview personnel to verify they are familiar with the documentation and process by which the documentation is updated. |
| c) Ensure all available services are approved by an authorized security manager. | Interview personnel to identify available services.<br>Examine evidence that available services were approved by an authorized security manager. |
| d) Implement logical and physical security controls that protect the integrity of network devices used. | Examine documentation of logical and physical security controls that protect the integrity of network devices used to verify existence.<br>Observe a sample of the controls to verify effective implementation. |
| e) Implement mechanisms to effectively monitor activity on network devices. | Interview personnel to verify mechanisms are defined and implemented to effectively monitor the activity on network devices.<br>Examine policies and procedures to verify mechanisms are defined to effectively monitor the activity on network devices. |
| f) Implement patches in compliance with Section C.6.14, "Configuration and Patch Management." | Examine a sample of device configurations and verify that patches have been implemented in compliance with Section C.6.14. |
| g) Maintain an audit trail of all changes and the associated approval. | Examine a sample of change-control logs to verify that an audit trail of changes and associated approvals is maintained. |
| h) Implement unique IDs for each administrator. | Examine a sample of administrator IDs and verify that unique IDs are used. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| i) Implement network device backups—e.g., system software, configuration data, and database files—prior to any change and securely store and manage all media. | Examine change-control documentation to verify there is a process for backing up network devices prior to any changes to those devices.<br>Examine procedures for backups and managing backup media to verify media are securely stored and managed.<br>Observe the media storage location to verify it provides a secure storage environment. |
| j) Implement a mechanism to ensure that only authorized changes are made to network devices. | Examine network device change logs to verify that changes to network devices were authorized before implementation. |
| ***C.5.4 Firewalls***<br>*The requirements in this section apply to firewalls protecting the security system networks.* | |
| **C.5.4.1 General** | |
| The vendor must: | |
| a) Ensure all documents relating to firewall configurations are stored securely. | Observe the firewall configuration documentation storage area to verify:<br>• Hard copy and non-digital documentation are stored in locked/secured areas with access only to authorized personnel.<br>• Digital records are stored in a secure directory with access limited to authorized personnel. |
| b) Deploy an external firewall outside the SOC to protect the SOC's DMZ. | Examine network diagrams and other relevant materials to verify that an external firewall outside the SOC is implemented to protect the SOC's DMZ in accordance with acceptable configurations.<br>Examine firewall rules to verify that an external firewall is in place outside the SOC to protect the SOC's DMZ. |
| c) Install a firewall between the managed vendor facility security system network and the SOC network. | Examine firewall rules to verify the separation via a firewall between the managed vendor facility security system network and the SOC network. |
| d) Deploy a physically separate firewall between the external network and the SOC DMZ and between the DMZ and the SOC network. | Examine network diagrams and firewall rules to verify that firewalls are installed between the external network and the SOC DMZ and between the DMZ and the SOC network. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| e) Have the capability to detect, isolate, and correct abnormal operations on network systems on a real-time basis, 24/7, on the external (DMZ) facing firewall. | Examine documentation to verify that abnormal operations on network systems can be:<br>• Detected,<br>• Isolated, and<br>• Corrected<br>on a real-time, 24/7, basis.<br>Examine a sample of logs to verify that abnormal operations on network systems are:<br>• Detected,<br>• Isolated, and<br>• Corrected<br>on a real-time, 24/7, basis. |
| f) Implement appropriate operating-system controls on firewalls. | Examine configurations to verify that appropriate operating-system controls are implemented on firewalls. |
| g) Review firewall rule sets and validate supporting business justification either monthly, or quarterly, with review after every firewall configuration change. | Examine evidence that firewall rule sets have been validated either:<br>• Monthly, or<br>• After every firewall configuration change and every 3 months<br>Examine a sample of firewall rule sets to verify that their business justification is documented. |
| h) Restrict physical and logical access to firewalls to only those designated personnel who are authorized to perform firewall or router administration activities. | Observe the firewall/router environment to verify that that physical access to firewalls is limited to only those designated personnel who are authorized to perform administration activities.<br>Examine a sample of access rules to verify logical access is restricted to only those designated personnel who are authorized to perform firewall or router administration activities. |
| i) Ensure that only authorized individuals can perform firewall administration. | Examine policies and procedures to verify that only authorized individuals can perform firewall administration.<br>Interview personnel to verify firewall administration is restricted to authorized individuals.<br>Examine a sample of access rules to verify that only authorized individuals can perform firewall administration. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| j) Run firewalls and routers on dedicated hardware. All non-firewall-related software such as compilers, editors, and communication software must be deleted or disabled. | Examine documentation to verify that non-firewall related software is deleted or disabled from firewalls and routers.<br>Examine a sample of firewalls and routers to verify they are dedicated hardware from which all non-firewall related software has been deleted or disabled. |
| k) Implement daily, automated analysis reports to monitor firewall activity. | Examine evidence that automated tools exist to monitor and analyze firewall activity.<br>Observe a sample of firewall analysis reports to verify that automated analysis is in place and that daily reports are produced. |
| l) Use unique administrator passwords for firewalls used by the both the security system and other network devices in the facility. | Examine authentication policies and procedures to verify passwords for firewall administration are different than passwords used for other network devices.<br>Interview personnel to verify that unique passwords are established for firewall administration. |
| m) Implement mechanisms to protect firewall and router system logs from tampering and to check the system integrity monthly. | Examine evidence that firewall and router system logs are protected from modification and a mechanism is in place to check their integrity monthly. |
| n) Explicitly permit inbound and outbound traffic to the security system networks. A rule must be in place to deny all other traffic. | Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the security system networks.<br>Examine a sample of firewall and router configurations to verify that:<br>• Approved inbound and outbound traffic for security system networks is explicitly permitted; and<br>• All other inbound and outbound traffic is specifically denied—for example by using an explicit “deny all” or an implicit “deny after allow” statement. |
| **C.5.4.2 Configuration** | |
| The firewalls must: | |
| a) Be configured to permit network access to required services only. | Examine policies and procedures for permitting network access to only required services.<br>Examine a sample of system configuration settings to verify that the configurations permit network access to only required services. |
| b) Be hardened in accordance with industry best practices if the firewall is implemented on a commercial off-the-shelf (COTS) operating system. | Examine policies and procedures for hardening firewalls in accordance with industry best practices.<br>Examine a sample of firewall configuration files to verify the configurations are consistent with industry-accepted hardening standards. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| c) Prohibit direct public access between any external networks and any system component that handles/stores security system data. | Examine policies and procedures for prohibiting direct public access between any external networks and any system component that stores cardholder data to verify existence.<br>Examine a sample of firewall and router configurations to verify there is no direct access between the Internet and system components that store cardholder data. |
| d) Implement IP masquerading or Network Address Translation (NAT) on the firewall between the DMZ and security system networks. | Examine policies and procedures for implementing IP masquerading or Network Address Translation (NAT) on the firewall between the DMZ and the security system networks to verify existence.<br>Examine a sample of firewall and router configurations to verify that methods are in place on the firewall between the DMZ and the security system networks to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet. |
| e) If managed remotely, be managed according to Section 4.6, "Remote Access," of the PCI CPP Logical Security Requirements. | If firewalls are managed remotely, examine policy and procedures documentation to verify management activities are managed according to Section 4.6 of the PCI CPP Logical Security Requirements. |
| f) Be configured to deny all services not expressly permitted. | Observe a sample of configuration settings to verify that all services not expressly permitted default to "deny." |
| g) Disable all unnecessary services, protocols, and ports. Authorized services must be documented with a business justification and be approved by the IT security manager. | Interview personnel to identify necessary services, protocols, and ports.<br>Examine a sample of systems/networks to verify that unnecessary services are disabled.<br>Examine a sample of services, protocols, and ports to verify that their business justification is documented, and they were approved by the IT security manager. |
| h) Disable source routing on the firewall. | Examine a sample of firewall configurations to verify that source routing is disabled. |
| i) Notify the administrator in real time of any items requiring immediate attention. | Examine policy and procedures to verify that administrator(s) are to be notified in real time of any items requiring immediate attention.<br>Interview administrators to verify that administrator(s) are notified in real time and that immediate attention is given when required. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| j) Maintain documented baseline security configuration standards for system components based on industry-accepted system hardening standards, which include, but are not limited to:<br>• Center for Internet Security (CIS).<br>• International Organization for Standardization (ISO).<br>• SysAdmin Audit Network Security (SANS) Institute.<br>• National Institute of Standards Technology (NIST).<br>• At a minimum, baseline configuration must address:<br>• User and group access security<br>• File and directory security<br>• Restricted services<br>• System update and installation standards<br>• Installed security software | Examine policies and procedures to verify that a baseline configuration has been established for the organization's system components and addresses at a minimum, but not limited to:<br>• User and group access security<br>• File and directory security<br>• Restricted services<br>• System update and installation standards<br>• Installed security software<br>Interview personnel to verify the baseline configuration standard is based on an industry standard. |
| k) The vendor must perform baseline security configuration checks in the SOC environment monthly or quarterly, with review after every configuration change. | Examine evidence to verify that the baseline security configuration was validated either:<br>• Monthly, or<br>• Quarterly with review after each configuration change.<br>Examine a sample of baseline configuration checks to verify that they occurred either:<br>• Monthly, or<br>• Quarterly with review after each configuration change. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| ***C.5.5 Anti-virus Software or Programs*** | |
| The vendor must: | |
| a) Define, document, and follow procedures to demonstrate:<br>• Identification of security alerts—e.g., subscribing to security alerts such as Microsoft and the Computer Emergency Response Team (CERT).<br>• Identification of system component updates that affect the supportability and stability of operating systems, software drivers, and firmware components.<br>• Inventory of current systems in the environment including information about installed software components and running services. | Examine policies and procedures documentation to verify coverage of:<br>• Identification of security alerts—e.g., subscribing to security alerts such as Microsoft and the Computer Emergency Response Team (CERT)<br>• Identification of system component updates that affect the supportability and stability of operating systems, software drivers, and firmware components<br>• Inventory of current systems in the environment including information about installed software components and about running services<br>Interview personnel to ensure procedures are known and followed. |
| b) Deploy anti-virus software on all systems potentially affected by malicious software—e.g., personal computers and servers. | Examine a sample of system components potentially affected by malicious software to verify that anti-virus software is deployed. |
| c) Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs. | Examine a sample of system components to verify that:<br>• Anti-virus software is present and running.<br>• Activity logs are generated. |
| d) Check for anti-virus updates at least daily and install updates in a manner consistent with Patch Management. Documentation must show why any updates were not installed. | Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date.<br>Examine a sample of systems to verify that either updates (based upon alerts collected as part of 6.6.1.a) were applied or documentation exists for why they were not. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| ***C.5.6 Remote Management*** | |
| *This section defines the remote connectivity of the managed vendor facility, the SOC, and third-party hosted locations.* | |
| **C.5.6.1 Remote Connection Methods** | |
| a) A managed vendor facility security system can only be connected to the SOC.<br>***Note:*** *A managed vendor facility is not permitted to be connected to the security system of another managed vendor facility.* | Examine network topology diagrams to verify that only a managed vendor facility can be connected to the SOC |
| b) Event Monitoring:<br>• Where a SOC is used for Event Monitoring, the SOC will be connected to the managed vendor facility security system and where applicable, to another SOC or SOCs of the same operational type using HTTPS/TLS secure communications.<br>• System administration of the managed vendor facility's security system is not permitted over this type of remote connection. | Examine policies and procedures to verify that remote access is NOT permitted for the administration of the managed vendor facility's security system. |
| c) Administration Services:<br>• Administration Services can be managed from a SOC or a location that meets the requirements of a Security Control Room (SCR). The location will be connected to the individual managed vendor facility security system and, where applicable, to another SOC or SOCs of the same operational type using VPN secure communications.<br>• Remote access for Administration Services must use a VPN that meets the requirements of Section C.6.7.3, "Virtual Private Network (VPN)." | Examine policies and procedures to verify that Administration Services are only managed from a SOC or a location that meets the requirements of an SCR.<br>Examine policies and procedures to verify that connections from the SOC to another SOC or managed vendor facility security system are done using a VPN meeting the requirements of Section C.6.7.3 (VPN) |
| d) Where a SOC is used for both monitoring and administration services, the services must be segregated using dedicated hardware to ensure there is no possibility of incorrect access. | Examine policies and procedures to verify that if a SOC is used for both monitoring and administration services, the services are segregated using dedicated hardware to ensure there is no possibility of incorrect access. |
| e) External third parties must not have access for purposes other than read-only system data on live monitoring systems. | Ensure policies and procedures to verify that external third parties do not have access to live monitoring systems other than read-only. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| **C.5.6.2 Remote Connection Conditions** | |
| a) Remote access is permitted only for the administration services of the network or system components. | Examine policies and procedures to verify that remote access is permitted only for the administration of the network or system components.<br>Examine a sample of users with remote access to verify such access is permitted only for the administration of the network or system components. |
| b) Remote access for administration services is permitted only from pre-determined and authorized locations using vendor-approved systems. | Examine a sample of remote access system configurations and access logs to verify access is accepted only from pre-determined and authorized locations using vendor-approved systems. |
| c) Access using personally owned hardware is prohibited. | Examine policies and procedures to verify that remote access using a personally owned device is prohibited.<br>Examine a sample of remote access system configurations and access logs to verify that remote access from personally owned devices is not permitted. |
| d) Remote access is not permitted where qualified personnel are temporarily off-site and remote access is a convenience. | Examine policies and procedures to verify that remote access is not permitted when qualified personnel are temporarily off-site. |
| e) The remote access process must be fully documented and include at least the following components:<br>• System components for which remote access is permitted.<br>• The location from which remote access is permitted.<br>• The conditions under which remote access is acceptable.<br>• Users with remote access permission.<br>• The access privileges applicable to each authorized user. | Examine policies and procedures to verify the remote access process is fully documented and includes the following components but is not limited to:<br>• System components for which remote access is permitted.<br>• The location from which remote access is permitted.<br>• The conditions under which remote access is acceptable.<br>• Users with remote access permission.<br>• The access privileges applicable to each authorized user. |
| f) All access privileges must be validated on a quarterly basis by an authorized individual. | Examine documentation from a sample of reviews to verify that remote access privileges are reviewed at least quarterly by an authorized individual. |
| g) The vendor must: | Examine policies and procedures to verify the following, at a minimum: |
| i. Ensure that systems allowing remote connections accept connections only from preauthorized source systems. | Remote administration is predefined and preauthorized by the vendor. |
| ii. Ensure remote administration is predefined and preauthorized by the vendor. | Remote administration is predefined and preauthorized by the vendor. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| iii. Ensure remote changes comply with change-management requirements as outlined in Section C.6.13, "Change Management." | Remote changes comply with change-management requirements as outlined in Section C.6.13, "Change Management." |
| iv. Ensure that all remote access locations are included in the facility assessment and meet these requirements. | All remote access locations are included in the facility's compliance assessment and meet these requirements. |
| v. Be able to provide evidence of compliance validation for any remote access location. | The vendor is able to provide evidence of compliance validation for any remote access location. |
| vi. Ensure that non-vendor staff performing remote administration maintains liability insurance to cover potential losses. All personnel performing remote administration must meet the same pre-screening qualification requirements as employees working in high-security areas. | Interview a sample of non-vendor staff performing remote administration and verify that they maintain liability insurance to cover potential losses.<br>Examine policies and procedures to verify that personnel performing remote administration must meet the same pre-screening qualification requirements as employees working in high security areas. |
| vii. All remote access must use a VPN that meets the requirements in the following section. | Examine a sample of remote access to verify that remote access occurs using a VPN that meets the requirements of Section 6.7.3, "Virtual Private Network (VPN)." |
| **C.5.6.3 Virtual Private Network (VPN)** | |
| a) For remote access, VPNs must start from the originating device—e.g., PC or off-the-shelf device specifically designed for secure remote access—and terminate at either the target device or the SOC firewall. If the termination point is the firewall, it must use IPSec or at least a TLS connection in accordance with PCI DSS Requirement 4.1 to the target device. | Examine VPN system documentation and a sample of configuration settings to verify that:<br>• For remote access, VPNs must start from the originating device and terminate at either the target device or the SOC firewall.<br>• When terminating at the SOC firewall, an IPSec or TLS connection to the target device is used in accordance with PCI Data Security Requirement 4.1. |
| b) For remote access to DMZ components, the VPN must terminate at the target device. | Examine policy and procedure documentation to verify that it defines that VPN tunnels for remote access to DMZ components must terminate at the target device. |
| c) SSL and TLS 1.0/1.1 are expressly prohibited in connection with the aforementioned. | Examine a sample of system configurations to verify that for remote access to DMZ components, SSL and TLS 1.0/1.1 are disabled. |
| d) Traffic on the VPN must be encrypted using Triple DES with at least double-length keys or Advanced Encryption Standard (AES). | Examine a sample of system configurations to verify that only the listed algorithms are implemented |
| e) Modifications to the VPN must be in compliance with the change-management requirements as outlined in Section C.6.13, "Change Management." | Examine a sample of modifications made to VPN configurations and verify that changes are in compliance with the change-management requirements as outlined in Section C.6.13, "Change Management." |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| f) Mechanisms—e.g., digital signatures, checksums—must exist to detect unauthorized changes to VPN configuration and change-control settings. | Examine a sample of VPN configuration files and change-control settings to verify they are protected from unauthorized modifications using mechanisms such as digital signatures and checksums. |
| g) Multi-factor authentication must be used for all VPN connections. | Examine a sample of VPN system documentation and configuration settings to verify multi-factor authentication is used for VPN connections.<br>Observe a sample of VPN access processes to verify multi-factor authentication is used. |
| h) Access must be declined after three consecutive unsuccessful access attempts. | Examine a sample of system component configuration setting to verify that authentication parameters are set to require that user accounts be locked out after not more than three consecutive invalid logon attempts. |
| i) Access counters may only be reset by an authorized individual after user validation by another authorized individual. | Examine documentation for access counter resets to verify that it is only reset by an authorized individual after user validation by another authorized individual. |
| j) The connection must time out within five minutes if the session is inactive. | Examine a sample of system component configuration settings to verify that system/session idle time-out features have been set to five minutes or less. |
| k) Remote access must be logged, and the log must be reviewed weekly for suspicious activity. Evidence of log review must be maintained. | Examine documented procedures to verify remote access logs are reviewed at least weekly to identify suspicious activity and that evidence of log review is retained.<br>Examine a sample of system configurations and audit logs to verify that remote access is logged, and that logs are reviewed. |
| l) VPN traffic using Internet Protocol Security (IPSec) must meet the following additional requirements:<br>• Tunnel mode must be used except where communication is host-to-host.<br>• Aggressive mode must not be used for tunnel establishment.<br>• The device authentication method must use certificates obtained from a trusted Certificate Authority.<br>• Encapsulating Security Payload (ESP) must be used to provide data confidentiality and authentication.<br>• The Perfect Forward Secrecy (PFS) option of Internet Key Exchange (IKE) must be used to protect against session key compromise. | Examine a sample of VPN configuration files to verify that the following requirements, at a minimum, are met:<br>• Tunnel mode must be used except where communication is host-to-host.<br>• Aggressive mode must not be used for tunnel establishment.<br>• The device authentication method must use certificates obtained from a trusted Certificate Authority.<br>• Encapsulating Security Payload (ESP) must be used to provide data confidentiality and authentication.<br>• The Perfect Forward Secrecy (PFS) option of Internet Key Exchange (IKE) must be used to protect against session key compromise. |

.

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| ***C.5.7 IT Infrastructure Requirements*** | |
| *The following defines the different IT infrastructure types that can be used for the SOC environment, whether internal to a certified location or using an external third-party hosting service provider. Each type has specific criteria to follow to ensure appropriate levels of security are achieved.* | |
| **C.5.7.2 PCI CP Certified Vendor Location, external to the SOC** | |
| a) IT Equipment that manages the SOC must be:<br>• Housed within a facility certified to the PCI Card Production and Provisioning Standard.<br>• Housed within a location that meets the requirements defined for a Security Control Room within the PCI Card Production and Provisioning Physical Security Requirements. | Examine documentation to verify that IT Equipment that manages the SOC is:<br>• Housed within a facility certified to the PCI Card Production and Provisioning Standard and is housed within a location that meets the requirements defined for a Security Control Room within the PCI Card Production and Provisioning Physical Security Requirements.<br>Observe to verify that IT Equipment that manages the SOC is:<br>• Housed within a facility certified to the PCI Card Production and Provisioning Standard.<br>• Housed within a location that meets the requirements defined for a Security Control Room within the PCI Card Production and Provisioning Physical Security Requirements. |
| **C.5.7.3 PCI CP Certified Vendor Location, internal to the SOC.** | |
| a) IT Equipment that manages the SOC must be:<br>• Housed within the SOC.<br>• Housed in a separated room under access control.<br>• Monitored by CCTV surveillance. | Examine documentation to verify that IT Equipment that manages the SOC is:<br>• Housed within the SOC<br>• Housed in a separated room under access control<br>• Monitored by CCTV surveillance<br>Observe to verify that IT Equipment that manages the SOC is:<br>• Housed within the SOC<br>• Housed in a separated room under access control<br>• Monitored by CCTV surveillance |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| ***C.5.8 Wireless Networks*** | |
| **C.5.8.1 General** | |
| The vendor must: | |
| a) Implement a documented policy regarding wireless communications and clearly communicate this policy to all employees. | Examine usage policies to verify that they address wireless communications.<br>Interview a sample of personnel and validate that the policy is clearly communicated to all card production staff. |
| b) Identify, analyze, and document all connections. Analysis must include purpose, risk assessment, and action to be taken. | Examine a sample of connections to verify that connections are identified, analyzed, and documented including purpose, risk assessment, and action to be taken. |
| c) Use a wireless intrusion-detection system (WIDS) capable of detecting hidden and spoofed networks for all authorized wireless networks. | Examine output from recent wireless scans to verify that, at a minimum:<br>• The scan is performed for all wireless networks.<br>• Hidden and spoofed networks can be detected. |
| d) When using a wireless network, use the WIDS to conduct random scans within the SOC environments at least monthly to detect rogue and hidden wireless networks. | Examine output from recent wireless scans to verify that the WIDS is used to conduct random scans within the SOC environment at least monthly to detect rogue and hidden wireless networks. |
| e) Document, investigate, and take action to resolve any issues identified when unauthorized connections or possible intrusions are detected. The investigation must occur immediately. Resolution must occur in a timely manner. | Examine policies and procedures for resolving any issues identified when unauthorized connections or possible intrusions are detected to verify existence, including that investigations must occur immediately and resolutions occur in a timely manner.<br>Examine output from recent scan reports and verify that all unauthorized connections or possible intrusions are detected, investigated immediately, and resolved in a timely manner. |
| f) Use a scanning device that is capable of detecting rogue and hidden wireless networks, regardless of whether or not the vendor uses a wireless network. Random scans of the SOC environments must be conducted at least monthly. | Examine policies and procedures to verify that a scanning device is used for rogue and hidden wireless networks—regardless of whether or not the vendor uses a wireless network—and that random scans of the SOC environment occur at least monthly.<br>Examine a sample of output from recent scans to verify that the scanning device is used to conduct random scans of the SOC environment at least monthly. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| **C.5.8.2 Additional Requirements for using Wi-Fi** | |
| If the wireless network uses Wi-Fi based on IEEE 802.11, the vendor must ensure that the following requirements are met: | |
| a) Default SSID must be changed upon installation and must be at least 8 characters. | Examine vendor documentation to verify that default SSIDs are not used and new passwords are at least 8 characters.<br><br>Observe a sample via using the system administrator's help to verify that default SSIDs have been changed and the new passwords are at least 8 characters. |
| b) A log of media access-control addresses and associated devices (including make, model, owner, and reason for access) must be maintained, and a check of authorized media access-control addresses on the access point (AP) must be conducted at least quarterly. | Examine a sample of logs of media access-control addresses and associated devices to verify they include at least the make, model, owner, and reason for access.<br><br>Interview personnel to verify that a check of authorized media access-control addresses on the access point (AP) is conducted at least quarterly.<br><br>Examine a sample of scan reports and verify that checks of authorized media access-control addresses on the access point (AP) occur at least quarterly. |
| c) A media access control address-based access-control list (ACL) must be used for access control of clients. | Interview responsible personnel to verify the use of ACLs for access control of clients<br><br>Examine supporting documentation to verify a media access control address-based access-control list (ACL) is used for access control of clients. |
| d) Wi-Fi Protected Access (WPA) must be enabled if the wireless system is WPA-capable. | Examine a sample of configurations and scan reports to verify that, where capable, Wi-Fi Protected Access (WPA) is enabled. |
| e) Default passwords on the AP must be changed. | Examine supporting documentation to verify that default passwords on the AP are required to be changed upon installation.<br><br>Observe a sample via the system administrator's help to verify that default passwords on the AP are changed. |
| f) The management feature for the AP must be disabled on the wireless interface and must only be managed via the trusted, wired interface. | Examine configurations and verify that the management feature for the access point is disabled on the wireless interface and can only be managed via the trusted, wired interface. |
| g) The AP must be assigned unique Internet protocol (IP) addresses instead of relying on Dynamic Host. | Examine configurations and verify that an access point is assigned unique Internet protocol (IP) addresses instead of relying on Dynamic Host. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| ***C.5.9 Media Handling*** | |
| a) The vendor must have a documented removable-media policy that includes laptops, mobile devices, and removable storage devices—e.g., USB devices, tapes, and disks. | Examine the vendor's policies and procedures for removable media documentation to verify it exists and includes devices such as laptops, mobile devices, USB devices, tapes, and disks. |
| b) All removable media—e.g., USB devices, tapes, disks—within the SOC must be clearly labelled with a unique identifier and the data classification. | Observe a sample of removable media within the HSA to verify it is clearly labeled with a unique identifier and data classification. |
| c) All removable media must be securely stored, controlled, and tracked. | Observe the removable media storage location to verify the area is secure.<br>Examine the removable media check-in/out process to verify an audit trail is maintained and that it provides an accurate record of media possession. |
| d) All removable media within the SOC must be in the custody of an authorized individual, and that individual must not have the ability to decrypt any sensitive or confidential data contained within that media. | Examine a sample of checked-out, removable media within the HSA or the cloud-based provisioning environment to verify:<br>• The media is in the custody of the person to whom the media was issued.<br>• The individual is authorized to possess the media.<br>• That individual does not have the ability to decrypt any sensitive or confidential data contained on that media other than in compliance with procedures for handling sensitive or confidential data.<br>• The media does not contain clear-text confidential data. |
| e) A log must be maintained when media is removed from or returned to its storage location or transferred to the custody of another individual. The log must contain:<br>• Unique identifier<br>• Date and time<br>• Name and signature of current custodian<br>• Name and signature of recipient custodian<br>• Reason for transfer | Examine the media audit trail documentation to verify that it contains at least the following data points.<br>• Unique media identifier<br>• Date and time logged out and returned<br>• Name and signature of the current custodian<br>• Name and signature of custodian recipient<br>• Reason for transfer |
| f) Transfers of custody between two individuals must be authorized and logged. | Examine evidence that any transfer of checked out media is authorized and logged. |
| g) Transfer of removable media to and from the SOC must be authorized and logged. | Examine a sample of media that was removed from the HSA to verify that the removal was authorized and logged. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| h) Physically destroy any media containing secret or confidential data when it is not possible to delete the data so that it is no longer recoverable. | Examine evidence that media containing secret or confidential media is destroyed in a manner that makes it impossible to recover the data. |
| ***C.5.10 Security Testing and Monitoring*** | |
| **C.5.10.1 Vulnerability** | |
| The vendor must: | |
| a) Perform quarterly external network vulnerability scans using an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). | Examine policies and procedures to verify that quarterly external network vulnerability scans using an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC) are required.<br>Examine a sample of external vulnerability scans and verify that quarterly external vulnerability scans occurred in the most recent 12-month period and were completed by a PCI SSC Approved Scanning Vendor (ASV). |
| b) Perform internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system-component installations, changes in network topology, firewall-rule modifications, product upgrades). Scans after changes may be performed by internal staff. | Examine policies and procedures to verify that internal and external network vulnerability scans are required at least quarterly and after any significant change in the network.<br>Examine a sample (including the most recent significant change in the network) of internal and external network vulnerability scans to verify scans occur at least quarterly and after any significant change in the network. |
| c) Ensure all findings from network vulnerability scans are prioritized and tracked. Corrective action for high-priority vulnerabilities must be started within two working days. | Interview responsible personnel to verify that all findings from network vulnerability scans are prioritized and tracked, and corrective action for high-priority vulnerabilities is started within two working days.<br>Examine a sample of documentation to verify that findings from network vulnerability scans are prioritized and tracked, and corrective action for high-priority vulnerabilities is started within two working days. |
| d) Retain evidence of successful remediation and make this evidence available during site compliance evaluations upon request. | Interview responsible personnel to verify evidence of successful remediation is retained and available upon request. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| **C.5.10.2 Penetration** | |
| The vendor must: | |
| a) Perform internal and external penetration tests at least once a year and after any significant infrastructure changes. | Examine policies and procedures to verify that internal and external penetration tests are performed at least once a year and after any significant infrastructure changes.<br><br>Examine the most recent internal and external penetration tests to verify that the following requirements, at a minimum, were met: |
| i. The internal penetration test must not be performed remotely. | The internal penetration test was not performed remotely. |
| ii. Penetration tests must be performed on the network layer and include all SOC network components as well as operating systems. | Penetration tests were performed on the network layer and included all personalization network components as well as operating systems. |
| b) Penetration tests must be performed on the application layer and must include:<br>• Injection flaws—e.g., SQL injection<br>• Buffer overflow<br>• Insecure cryptographic storage<br>• Improper error handling<br>• All other discovered network vulnerabilities | Penetration tests were performed on the application layer and included at least the following:<br>• Injection flaws—e.g., SQL injection<br>• Buffer overflow<br>• Insecure cryptographic storage<br>• Improper error handling<br>• Insecure communications<br>• All other discovered high-risk network vulnerabilities |
| c) Ensure all findings from penetration tests are prioritized and tracked. Corrective action for high-priority vulnerabilities must be started within two working days. | Interview responsible personnel to verify that all findings from penetration tests are prioritized and tracked; and corrective action for high-priority vulnerabilities is started within two working days.<br><br>Examine a sample of documentation to verify that findings from penetration tests are prioritized and tracked; and corrective action for high-priority vulnerabilities is started within two working days. |
| d) Retain evidence of successful remediation and make this evidence available during site compliance evaluations upon request. | Interview responsible personnel to verify evidence of successful remediation is retained and available upon request. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| ***C.5.11 Intrusion-Detection Systems*** | |
| The vendor must: | |
| a) Use intrusion-detection systems (IDS) for network traffic analysis. IDS may be implemented as part of an intrusion-prevention system (IPS) if an IPS is used. These must be deployed, managed, and maintained across the vendor networks not only for intrusion detection and prevention but also to monitor all SOC network traffic. | Examine policies and procedures to verify that intrusion-detection systems are in place to monitor all traffic across the vendor networks, generated by machines within the perimeter, all SOC network traffic.<br><br>Examine a sample of system configurations and network diagrams to verify that intrusion-detection systems are in place to monitor all traffic across the vendor networks, generated by machines within the perimeter, all SOC network traffic. |
| b) Ensure the IDS alerts personnel to suspicious activity in real time. | Interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises in real time.<br><br>Examine a sample of records to verify the IDS alerts personnel to suspicious activity in real time. |
| c) Ensure the IDS monitors all traffic at the SOC network perimeter as well as at critical points inside the SOC network. | Examine system configurations and network diagrams to verify that intrusion-detection systems are in place to monitor all traffic:<br>• At the perimeter of the SOC network<br>• At critical points inside the SOC network |
| ***C.5.12 Change Management*** | |
| The vendor must: | |
| a) Ensure that change-control procedures address, at a minimum:<br>• That requests for changes are submitted by authorized users.<br>• Identification of components that will be changed.<br>• Documentation of impact and back-out procedures.<br>• Attestation of successful testing, when required.<br>• Maintenance of an audit trail of all change requests.<br>• Record of whether or not change was successful. | Examine change-control policies and procedures to verify the following are defined:<br>• Ensuring that requests for changes are submitted by authorized users<br>• Identification of components that will be changed<br>• Documentation of impact and back-out procedures<br>• Attestation of successful testing, when required<br>• Maintenance of an audit trail of all change requests<br>• Record of whether or not the change was successful |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| b) Ensure that network and system changes follow a documented change-management process and the process is validated at least every 12 months. | Examine a sample of changes to network and system components to verify changes follow the documented change-management process.<br>Examine documentation and supporting evidence to verify that the change-management process is validated at least every 12 months. |
| c) Ensure all changes are approved by the CISO or authorized individual prior to deployment. | Examine a sample of changes to network and system components to verify changes were approved by the CISO or authorized individual before deployment. |
| d) Ensure that the change-management process includes procedures for emergency changes. | Interview personnel and review documentation to verify that the change-management process includes procedures for emergency changes.<br>Examine a sample (if applicable) of emergency changes to verify they followed procedures. |
| e) Implement version identification and control for all software and documentation. | Examine documentation to verify the organization's change-management policies and procedures include requirements for version control and identification. |
| f) Ensure that the version identification is updated when a change is released or published. | Examine documentation to verify that version identification is updated when a change is released or published. |
| g) Implement a controlled process for the transfer of a system from test mode to live mode, and from live mode to test mode. | Examine documentation to verify the existence of a controlled process for the transfer of a system from test mode to live mode, and from live mode to test mode. |
| h) Ensure that both development and production staff must sign off on the transfer of a system from test to live, and from live to test. This sign-off must be witnessed under dual control. | Examine a sample of change-management documentation for system transfers from test to live and from live to test to verify that:<br>• Both development and production staff sign off on the transfer of a system from test to live, and from live to test; and<br>• This sign-off must be witnessed under dual control. |
| ***C.5.13 Configuration and Patch Management*** | |
| The vendor must: | |
| a) Implement a documented procedure to determine whether applicable patches and updates have become available. | Examine documented procedures to verify that they include determination of whether applicable patches and updates have become available. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| b) Make certain a process is implemented to identify and evaluate newly discovered security vulnerabilities and security patches from software vendors. | Examine documentation to verify that processes are defined to identify new security vulnerabilities and obtain security patches from appropriate software vendors. |
| c) Ensure that secure configuration standards are established for all system components. | Examine documentation to verify that secure configuration standards are established for all system components. |
| 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. | Examine configuration standards and verify there are requirements to remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. |
| e) Ensure that the configuration of all system components associated with data transmission, storage, and SOC activities is validated against the authorized configuration monthly. | Examine documentation to verify all system components associated with data transmission, storage, and personalization are validated against the authorized configuration monthly. |
| f) Ensure all systems used in support of the SOC networks are actively supported in the form of regular updates. | Examine documentation to verify that all systems used in support of the SOC networks are actively supported in the form of regular updates. |
| g) Evaluate and install the latest security-relevant patches for all system components within 30 days of their release (if they pass validation tests). | Examine a sample of system components and related software to:<br>• Compare the list of security patches installed on each system component to the most recent vendor security-patch list; and<br>• Verify the applicable vendor-supplied security patches are installed within 30 days of their release. |
| h) Verify the integrity and quality of the patches before application, including source authenticity. | Examine procedures to verify that a process is defined, the source of the patches is authenticated, and that the quality of the patch is validated before installation.<br>Interview personnel to verify that patch installation process conforms to written procedures. |
| i) Make a backup of the system being changed before applying any patches. The backup must be securely stored. | Examine a sample of system components and related software and compare the list of security patches installed against backup file entries to verify backups are performed.<br>Observe security control mechanisms for backups and verify they are in place and active.<br>Interview personnel and review patch update procedures to verify backups are required before applying patches. Identify controls for secure storage. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| j) Implement critical patches to all Internet-facing system components within seven business days of release. When this is not possible the CISO, IT security manager, or 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. | Examine policies and procedures related to security-patch installation to verify processes are defined for installation of critical patches to Internet-facing system components within 7 business days of release.<br><br>Examine a sample of Internet-facing system components and compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify that:<br><br>• Applicable, critical vendor-supplied security patches are installed within 7 days of release. OR<br>• Supporting documentation is in place recording that the CISO, IT security manager, and IT director understand and accept the risk and ensure implementation occurs within 30 business days. |
| k) Ensure that emergency hardware and software implementations comply with the procedures and validation requirements established for emergency implementations. | Examine the documented procedures for emergency hardware and software implementation.<br><br>Examine a sample of emergency and hardware and software changes to verify they follow documented procedures. |
| l) Ensure that emergency hardware and software implementations follow the configuration and patch management requirements in this section. | Examine a sample of emergency hardware and software implementations to verify that all configuration and patch management procedures are followed.<br><br>Interview personnel and review documentation to verify that emergency changes followed stated configuration and patch management requirements. |
| ***C.5.14 Audit Logs*** | |
| The vendor must: | |
| a) Ensure that audit logs exist for all networks and network devices in the vendor environment. This includes operating system logs, security software logs, or product logs and application logs containing security events. | Examine all networks and network devices in the vendor environment—including systems and applications connected to the cloud-based provision network—to ensure that audit logs are enabled and function correctly.<br><br>Interview personnel to ensure that audit trails are enabled and active for identified items, including operating system logs, security software logs, product logs, and application logs containing security events. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| b) Ensure that audit logs include at least the following components:<br>• User identification<br>• Event type<br>• Valid date and time stamp<br>• Success or failure indication<br>• Origination of the event<br>• Identity or name of the affected data, system component, or resources<br>• Access to audit logs<br>• Changes in access privileges | Examine the audit logs to ensure they contain the required components.<br>• User identification<br>• Event type<br>• Valid date and time stamp<br>• Success or failure indication<br>• Origination of the event<br>• Identity or name of the affected data, system component, or resources<br>• Access to audit logs<br>• Changes in access privileges |
| 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 include authentication, authorization, and directory servers. At a minimum, log review frequency must adhere to the following:<br>• Immediate (real time) response to threats designated as alerts for high risk associated events<br>• Daily review of IDS and IPS systems<br>• Weekly review for wireless access points and authentication servers<br>• Monthly review for routers<br>• Monthly review of user account audit logs for databases, application, and operating systems. | Examine policies and procedures to verify that procedures are defined for reviewing and reporting of unusual activity and include requirements for log frequency as stated in the requirement.<br>Examine a sample of each log type and frequency and obtain evidence that log review was performed. Unless specified by the procedures, the order of assessment is at the discretion of the auditor.<br>Interview personnel to verify the stated policies and procedures are known and followed. |
| d) Verify at least once a month that all systems are meeting log requirements. | Examine evidence that demonstrates monthly verification that systems are meeting the logging requirements.<br>Interview personnel to ensure they verify at least monthly that systems are meeting the logging requirements. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| e) Ensure that logs for all critical systems 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. | Examine logs for critical systems to:<br>• Verify that logs are securely backed up daily.<br>• Verify that logs are accessible online for at least three months.<br>• Verify that logs are retained offline for one year.<br>For both online and backed-up audit logs, review relevant security controls to ensure access is appropriate. |
| f) Protect and maintain the integrity of the audit logs from any form of modification. | Examine relevant security controls for both online and backed-up audit logs to ensure the ability to modify or delete audit logs is prohibited. |
| g) Implement a security-incident and event-logging framework for its organization. | Examine documentation to ensure existence of an incident-response process.<br>interview personnel to verify they are aware of their security-incident and event-logging framework.<br>Examine log entries to verify framework is active and in use. |
| ***C.5.15 Backup and Recovery for SOC Networks*** | |
| a) The backup and recovery procedures for SOC environments must be documented. | Examine documentation to verify existence of procedures supporting the backup and recovery of the SOC environments must be documented. |
| b) The procedures must include the backup and recovery of hardware and software that support the SOC activity. | Examine documented procedures to verify they include requirements for the backup and recovery of hardware and software that support the SOC activity. |
| c) The procedures must differentiate between and address short-term and long-term service outages. | Examine documented procedures to verify they include requirements for both short-term and long-term service outages. |
| d) The vendor must protect backup copies from intentional or unintentional modifications or destruction. | Examine applicable access-control lists to ensure the ability to modify or delete audit backups is prohibited. |
| e) Backups must be encrypted and protected equivalent to the primary data as delineated in Section 3.1, “Classifications,” of the PCI CPP Logical Security Standards. | Interview personnel and review documentation to identify backups and their data classification.<br>Examine documentation about the system used to protect backups to ensure that it is protected equivalent to the primary data—e.g., including the vendor, type of system/process, and the encryption algorithms used to encrypt backups.<br>Examine a sample of backups and verify strong cryptography, with associated key-management processes and procedures where used. |

## C.5 Data Security

| Requirement | Test Procedure |
|---|---|
| f) Controls must be established to prohibit creating unauthorized backups. | Examine existing security controls to verify they prohibit the creation of unauthorized backups. |
| g) If the recovery procedures include an alternate processing site, the alternate site must be VPA-approved for SOC activities before any SOC activity service may begin at the alternate site. | Interview personnel and review documentation to identify alternate processing sites.<br>Examine documentation to verify that the alternate site has been VPA-approved to perform provisioning services before the provisioning occurs. |

## C.6 Software Design and Development

| Requirement | Test Procedure |
|---|---|
| ***C.6.1 General*** | |
| The vendor must: | |
| a) Document the design, development, and maintenance processes. | Examine documentation of design, development, and maintenance processes to verify existence. |
| b) Ensure these activities are based on industry standards and security is an integral part of the software lifecycle process. Web applications must be developed based on secure coding guidelines such as the OWASP Guide, SANS CWE Top 25, and CERT Secure Coding. | Examine policies and procedures to verify that:<br>• The software life cycle process aligns with industry standards; and<br>• Web application development is based on recognized secure coding guidelines. |
| c) Document all software components for each system and describe the functionality provided. | Examine documentation to verify it covers software components for each system and describes how they function. |
| d) Protect any software backup copies from accidental destruction. | Examine a sample of backups to verify they are adequately protected from accidental destruction. |
| ***C.6.2 Design*** | |
| a) The vendor must document the flow of SMS data within the environment from the receipt/generation to end of lifecycle. | Examine data-flow diagrams for SMS data within the environment from the receipt/generation to end of lifecycle.<br>Interview personnel to verify documentation includes information to support the receipt/generation of data to the end of the lifecycle. |

## C.6 Software Design and Development

| Requirement | Test Procedure |
|---|---|
| ***C.6.3 Development*** | |
| The vendor must: | |
| a) Ensure access to source code for applications used on the SOC network is restricted to authorized personnel only. | Interview personnel to identify locations of application source code.<br>Examine system configuration and access-control lists to identify users and processes that have access to source code components.<br>Examine approval records to ensure access to source code was authorized. |
| b) Ensure separation of duties exists between the staff assigned to the development environment and those assigned to the SOC environment. | Examine policies and procedures to verify a separation of duties between personnel assigned to the development/test environments and those assigned to the SOC environment.<br>Examine access-control settings to verify that access controls are in place to enforce separation of personnel assigned to the development/test environments and the SOC environment(s). |
| c) Ensure that software source code is restricted to only authorized staff. Staff access of source code must follow a documented process. The authorizations and approvals must be documented. | Examine system configuration and access-control lists to identify users and processes that have access to source code components.<br>Examine documented policies and procedures for granting access to source code and verify authorizations and approvals are required.<br>Examine a sample of access request records to verify the access followed the documented process and was authorized. |
| ***C.6.4 Software implementation*** | |
| The vendor must: | |
| a) Establish and maintain a documented software release process. Quality assurance must include testing of the code for security issues prior to any software releases. | Interview personnel to verify a software release process exists and is in use.<br>Examine documentation to verify a quality assurance process is required as part of the software release process and testing of code is performed before software is released.<br>Examine a sample of recent software updates and identify evidence to verify testing of the code was performed. |

## C.6 Software Design and Development

| Requirement | Test Procedure |
|---|---|
| b) For internally developed software, ensure that security testing includes verification that temporary code, hard-coded keys, and suspicious code are removed. | Examine policies/procedures to identify testing processes for internally developed software.<br>Examine documentation to verify it addresses removing temporary code, hard-coded keys, and suspicious code.<br>Examine a sample of recent internally developed software updates and verify steps to remove temporary code, hard-coded keys, and suspicious code were performed. |
| c) Ensure all software implementation complies with Section C.6.13, "Change Management." | Examine a sample of recent software updates to verify they comply with Section C.6.13, "Change Management." |
| d) Test software prior to implementation to ensure correct operation. | Examine a sample of recent software updates and verify evidence exists that testing software prior to implementation was performed. |
| e) All testing must be done on a dedicated test environment. | Interview personnel to identify the controls in place to prevent debugging in the production environment.<br>Examine policies/procedures to verify they address prevention of debugging within production environment. |
| f) Test and live environments must be segregated. | Examine policies and procedures to verify that test and live environments are required to be separated |
| g) Prevent debugging within SOC environment. | Examine policies and procedures to verify that debugging is not allowed within the SOC environment. |
| h) Have a predefined PC device configuration for PC devices used within the SOC environment. | Examine policies and procedure that specify a pre-defined PC device configuration for PC devices used within the SOC environment. |
| i) Implement an approval process for all software beyond the standard PC device configuration for PC devices used within the SOC environment. | Examine policies and procedures to verify that an approval process exists for any PC software installed beyond the standard configuration |
| j) Ensure no unauthorized software can be installed. | Examine policies and procedures to verify that unauthorized software is not allowed to be installed |
| k) Ensure all software is transferred from development to production in accordance with the change-control process. | Examine policies and procedures to verify that all software transferred from development to production is required to follow the change-control process.<br>Examine a sample of software installs to verify they followed the change-control process. |

## C.7 User Management and System Access Control

| Requirement | Test Procedure |
|---|---|
| ***C.7.1 User Management*** | |
| The vendor must: | |
| a) Ensure that procedures are documented and followed by security personnel responsible for granting access to vendor's networks, applications, and information. | Interview personnel to identify those authorized to perform and processes followed for granting access to vendor's network, applications, and information.<br>Examine documented procedures to ensure they address granting access to vendor's networks, applications, and information.<br>Examine a sample of recent access requests to verify they were processed by authorized personnel and in accordance with documented procedures. |
| b) Restrict approval and level of access to staff with documented business need before access is granted. At a minimum, documented approvals must be retained while the account is active. | Examine policies/procedures to ensure they address that:<br>• Approval and level of access must be restricted to those with a documented business need before access is granted; and<br>• Documented approvals of access in place must be retained while the account is active. |
| c) Restrict systems access by unique user ID to only those individuals who have a business need. | Examine a sample of user accounts to verify each individual associated with a unique user ID has a documented, valid business need for the system access. |
| d) Only grant individuals the minimum level of access sufficient to perform their duties. | Interview security administration personnel to verify access is granted based on least-privilege principles sufficient to perform their duties.<br>Examine policies/procedures to verify they require that access be granted based on least-privilege principles sufficient to perform their duties.<br>Examine a sample of recent access requests to verify user access is limited to least privilege and based on documented business need. |
| e) Make certain that systems authentication requires at least the use of a unique ID and password. | Examine policies/procedures for system access to verify they require at least the use of a unique ID and password.<br>Examine system authentication settings and verify that user IDs in the system are unique and in order to gain access, a password is required. |

## C.7 User Management and System Access Control

| Requirement | Test Procedure |
|---|---|
| f) Restrict administrative access to the minimum number of individuals required for management of the system. | Interview management to understand the minimum number of administrative user resources required to support the personalization environment.<br><br>Examine user ID lists and security privileges to identify users with administrative access and verify the number of users with administrative access aligns with management's expectations. |
| g) Ensure that group, shared, and generic accounts and passwords are disabled wherever the system supports unique values. | Examine polices/procedures to verify they require that group, shared, and generic accounts and passwords are disabled wherever the system supports unique values.<br><br>Examine a sample of system components and user ID lists to verify group, shared, and generic accounts and passwords are disabled. |
| h) 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. | Interview system administration personnel to identify existence of generic accounts and how their usage is controlled.<br><br>Examine policies/procedures for the management of generic administrative accounts that cannot be disabled. Verify these accounts are used only when unique administrator sign-on credentials are not possible and only in an emergency.<br><br>Examine system security event log to identify when applicable generic administrative accounts were used and verify there is supporting documentation that authorizes their use in an emergency. |
| i) 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 Section C.6.2, "Password Control." | Interview system administration personnel to verify password-management practices require that generic administrative passwords are managed under dual control and in accordance with Section 6.2<br><br>Examine policies/procedures for the management of generic administrative account passwords and verify procedures require that such passwords be managed under dual control and in accordance with Section C.6.2, "Password Control." |
| j) Validate all system access at least quarterly. | Interview personnel to verify system access is re-validated at least quarterly.<br><br>Examine validation evidence to verify the activity is performed. |
| k) Revalidate employee access to any systems upon a change of duties. | Interview personnel to verify any staff access is revalidated when there is a change in duties.<br><br>Examine a sample of HR transfer records and verify that revalidation was performed. |
| l) Ensure that access controls enforce segregation of duties. | Interview personnel to identify that policies/procedures support segregation of duties. See glossary definition, "Segregation of Duties," in the Security Requirements. |

## C.7 User Management and System Access Control

| Requirement | Test Procedure |
|---|---|
| m) Strictly limit privileged or administrative access and ensure such access is approved by both the user's manager and the IT security manager. | Interview personnel to identify controls that limit privileged or administrative access.<br>Examine access-control settings to ensure access confirms to stated policies.<br>Examine a sample of administrative-access requests and verify access was approved by the user's manager and IT Security Manager. |
| n) Establish management oversight of privileged access to ensure compliance with segregation of duties. | Interview personnel to identify controls that provide oversight of privileged access and compliance with segregation of duties policies.<br>Examine policies/procedures to verify they require oversight of privileged access that ensures compliance with segregation of duties.<br>Examine evidence—e.g., audit logs—to verify management oversight is performed. |
| o) Ensure that all privileged administrative access is logged and reviewed weekly. | Examine policies/procedures to verify that they require weekly review of privileged administrative access.<br>Examine evidence—e.g., access logs—to verify reviews are performed according to policies and procedures. |
| ***C.7.2 Password Control*** | |
| **C.7.2.1 General** | |
| The vendor must: | |
| a) Implement a policy and detailed procedures relating to the generation, use, renewal, and distribution of passwords. | Examine policy and detailed procedures to identify processes for generation, use, renewal, and distribution of passwords. |
| b) Implement procedures for handling lost, forgotten, and compromised passwords. | Examine policy and detailed procedures to identify processes for handling lost, forgotten, and compromised passwords.<br>Interview system administrators to validate adherence to procedures. |
| c) Distribute password procedures and policies to all users who have access to any information or system used as part of the SOC process. | Examine procedures for disseminating password procedures and policies to users with access to cardholder data or any system used as part of the personalization process.<br>Interview a sample of user population to verify password procedures and policies were distributed. |

## C.7 User Management and System Access Control

| Requirement | Test Procedure |
|---|---|
| d) Ensure that only users with administrative privileges can administer other users' passwords. | Examine procedures for managing user IDs and verify that only users with administrative privileges can administer user passwords.<br><br>Observe a sample of user password resets and verify only users with administrative privileges can perform a reset. |
| e) Not store passwords in clear text. | Examine system documentation and configuration settings to verify that passwords are not stored in clear text.<br><br>Examine a sample of system components and their password files to verify that passwords are unreadable during storage. Change all default passwords. |
| f) Change all default passwords. | Examine a sample of system components and attempts to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.) |
| **C.7.2.2 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. | Interview personnel to verify newly issued and reset passwords are set to a unique value for each user.<br><br>Examine a sample of system configuration settings to verify newly issued and reset passwords are set to a unique value for each user. |
| b) Newly issued passwords are changed on first use. | Examine system configuration settings to verify newly issued passwords are changed on first use. |
| c) "First use" passwords expire if not used within 24 hours of distribution. | Examine system configuration settings to verify that first-time passwords are set to expire if not used within 24 hours. |
| d) Systems enforce password lengths of at least 12 characters. | Examine the system configuration settings for a sample of system components to verify that password parameters are set to require a minimum length of at least 12 characters. |

## C.7 User Management and System Access Control

| Requirement | Test Procedure |
|---|---|
| e) Passwords consist of a combination of at least three of the following:<br>• Upper-case letters<br>• Lower-case letters<br>• Numbers<br>• Special characters | Examine the system configuration settings for a sample of system components to verify that user passwords are set to require at least the following strength/complexity:<br>• Upper-case letters<br>• Lower-case letters<br>• Numbers<br>• Special characters |
| f) Passwords are not the same as user IDs. | Examine the system configuration settings for a sample of system components to verify passwords cannot be the same as the user ID. |
| g) Passwords are not displayed during entry. | Observe authentication procedures for entering a password and verify the password is not displayed as it is entered. |
| h) Passwords are encrypted during transmission and rendered unreadable when stored. | Examine password configurations to verify passwords are encrypted during transmission and rendered unreadable when stored.<br>Examine a sample of passwords in transit and in storage to verify password values are not in clear text. |
| i) Passwords have a maximum life not to exceed 90 days and a minimum life of at least one day. | Examine the system configuration settings for a sample of system components to verify that user password parameters are set to have a maximum life of not more than 90 days and a minimum life of at least one day. |
| j) When updating passwords, the system prevents users from using a password that is the same as one of their previous four passwords. | Examine the system configuration settings for a sample of system components to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords. |
| k) The user's identity is verified prior to resetting a user password. | Interview system administration personnel to verify the user's identity is verified prior to resetting a user password.<br>Examine password reset procedures to verify the user's identify is verified prior to resetting a user password.<br>Observe a password reset request to verify user identify is verified. |

## C.7 User Management and System Access Control

| Requirement | Test Procedure |
|---|---|
| **C.7.2.3 Session Locking** | |
| The vendor must: | |
| a) 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. | Examine the system configuration settings for a sample of system components to verify that system/session inactivity time out has been set to 15 minutes or less.<br>Observe a user session to verify the user is logged out after 15 minutes, if the system does not permit session locking. |
| **C.7.2.4 Account Locking** | |
| a) Accounts that have been inactive for a specified period (with a maximum of 90 days) must be removed from the system. | Examine user accounts to verify that any inactive accounts over 90 days old are either removed or disabled. |
| b) Systems must enforce the locking of a user account after a maximum of six unsuccessful authentication attempts. | Examine the system configuration settings for a sample of system components to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts. |
| 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. | Examine documented procedures to verify that accounts can only be unlocked by either the security administrator or other authorized individual, or via an automated password reset mechanism.<br>Interview administrators to verify that an account is unlocked only after the identity of the user is verified.<br>Examine polices/procedures for automated password reset mechanisms to verify they require conformance to the stipulated criteria.<br>Observe the mechanism including the challenge/response criteria, for accounts that can be unlocked via an automated reset mechanism, to verify the questions are designed as stipulated in the requirement. |
| d) A user's account must be locked immediately upon that user leaving the vendor's employment until it is removed. | Examine policies/procedures to verify that user access is locked when the user leaves the vendor's employment.<br>Examine a record sample of users leaving vendor employment to verify that their account(s) were locked immediately. |
| e) A user's account must be locked immediately if that user's password is known or suspected of being compromised. | Examine policies/procedures to verify that any user account is immediately locked if the password is known or suspected of being compromised. |

## C.7 User Management and System Access Control

| Requirement | Test Procedure |
|---|---|
| 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:<br>• Remote access<br>• Database<br>• Application<br>• OS | Examine the system configuration settings and audit logs for a sample of system components to verify that lock-out activity is logged.<br>Examine documented procedures to verify access logs are reviewed at least weekly to identify suspicious activity. |

## C.8 Continuity of Service

| Requirement | Test Procedure |
|---|---|
| ***C.8.1 General Requirements*** | |
| a) The vendor must have a documented contingency plan to guarantee the continuation of service provided by the SOC and each defined managed vendor facility. | Examine documentation to verify existence of a contingency plan to provide for the continuation of service provided by the SOC and each defined managed vendor facility. |
| b) SOC and defined managed vendor facilities data must be backed up for recovery purposes in case of critical business interruption. | Examine documentation to verify that SOC and defined managed vendor facilities data must be backed up for recovery purposes in case of critical business interruption.<br>Interview personnel to verify that data backup occurs as defined in the documentation. |
| ***C.8.2 SOC Infrastructure***<br>***Note:*** *Information based on Uptime Institute definitions for "Concurrently Maintainable Site Infrastructure"* | |
| The SOC infrastructure must meet specific requirements to ensure an adequate level of continued service is maintained. The following points are the minimum of what is needed to provide to stable service: | |
| a) Each SOC supplied with at least two independent internet connections to provide suitable fail-over. This enables all local sites serviced by the SOC to maintain connectivity with the SOC. | Examine documentation to verify the existence of at least two independent internet connections to provide suitable fail-over. |

## C.8 Continuity of Service

| Requirement | Test Procedure |
|---|---|
| b) Each SOC location must have auxiliary power or battery backup system to ensure all associated equipment used by the SOC is fully supported at all times. | Examine documentation to verify that each SOC location has auxiliary power or battery backup system to ensure all associated equipment used by the SOC is fully supported at all times. |
| c) Recovery point objectives must be defined as part of SLAs to ensure minimal data loss at SOC. Source data at local site remains under the control of current requirements. | Examine documentation to verify that recovery point objectives are defined as part of SLAs to ensure minimal data loss at SOC. |
| ***C.8.3 Performance Testing*** | |
| a) Each SOC must test quarterly to ensure that the level of resilience and redundancy is of sufficient adequacy to ensure continued operation for the support of the defined managed vendor facilities. The testing must include, but not limited to:<br>• Application performance when switched between SOCs and/or the defined managed vendor facilities.<br>• Hardware performance to ensure appropriate levels of redundancy which minimizes impacts of SOC and/or the defined managed vendor facility operations for potential outages. | Examine documentation to verify that each SOC tests quarterly to ensure that the level of resilience and redundancy is of sufficient adequacy to ensure continued operation for the support of the defined managed vendor facilities and the testing includes:<br>• Application performance when switched between SOCs and/or the defined managed vendor facilities.<br>• Hardware performance to ensure appropriate levels of redundancy which minimizes impacts of SOC and/or the defined managed vendor facility operations for potential outages. |
| b) Each SOC must undergo an annual internal review to ensure the adequacy of meeting its prescribed SLAs. The following points must be included, at a minimum, but not limited to:<br>• Standard Operating Procedure review.<br>• Event Matrix review to ensure correct resource level is maintained.<br>• SOC Operational team training.<br>• SOC Operational team performance in the event of an outage. | Examine documentation to verify that each SOC undergoes an annual internal review to ensure the adequacy of meeting its prescribed SLAs that includes:<br>• Standard Operating Procedure review.<br>• Event Matrix review to ensure correct resource level is maintained.<br>• SOC Operational team training.<br>• SOC Operational team performance in the event of an outage. |
| c) For each test performed above, a report must be created which details the following points:<br>• Scope of test (included the location tested/reviewed).<br>• Names of all individuals who were involved in the test/review.<br>• Date of the test/review.<br>• Evidence of the performance of the scoped area.<br>• List of all issues that require action. | Examine documentation to verify that the SOC produces a report that details the following for this Performance Testing Section:<br>• Scope of test (included the location tested/reviewed).<br>• Names of all individuals who were involved in the test/review.<br>• Date of the test/review.<br>• Evidence of the performance of the scoped area.<br>• List of all issues that require action. |

## C.8 Continuity of Service

| Requirement | Test Procedure |
|---|---|
| d) Each reported issue must be categorized and suitable timescales applied, as defined in the vendor policies. | Examine documentation to verify that each reported issue must be categorized and suitable timescales applied, as defined in the vendor policies. |
| e) The Corporate Security Director must review each report on completion. | Interview personnel to verify the Corporate Security Director reviews each report upon completions. |

# Glossary

| Term | Definition |
|---|---|
| **Access Credentials** | The mechanism for identifying a user on the access-control system—e.g., Security Pass, ID Badge, Biometrics, Mobile Phone Tokens. |
| **Administration Services** | Administration-related activities that are required for management of the SMS and the managed vendor facility security systems |
| **Anti-pass-back** | A security mechanism preventing an access card or similar device from being used to enter an area a second time without first leaving it (so that the card cannot be passed back to a second person who wants to enter). |
| **Area** | Area is an unenclosed space, with the exception of the HSA. |
| **Armored Vehicle** | The armored vehicle is designed to protect and ensure the well-being of the transported individuals. These vehicles are designed to resist attempts at robbery or hijacking through the use of bullet-resistant glass and reinforced shell/cab to protect occupants. If the cargo area itself is not armored, additional stipulations apply. |
| **Authorized Personnel** | Card production staff who have been authorized by the physical security manager or other executive to undertake specific roles or functions |
| **Card Components** | This includes sensitive materials such as, but not limited to<br>a) Holographic materials<br>b) Origination materials<br>c) Signature panels<br>d) Core sheets or cards printed with the brand mark<br>e) Chips<br>f) Materials containing any of the above |
| **Cardholder Data** | At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code. |
| **Card Manufacturer** | An entity that is responsible for producing cards on behalf of a card issuer. The set of services performed depends on its contractual relationship with the issuer and may include part, or all, of the card production process. |

| Term | Definition |
|---|---|
| **Card Manufacturing** | Card production process composed of the following phases:<br>a) Pre-press (card design layout, printing films, and printing plates generation)<br>b) White-plastic sheets printing<br>c) Sheets assembly<br>d) Sheets lamination<br>e) Sheets cutting or punching<br>f) Hologram and signature panel hot stamping |
| **Card Production Staff** | Employees and contractors of the Card Vendor. Card Production Staff applies to any employees or contractors who are involved in card production-related activities that could impact security, including administration, support activities, and IT infrastructure. |
| **Card Products** | Cards and the components required to manufacture a credit or debit card, such as plastic sheets, chips, contact plates, etc. |
| **Chip** | The integrated circuit that is embedded into a plastic card designed to perform processing or memory functions. See also Chip Card. |
| **Chip card** | A card or device embedded with an integrated circuit or chip that communicates information to a point-of-transaction terminal. Chip cards offer increased functionality through the combination of significant computing power and substantial data storage. |
| **Chip Embedding** | The process by which an integrated circuit is permanently attached to the plastic of a payment card to become an integral part of that card. |
| **Chip Personalization** | Any process that writes issuer-or cardholder-specific data to the integrated circuit on the card. Generally, includes:<br>a) Bank branch identification (optional)<br>b) Cardholder account number<br>c) Cardholder name<br>d) Validity dates<br>e) Company identification (optional) |
| **CISO** | Chief Information Security Officer. Senior-level executive within an organization responsible for establishing and maintaining programs to ensure information assets are adequately protected. |
| **Cloud-Based Provisioning** | Preparation and delivery of Host Card Emulation data to a device. |

| Term | Definition |
|---|---|
| **COTS** | Commercial off-the-shelf (consumer-grade) devices such as mobile phones and tablets. |
| **Data Preparation** | Any formatting, sorting, or other manipulation of personalization data in readiness for card production. |
| **Dual Control** | A process of utilizing two or more separate persons operating together to protect sensitive functions or information whereby no single person is able to access or utilize the materials—e.g., a cryptographic key. |
| **Dual Presence** | Two or more individuals are in the HSA as a whole. This does not supplant or replace any requirements for dual control. For example, if three people are in the HSA, and two go into a room that requires dual control, the requirement for dual presence in the HSA as a whole is still met. |
| **Encoding** | Process by which data is written to the magnetic stripe located on the card. |
| **Embossing** | Personalization process that produces raised characters on the plastic card body. Embossing requirements may vary by card program, but generally include:<br>a) Cardholder account number<br>b) Cardholder name<br>c) Validity dates<br>d) Company identification (optional)<br>e) Payment brand security characters |

| Term | Definition |
|---|---|
| **Event** | Alarms and notices from the Security systems, including:<br>1. Unauthorized access attempts<br>2. Access attempts results<br>3. Anti-pass-back violations<br>4. Door open too long alarm<br>5. Forced door<br>6. Occupancy violations<br>a) Dual occupancy<br>b) Occupancy is greater or equal to one, with no motion detected within 15 or fewer minutes<br>c) Motion detected when occupancy equals zero<br>d) Motion detected inside the inner room of the loading bay when both intermediate and inner doors are closed<br>7. Duress Alarm activation<br>8. 24/7 monitored Intruder alarm device activation<br>9. Activations from managed vendor facilities where Intruder Alarm Systems are set<br>10. Intruder alarm system not set or unset within a scheduled time<br>11. Fire alarm activation<br>12. Auxiliary power or battery backup system is invoked<br>13. CCTV involuntary or voluntary disconnection |
| **Event Management** | Management of all security systems events from any managed vendor facility the under SOC responsibility. |
| **Facility** | Facility includes external and internal structures subject to the requirements of Section 2, “Facilities,” even if the vendor is leasing the space. |
| **Goods-Tools Trap** | Controlled area for transfer of materials between two areas. |
| **High Security Areas (HSAs)** | Areas in production facilities where card products, components, or data associated with personalization or mobile provisioning is stored or processed. |
| **Host Card Emulation (HCE)** | Technology that permits a device to perform the function of a payment card on a Near Field Communication (NFC)-enabled device or via In-Apps without the use of a secure element. |
| **Hostile Vehicle Mitigation (HVM)** | Methods to mitigate and reduce the risk of vehicles penetrating concerned areas |
| **HSA Rooms** | HSA rooms are enclosed spaces with controlled access in production facilities where card products, components, or data are stored or processed, and are where card-production activities occur. |

| Term | Definition |
|---|---|
| **Indent Printing Module** | Component of the personalization equipment that can be used to print account number and card validation code on the back of a card. These values are printed using a reverse italic font, which creates a physical indent on the card as per payment system specifications. This component is usually a separate module that is removable and can be replaced. When used by a payment system, the indent-printing module is a security feature that is sensitive and must be protected while in the vendor's possession. |
| **Investigation room** | Location for thorough event investigation and for non-SOC personnel to review the activities of the SOC with minimal disruption to operations. |
| **Issuer** | An entity licensed by a payment brand to issue cards and enter into a contractual relationship with the cardholder. |
| **Managed Vendor Facility** | Vendor facility where the security monitoring and administration is performed by a remote SOC. |
| **Mobile Provisioning** | The personalization (provisioning) of a commercial off-the-shelf (COTS) device, such as an NFC-equipped mobile phone with appropriate cardholder account information. The information is transmitted to the device by a process called over-the-air (OTA) provisioning or, alternatively, over-the-internet (OTI). |
| **Monitoring room** | Location specialized in event monitoring and management of the security systems of all managed vendor facilities. |
| **Non-Personalized Cards** | Cards that have been through the personalization process and have account data embossed or printed on the card and/or chip and magnetic stripe according to the scheme's rules but are not associated with a cardholder. |
| **OTA** | Over-the-air (OTA) refers to any process that involves the transfer of data (including applications) to the mobile device or any component within the mobile device via a mobile network. |
| **OTI** | Over-the-Internet (OTI) A remote connection from a security domain in the secure element to a backend server, using TLS over HTTP. |

| Term | Definition |
|---|---|
| **Participating Payment Brand** | A payment card brand that, as of the time in question, is then formally admitted as (or an affiliate of) a member of PCI SSC pursuant to its governing documents. At the time of this publication, Participating Payment Brands include PCI SSC's Founding Members and Strategic Members. |
| **Personalization** | The process of applying the account and, when required for the product, cardholder-specific data to the card, uniquely tying the card to a given account. This includes encoding the magnetic stripe, embossing the card (if applicable), and loading data on to the chip.<br>Personalization uses technology such as:<br>a) Embossing<br>b) Laser engraving<br>c) Thermal transfer<br>d) Indent printing |
| **Personalized Cards** | Cards that have been through the personalization process and are associated with an individual person. That person's name may be encoded, embossed, or printed on the card and/or chip and magnetic stripe according to the scheme's rules. |
| **Physical Security Manager** | Manager designated with the overall responsibility for physical security for the card production and provisioning facility. The physical security manager must not report to the production manager or director. There must also be a nominated deputy physical security manager to cover when the physical security manager is not on site. |
| **Pre-personalization (Chip Initialization)** | The process of replacing a transport key on a chip with an issuer-specific key and (optionally) activating the application. |
| **Public Network** | Network established and operated by a third-party telecommunications provider for the specific purpose of providing data transmission services for the public. Data over public networks can be intercepted, modified, and/or diverted while in transit. Examples of public networks include, but are not limited to:<br>▪ The Internet,<br>▪ Wireless technologies, including 802.11 and Bluetooth,<br>▪ Cellular technologies, for example, Global System for Mobile, communications (GSM), code division multiple access (CDMA),<br>▪ General Packet Radio Service (GPRS),<br>▪ Satellite communications. |
| **Secure or Sensitive Job or Task** | Jobs and tasks in association with card production or provisioning. |

| Term | Definition |
|---|---|
| **Secure Element** | Tamper-resistant module in a mobile device capable of hosting/embedding applications in a secure manner. A secure element may be an integral part of the mobile device or may be a removable element that is inserted into the mobile device for use. |
| **Security Components** | Security features that protect the card and may vary from payment brand to payment brand—e.g., holographic materials, signature panels, indent-printing modules when not installed. |
| **Security Manager** | See Physical Security Manager. |
| **Segregation of Duties** | Practice of dividing steps in a function among different individuals so as to keep a single individual from being able to subvert the process. |
| **Security Management System (SMS)** | Command and control software to manage all managed vendor facility security systems. |
| **Security Operation Center (SOC)** | High-security environment purposefully established for the monitoring and administration of the Security systems of the managed vendor facilities. |
| **Security System** | Managed vendor facility systems, such as Access Control, CCTV, and Intruder Alarm. |
| **Security system data** | All data from the security systems. |
| **Unpersonalized Cards** | Cards that have not been through a personalization process, are not unique, and have no cardholder or account data on them. |
| **Vendor** | The legal entity and its associated facilities that undertakes card production or provisioning. |
| **Vendor Agent** | A vendor agent is a separate organization or legal entity from the certified vendor that performs sales or promotional activities on behalf of a certified vendor. The agent is not authorized to physically take possession of a card or perform any card production or provisioning activities for which certification is required. Actual card production, provisioning and distribution services are performed by the certified vendor at an authorized facility. |
| **Vendor Program Administrator (VPA)** | The payment system contact person or team that manages vendor compliance with the security requirements defined in this document. |
| **Video Wall** | Special multi-monitor setup that consists of multiple computer monitors, video projectors, or television sets tiled together contiguously or overlapped in order to form one large screen. |