## ISO 27002

### A.5 Information Security Policies

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **5.1 Management Direction for Information Security** | | | |
| **5.1.1** Information security policy document. | | | |
| An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties. | **Identify the documented information security policy** examined. |  |  |
| **Describe how** the information security policy was examined to verify that it is published and disseminated to: | |
| All relevant personnel. |  |
| All relevant vendors and business partners. |  |
| **5.1.2** Review of the policies for information security. | | | |
| The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | **Identify** **the information security policies and procedures** reviewed to verify:   * The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. * The following information security responsibilities are specifically and formally assigned: |  |  |

### A.6 Organization of Information Security

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **6.1 Internal organization** | | | |
| **6.1.1** Information security roles and responsibilities | | | |
| All information security responsibilities should be defined and allocated. | **Identify** **the information security policies and procedures** reviewed to verify:   * The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. * The following information security responsibilities are specifically and formally assigned: |  |  |
| **6.1.2** Segregation of duties | | | |
| Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets. | **Identify the documented policy** reviewed to verify responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets. |  |  |
| **6.1.3** Contact with authorities | | | |
| Appropriate contacts with relevant authorities should be maintained. | **Identify the documented policy** reviewed to verify appropriate contacts with relevant authorities should be maintained. |  |  |
| **6.1.4** Contact with special interest groups | | | |
| Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained. | **Identify the documented policy** reviewed to verify appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained. |  |  |
| **6.1.5** Information security in project management | | | |
| Information security should be addressed in project management, regardless of the type of the project. | **Identify** the personnel interviewed to confirm that Information Security is addressed in project management. |  |  |
| **6.2**  **Mobile devices and teleworking** | | | |
| **6.2.1** Mobile device policy | | | |
| A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices. | **Indicate whether** mobile and/or employee-owned computers with direct connectivity to the Internet when outside the network are used to access the organization’s network. **(yes/no)** |  |  |
| *If “no,”* **identify** **the document** reviewed that explicitly prohibits mobile and/or employee-owned computers with direct connectivity to the Internet when outside the network from being used to access the organization’s network. |  |
| *If “yes,”* **identify** **the documented policies and configuration standards** that define the following:   * Personal firewall software is required for all mobile and/or employee-owned devices that connect to the Internet when outside the network, and which are also used to access the network. * Specific configuration settings are defined for personal firewall software. * Personal firewall software is configured to actively run. * Personal firewall software is configured to not be alterable by users of mobile and/or employee-owned devices. |  |
| **6.2.2** Teleworking | | | |
| A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites. | **Identify the documented policy** reviewed to verify policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites. |  |  |

### A.7 Human resources security

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **7.1 Prior to employment** | | | |
| **7.1.1** Screening | | | |
| Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. | **Identify the Human Resources personnel** interviewed who confirm background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment. |  |  |
| **Describe how** it was observed that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment. |  |
| **7.1.2** Terms and conditions of employment | | | |
| The contractual agreements with employees and contractors should state their and the organization’s responsibilities for information security. | **Describe how** it was verified that, per the security awareness program, all personnel: | |  |
| * Acknowledge that they have read and understand the information security policy (including whether this is in writing or electronic). |  |
| * Provide an acknowledgement at least annually. |  |
| **7.2 During employment** | | | |
| **7.2.1** Management responsibilities | | | |
| Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization. | **Describe how** the security awareness program provides multiple methods of communicating awareness and educating personnel. |  |  |
| **7.2.2** Information security awareness, education and training | | | |
| All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function. | **Provide the name of the assessor** who attests that the security awareness program was verified to provide awareness to all personnel about the cardholder data security policy and procedures. |  |  |
| **Identify the documented security awareness program procedures and additional documentation** examined to verify that:   * The security awareness program provides multiple methods of communicating awareness and educating personnel. * Personnel attend security awareness training: * Upon hire, and * At least annually * Personnel acknowledge, in writing or electronically and at least annually, that they have read and understand the information security policy. |  |
| **7.2.3** Disciplinary process | | | |
| There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach. | **Identify the documented policy** reviewed to verify appropriate contacts with relevant authorities should be maintained. |  |  |
| **7.3 Termination and change of employment** | | | |
| **7.3.1** Termination or change of employment responsibilities | | | |
| Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced. | **Identify the documented policy** reviewed to verify responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced. |  |  |

### A.8 Asset management

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **8.1 Responsibility for assets** | | | |
| **8.1.1** Inventory of assets | | | |
| Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained. | **Describe how** the system inventory was examined to verify that a list of hardware and software components is: | |  |
| * Maintained |  |
| * Includes a description of function/use for each |  |
| **8.1.2** Ownership of assets | | | |
| Assets maintained in the inventory should be owned. | **Identify the documented policy** reviewed to verify assets maintained in the inventory should be owned. |  |  |
| **8.1.3** Acceptable use of assets | | | |
| Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented. | **Provide the name of the assessor** who attests that the usage policies were verified to define acceptable uses for the technology. |  |  |
| **8.1.4** Return of assets | | | |
| All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement. | **Identify the documented policy** reviewed to verify assets maintained in the inventory should be owned. |  |  |
| **8.2 Information classification** | | | |
| **8.2.1** Classification of information | | | |
| Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. | **Identify the documented policy** reviewed to verify Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. |  |  |
| **8.2.2** Labelling of information | | | |
| An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization. | **Provide the name of the assessor** who attests that the usage policies were verified to define a method to accurately and readily determine:   * Owner * Contact Information * Purpose |  |  |
| **8.2.3** Handling of assets | | | |
| Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by the organization. | **Identify the documented policy** reviewed to verify assets maintained in the inventory should be owned. |  |  |
| **8.3 Media handling** | | | |
| **8.3.1** Management of removable media | | | |
| Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization. | **Describe how** media was observed to be classified so the sensitivity of the data can be determined. |  |  |
| **8.3.2** Disposal of media | | | |
| Media should be disposed of securely when no longer required, using formal procedures. | **Identify** **the responsible personnel** interviewed who confirm that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. |  |  |
| **Provide the name of the assessor** who attests that the procedures state that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance that hardcopy materials cannot be reconstructed. |  |
| **8.3.3** Physical media transfer | | | |
| Media containing information should be protected against unauthorized access, misuse or corruption during transportation. | **Identify** **responsible personnel** interviewed who confirm that proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). |  |  |
| **Describe how** offsite tracking logs were examined to verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals). |  |

### A.9 Access Control

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **9.1 Business requirements of access control** | | | |
| **9.1.1** Access control policy | | | |
| An access control policy should be established, documented and reviewed based on business and information security requirements. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  |  |
| **9.1.2** Access to networks and network services | | | |
| Users should only be provided with access to the network and network services that they have been specifically authorized to use. | **Identify the sample** of user IDs examined for this testing procedure. |  |  |
| **Describe how** each item in the sample of user IDs was compared with documented approvals to verify that: | |
| * Documented approval exists for the assigned privileges. |  |
| * The approval was by authorized parties. |  |
| * That specified privileges match the roles assigned to the individual. |  |
| **9.2 User access management** | | | |
| **9.2.1** User registration and de-registration | | | |
| A formal user registration and de-registration process should be implemented to enable assignment of access rights. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  |  |
| **9.2.2** User access provisioning | | | |
| A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services. | **Identify** **the selected sample** of roles for this testing procedure. |  |  |
| *For each role in the selected sample***, describe how** the role was examined to verify access needs for each role are defined and include: | |
| * System components and data resources that each role needs to access for their job function. |  |
| * Identification of privilege necessary for each role to perform their job function. |  |
| **9.2.3** Management of privileged access rights | | | |
| The allocation and use of privileged access rights should be restricted and controlled. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates as follows:   * Defining access needs and privilege assignments for each role. * Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities. * Assignment of access based on individual personnel’s job classification and function * Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  |  |
| **9.2.4** Management of secret authentication information for users | | | |
| The allocation of secret authentication information should be controlled through a formal management process. | **Identify** **the document** that contains the management of secret authentication information for users. |  |  |
| **9.2.5** Review of user access rights | | | |
| Asset owners should review users’ access rights at regular intervals. | **Describe how** user accounts were observed to verify that any inactive accounts over 90 days old are either removed or disabled. |  |  |
| **9.2.6** Removal or adjustment of user access rights | | | |
| The access rights of all employees and external party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change. | **Identify** **the sample** of users terminated in the past six months that were selected for this testing procedure. |  |  |
| **Describe how** the current user access lists for ***local access*** verified that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **Describe how** the current user access lists for ***remote access*** verified that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **9.3 User responsibilities** | | | |
| **9.3.1** User of secret authentication information | | | |
| Users should be required to follow the organization’s practices in the use of secret authentication information. | **Identify** **the document** that contains the management of secret authentication information for users. |  |  |
| **9.4 System and application access control** | | | |
| **9.4.1** Information access restriction | | | |
| Access to information and application system functions should be restricted in accordance with the access control policy. | **Identify** **the written policy for access control** that was examined to verify the policy incorporates:   * Access to information and application system. |  |  |
| **9.4.2** Secure log-on procedures | | | |
| Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure. | **Identify** all databases containing cardholder data. |  |  |
| **Describe how** database and/or application configuration settings verified that all users are authenticated prior to access. |  |
| **9.4.3** Password management system | | | |
| Password management systems should be interactive and should ensure quality passwords. | **Identify** **the written procedures for user identification management** examined to verify processes are defined for each of the items below:   * Assign all users a unique ID before allowing them to access system components or cardholder data. * Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. * Immediately revoke access for any terminated users. * Remove/disable inactive user accounts at least every 90 days. * Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: * Enabled only during the time period needed and disabled when not in use. * Monitored when in use. * Limit repeated access attempts by locking out the user ID after not more than six attempts. * Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. * If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. |  |  |
| **9.4.4** Use of privileged utility programs | | | |
| The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled. | **Identify the assessor** who attests that users cannot installed software or utility programs and that they are tightly controlled. |  |  |
| **9.4.5** Access control to program source code | | | |
| Access to program source code should be restricted. | **Identify the assessor** who attests that access to program source code is restricted. |  |  |

### A.10 Cryptography

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **10.1 Cryptographic controls** | | | |
| **10.1.1** Policy on the use of cryptographic controls | | | |
| A policy on the use of cryptographic controls for protection of information should be developed and implemented. | **Identify** **the documentation** examined to verify that the NPI is rendered unreadable using any of the following methods:   * One-way hashes based on strong cryptography, * Truncation * Index tokens and pads, with the pads being securely stored * Strong cryptography, with associated key-management processes and procedures |  |  |
| **10.1.2** Key management | | | |
| A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle. | **Identify** **the documented key-management policies and processes** examined to verify processes are defined to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following:   * Access to keys is restricted to the fewest number of custodians necessary. * Key-encrypting keys are at least as strong as the data-encrypting keys they protect. * Key-encrypting keys are stored separately from data-encrypting keys. * Keys are stored securely in the fewest possible locations and forms. |  |  |

### A.11 Physical and environmental security

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **11.1 Secure areas** | | | |
| **11.1.1** Physical security perimeter | | | |
| Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities. | **Identify and briefly describe** all of the following with systems in the confidential data environment: | |  |
| * All computer rooms |  |
| * All data centers |  |
| * Any other physical areas |  |
| *For each area identified (add rows as needed),* complete the following: | |
| **Describe** the physical security controls to be in place, including authorized badges and lock and key. |  |
| **Identify** the randomly selected systems in the confidential environment for which a system administrator login attempt was observed. |  |
| **Describe how** consoles for the randomly selected systems were observed to verify that they are “locked” when not in use to prevent unauthorized use. |  |
| **11.1.2** Physical entry controls | | | |
| Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. | **Describe how** personnel accessing sensitive areas were observed to verify that all personnel are authorized before being granted access. |  |  |
| **11.1.3** Securing offices, rooms, facilities | | | |
| Physical security for offices, rooms and facilities should be designed and applied. | **Describe** either the video cameras or access control mechanisms (or both) observed to monitor the entry/exit points to sensitive areas. |  |  |
| **11.1.4** Protecting against external and environmental threats | | | |
| Physical protection against natural disasters, malicious attack or accidents should be designed and applied. | **Identify the documented**  **Business Continuity and Disaster Recovery Policy to show** Protecting against external and environmental threats |  |  |
| **11.1.5** Working in secure areas | | | |
| Procedures for working in secure areas should be designed and applied. | **Identify** **the documented processes** reviewed to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors, including the following:   * Identifying onsite personnel and visitors (for example, assigning badges), * Changing access requirements, and * Revoking terminated onsite personnel and expired visitor identification (such as ID badges). |  |  |
| **11.1.6** Delivery and loading areas | | | |
| Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. | **Describe** how access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. |  |  |
| **11.2 Equipment** | | | |
| **11.2.1** Equipment siting and protection | | | |
| Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. | **Identify** **the assessor who confirms** equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. |  |  |
| **11.2.2** Supporting utilities | | | |
| Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. | **Identify** **the assessor who confirms** equipment is protected from power failures and other disruptions caused by failures in supporting utilities. |  |  |
| **11.2.3** Cabling security | | | |
| Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage. | **Identify** **the assessor who confirms** power and telecommunications cabling carrying data or supporting information services is protected from interception, interference or damage. |  |  |
| **11.2.4** Equipment maintenance | | | |
| Equipment should be correctly maintained to ensure its continued availability and integrity. | **Identify** **the assessor who confirms** equipment is correctly maintained to ensure its continued availability and integrity. |  |  |
| **11.2.5** Removal of assets | | | |
| Equipment, information or software should not be taken off-site without prior authorization. | **Identify** **the assessor who confirms** equipment, information or software is not taken off-site without prior authorization. |  |  |
| **11.2.6** Security of equipment and assets off-premises | | | |
| Security should be applied to off-site assets taking into account the different risks of working outside the organization’s. premises | **Identify** **the assessor who confirms** security is applied to off-site assets taking into account the different risks of working outside the organization’s premises. |  |  |
| **11.2.7** Secure disposal or re-use of equipment | | | |
| All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. | **Identify the policy document for periodic media destruction** that was examined to verify it covers all media and defines requirements for the following:   * Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. * Storage containers used for materials that are to be destroyed must be secured. * Confidential data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media). |  |  |
| **11.2.8** Unattended user equipment | | | |
| Users should ensure that unattended equipment has appropriate protection. | **Describe how** processes were observed to verify that the storage location is reviewed at least annually to confirm that backup media storage is secure. |  |  |
| **11.2.9** Clear desk and clear screen policy | | | |
| A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted. | **Describe how** it was observed that a clear desk policy exists and is followed on the premises. |  |  |

### A.12 Operations security

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **12.1 Operational procedures and responsibilities** | | | |
| **12.1.1** Documented operating procedures | | | |
| Operating procedures should be documented and made available to all users who need them. | **Identify** **all** operating procedure documents. |  |  |
| **12.1.2** Change management | | | |
| Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled. | **Identify** **the documented change-control procedures** related to implementing security patches and software modification examined to verify procedures are defined for:   * Documentation of impact. * Documentedchange approval by authorized parties. * Functionality testing to verify that the change does not adversely impact the security of the system. * Back-out procedures. |  |  |
| **12.1.3** Capacity management | | | |
| The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance. | **Identifiy** how resources are monitored. |  |  |
| **12.1.4** Separation of development, testing and operational environments | | | |
| Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment. | **Identify the network documentation** that illustrates that the development/test environments are separate from the production environment(s). |  |  |
| **Describe how** network device configurations were examined to verify that the development/test environments are separate from the production environment(s). |  |
| **12.2 Protection from malware** | | | |
| **12.2.1** Controls against malware | | | |
| Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness. | **Identify** **the vendor documentation** reviewed to verify that anti-virus programs:   * Detect all known types of malicious software, * Remove all known types of malicious software, and * Protect against all known types of malicious software. |  |  |
| **Describe how** anti-virus configurations were examined to verify that anti-virus programs: | |
| * Detect all known types of malicious software, |  |
| * Remove all known types of malicious software, and |  |
| * Protect against all known types of malicious software. |  |
| **12.3 Backup** | | | |
| **12.3.1** Information backup | | | |
| Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy. | **Identify** **the assessor who attests b**ackup copies of information, software and system images are taken and tested regularly in accordance with an agreed backup policy. |  |  |
| **12.4 Logging and monitoring** | | | |
| **12.4.1** Event logging | | | |
| Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed. | **Identify the responsible personnel** interviewed who confirm the following are logged:   * All individual access to cardholder data. * All actions taken by any individual with root or administrative privileges. * Access to all audit trails. * Invalid logical access attempts. * Use of and changes to identification and authentication mechanisms, including:   + All elevation of privileges.   + All changes, additions, or deletions to any account with root or administrative privileges. * Initialization of audit logs. * Stopping or pausing of audit logs. * Creation and deletion of system level objects. |  |  |
| **Identify the sample of audit logs** selected for reviewing all the above is logged. |  |
| **12.4.2** Protection of log information | | | |
| Logging facilities and log information should be protected against tampering and unauthorized access. | **Describe how** system configurations and permissions were examined to verify that current audit trail files are protected from unauthorized modifications. (e.g., via access control mechanisms, physical segregation, and/or network segregation). |  |  |
| **12.4.3** Administrator and operator logs | | | |
| System administrator and system operator activities should be logged and the logs protected and regularly reviewed. | **Describe how** configuration settings were observed to verify all actions taken by any individual with root or administrative privileges are logged. |  |  |
| **12.4.4** Clock synchronization | | | |
| The clocks of all relevant information processing systems within an organization or security domain should be synchronized to a single reference time source. | **Identify** **the documented time-synchronization configuration standards** examined to verify that time synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2. |  |  |
| **12.5 Control of operational software** | | | |
| **12.5.1** Installation of software on operational systems | | | |
| Procedures should be implemented to control the installation of software on operational systems. | **Identify the responsible personnel** interviewed who confirm that access to privileged user IDs is:   * Assigned only to roles that specifically require such privileged access. * Restricted to least privileges necessary to perform job responsibilities. |  |  |
| **12.6 Technical Vulnerability Management** | | | |
| **12.6.1** Management of technical vulnerabilities | | | |
| Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization’s exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. | **Identify** **the documented policies and procedures** related to security-patch installation examined to verify processes are defined for:   * Installation of applicable critical vendor-supplied security patches within one month of release. * Installation of all applicable vendor-supplied security patches within an appropriate time frame. |  |  |
| **12.6.2** Restrictions on software installation | | | |
| Rules governing the installation of software by users should be established and implemented. | **Identify** **the assessor who attests** rules governing the installation of software by users should be established and implemented. |  |  |
| **12.7 Information systems audit considerations** | | | |
| **12.7.1** Information systems audit controls | | | |
| Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes. | **Identify** **the assessor who attests** audit requirements and activities involving verification of operational systems are carefully planned and agreed to minimize disruptions to business processes. |  |  |

### A.13 Communications security

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **13.1 Network security management** | | | |
| **13.1.1** Network controls | | | |
| Networks should be managed and controlled to protect information in systems and applications. | **Identify the document(s)** reviewed to verify procedures define the formal processes for: | |  |
| * Testing and approval of all network connections. |  |
| * Testing and approval of all changes to firewall and router configurations. |  |
| **13.1.2** Security of network services | | | |
| Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced. | **Identify** **the assessor who attests** Security mechanisms, service levels and management requirements of all network services are identified and included in network services agreements, whether these services are provided in-house or outsourced. |  |  |
| **13.1.3** Segregation in networks | | | |
| Groups of information services, users and information systems should be segregated on networks. | **Identify** **the assessor who attests** Groups of information services, users and information systems are segregated on networks. |  |  |
| **13.2 Information transfer** | | | |
| **13.2.1** Information transfer policies and procedures | | | |
| Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities. | **Identify the document** reviewed to verify that processes are specified for the following:   * For acceptance of only trusted keys and/or certificates. * For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported). * For implementation of proper encryption strength per the encryption methodology in use. |  |  |
| **13.2.2** Agreements on information transfer | | | |
| Agreements should address the secure transfer of business information between the organization and external parties. | **Identify** **the assessor who attests a**greements address the secure transfer of business information between the organization and external parties. |  |  |
| **13.2.3** Electronic messaging | | | |
| Information involved in electronic messaging should be appropriately protected. | **Indicate** **whether** end-user messaging technologies are used to send cardholder data. **(yes/no)** |  |  |
| *If “no,” mark the remainder of 4.2.a as “Not Applicable” and proceed to 4.2.b.*  *If “yes,” complete the following:* | |
| **Describe how** processes for sending PAN were observed to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  |
| **Describe** **the sample** of outbound transmissions that were observed as they occurred. |  |
| **Describe how** the sample of outbound transmissions verified that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  |
| **13.2.4** Confidentiality or non-disclosure agreements | | | |
| Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified, regularly reviewed and documented. | **Identify** **the assessor who attests** requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information are identified, regularly reviewed and documented. |  |  |

### A.14 System acquisition, development and maintenance

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **14.1 Security requirements of information systems** | | | |
| **14.1.1** Information security requirements analysis and specification | | | |
| The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems. | **Identify** **the policy documentation** examined to verify it defines that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network |  |  |
| **Identify** **the responsible personnel** interviewed who confirm that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network. |  |
| **14.1.2** Securing application services on public networks | | | |
| Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification. | **Describe** **the sample** of inbound and outbound transmissions observed as they occurred. |  |  |
| **Describe how** the samples of inbound and outbound transmissions were observed as they occurred to verify that all confidential data is encrypted with strong cryptography during transit. |  |
| **14.1.3** Protecting application services transactions | | | |
| Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. | **Identify** **the assessor who attests** users are trained and applications require secure connections to communicate. |  |  |
| **14.2 Security in development and support processes** | | | |
| **14.2.1** Secure development policy | | | |
| Rules for the development of software and systems should be established and applied to developments within the organization. | **Identify** **the assessor who attests** development systems and software follow best practice for security within the organization. |  |  |
| **14.2.2** System change control procedures | | | |
| Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures. | **Identify** **the documented change-control procedures** related to implementing security patches and software modification examined to verify procedures are defined for:   * Documentation of impact. * Documentedchange approval by authorized parties. * Functionality testing to verify that the change does not adversely impact the security of the system. * Back-out procedures. |  |  |
| **14.2.3** Technical review of applications after operating platform changes | | | |
| When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. | **Identify** **the responsible personnel** interviewed for this testing procedure who confirm that all custom application code changes are reviewed as follows:   * Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code-review techniques and secure coding practices. * Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). * Appropriate corrections are implemented prior to release. * Code-review results are reviewed and approved by management prior to release. |  |  |
| **14.2.4** Restrictions on changes to software packages | | | |
| Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled. | **Identify the personnel assigned to development/test environments** interviewed who confirm that separation of duties is in place between development/test environments and the production environment. |  |  |
| **Identify the personnel assigned to production environments** interviewed who confirm that separation of duties is in place between development/test environments and the production environment. |  |
| **Describe how** processes were observed to verify that separation of duties is in place between development/test environments and the production environment. |  |
| **14.2.5** Secure system engineering principles | | | |
| Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts. | **Identify** **the document** examined to verify that software-development processes are based on industry standards and/or best practices. |  |  |
| **14.2.6** Secure development environment | | | |
| Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle. | **Identify** **the assessor who attests** development systems and software follow best practice for security within the organization. |  |  |
| **14.2.7** Outsourced development | | | |
| The organization should supervise and monitor the activity of outsourced system development. | **Identify** **the document** that describes how the organization should supervise and monitor the activity of outsourced system development. |  |  |
| **14.2.8** System security testing | | | |
| Testing of security functionality should be carried out during development. | **Identify** **the document** that describes how testing of security functionality should be carried out during development. |  |  |
| **14.2.9** System acceptance testing | | | |
| Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions. | **Identify** **the document** that describes User Acceptance testing |  |  |
| **14.3 Test data** | | | |
| **14.3.1** Protection of test data | | | |
| Test data should be selected carefully, protected and controlled. | **Identify** **the document** that describes how test data is protected. |  |  |

### A.15 Supplier relationships

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **15.1 Information security in supplier relationships** | | | |
| **15.1.1** Information security policy for supplier relationships | | | |
| Information security requirements for mitigating the risks associated with supplier’s access to the organization’s assets should be agreed with the supplier and documented. | **Identify** **the document** that contains Information security policy for supplier relationships. |  |  |
| **15.1.2** Addressing security within supplier agreements | | | |
| All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization’s information. | **Identify** **the document** addressing security within supplier agreements. |  |  |
| **15.1.3** Information and communication technology supply chain | | | |
| Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain. | **Identify** **the document** that addresses Information and communication technology supply chain |  |  |
| **15.2 Supplier service delivery management** | | | |
| **15.2.1** Monitoring and review of supplier services | | | |
| Organizations should regularly monitor, review and audit supplier service delivery. | **Identify the documented policies and procedures** reviewed to verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data. |  |  |
| **15.2.2** Managing changes to supplier services | | | |
| Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks. | **Identify** **the assessor who attests** when changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, are managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks. |  |  |

### A.16 Information security incident management

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **16.1 Management of information security incidents and improvements** | | | |
| **16.1.1** Responsibilities and procedures | | | |
| Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Roles and responsibilities. |  |  |
| **16.1.2** Reporting information security events | | | |
| Information security events should be reported through appropriate management channels as quickly as possible. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Communication strategies. |  |  |
| **16.1.3** Reporting information security weaknesses | | | |
| Employees and contractors using the organization’s information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Reporting information security weaknesses |  |  |
| **16.1.4** Assessment of and decision on information security events | | | |
| Information security events should be assessed and it should be decided if they are to be classified as information security incidents. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Assessment of and decision on information security events. |  |  |
| **16.1.5** Response to information security incidents | | | |
| Information security incidents should be responded to in accordance with the documented procedures. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Business recovery and continuity procedures. * Analysis of legal requirements for reporting compromises. * Responses for all critical system components. * Reference or inclusion of incident response procedures from the payment brands. |  |  |
| **16.1.6** Learning from information security incidents | | | |
| Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents. | **Identify the documented policy** reviewed to verify that processes are defined to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |  |
| **Identify the sample of responsible personnel** interviewed who confirm that processes are implemented to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |
| **Describe how** it was observed that processes are implemented to modify and evolve the incident response plan: | |
| * According to lessons learned. |  |
| * To incorporate industry developments. |  |
| **16.1.7** Collection of evidence | | | |
| The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence. | **Provide the name of the assessor** who attests that the incident response plan was verified to include:   * Collection of evidence |  |  |

### A.17 Information security aspects of business continuity management

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **17.1 Information security continuity** | | | |
| **17.1.1** Planning information security continuity | | | |
| The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster. | **Identify the documented** **Business Continuity and Disaster Recovery Policy to show** Planning information security continuity |  |  |
| **17.1.2** Implementing information security continuity | | | |
| The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation. | **Identify the documented** **Business Continuity and Disaster Recovery Policy to show I**mplementing information security continuity |  |  |
| **17.1.3** Verify, review and evaluate information security continuity | | | |
| The organization should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. | **Identify the documented** **Business Continuity and Disaster Recovery Policy to show it** verifies, review and evaluate information security continuity |  |  |
| **17.2 Redundancies** | | | |
| **17.2.1** Availability of information processing facilities | | | |
| Information processing facilities should be implemented with redundancy sufficient to meet availability requirements. | **Describe how** processes were observed to verify that the storage location is reviewed at least annually to confirm that backup media storage is secure. |  |  |

### A.18 Compliance

|  |  |  |  |
| --- | --- | --- | --- |
| **ISO 27002 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **18.1 Compliance with legal and contractual requirements** | | | |
| **18.1.1** Identification of applicable legislation and contractual requirements | | | |
| All relevant legislative statutory, regulatory, contractual requirements and the organization’s approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organization. | **Identify the documented** policy that contains applicable legislation and contractual requirements. |  |  |
| **18.1.2** Intellectual property rights | | | |
| Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products. | **Identify the documented** policy that contains intellectual property rights. |  |  |
| **18.1.3** Protection of records | | | |
| Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislated, regulatory, contractual and business requirements. | **Identify the documented** policy that contains protection of records. |  |  |
| **18.1.4** Privacy and protection of personally identifiable information | | | |
| Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable. | **Identify the documented** policy that contains the privacy and protection of personally identifiable information. |  |  |
| **18.1.5** Regulation of cryptographic controls | | | |
| Cryptographic controls should be used in compliance with all relevant agreements, legislation and regulations. | **Identify the documented** policy that contains the regulation of cryptographic controls. |  |  |
| **18.2 Information security reviews** | | | |
| **18.2.1** Independent review of information security | | | |
| The organization’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur. | **Identify the documented** audits that have occurred. |  |  |
| **18.2.2** Compliance with security policies and standards | | | |
| Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. | **Describe how** the information security policy was verified to be: | |  |
| * Reviewed at least annually. |  |
| * Updated as needed to reflect changes to business objectives or the risk environment. |  |
| **18.2.3** Technical compliance review | | | |
| Information systems should be regularly reviewed for compliance with the organization’s information security policies and standards. | **Identify** **the policy documentation** examined toverify thatsystem configuration standards are updated as new vulnerability issues are identified. |  |  |
| **Identify** **the responsible personnel** interviewed who confirm thatsystem configuration standards are updated as new vulnerability issues are identified. |  |