Instructure - Confidential

Instructure PCI Responsibility Matrix	F	Responsibilit	V
Requirement	AWS	Instructure	Customer
1.1 Establish and implement firewall and router configuration standards that include the following:			
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	x	x	
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks		х	
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	x	x	
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	х	х	
1.1.5 Description of groups, roles, and responsibilities for management of network components	x	x	
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	X	х	
1.1.7 Requirement to review firewall and router rule sets at least every six months	x	x	
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.			
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	Х	х	
1.2.2 Secure and synchronize router configuration files.	x		
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	X	x	
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.			
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	х	x	
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	Х	х	
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.	х	х	
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	х	х	
1.3.5 Permit only "established" connections into the network.	х	х	
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	х	х	
1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties.	х	x	
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE.		х	
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.		x	
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).	х	х	
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.		x	
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: Center for Internet Security (CIS) International Organization for Standardization (ISO) SysAdmin Audit Network Security (SANS) Institute National Institute of Standards Technology (NIST).	х	х	
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)	х	х	
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	Х	x	
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.	х	х	
2.2.4 Configure system security parameters to prevent misuse.	Х	x	
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	х	х	
2.3 Encrypt all non-console administrative access using strong cryptography.	Х	х	
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	Х	х	
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	X	х	
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.	х	х	
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements Specific retention requirements for cardholder data Processes for secure deletion of data when no longer needed A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.		х	

Instructure PCI Responsibility Matrix		Responsibilit	V
Requirement	AWS	Instructure	Customer
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: There is a business justification and The data is stored securely.		х	
Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:			
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.		x	
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not- present transactions) after authorization.		х	
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.		х	
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.		х	
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: One-way hashes based on strong cryptography, (hash must be of the entire PAN) Truncation (hashing cannot be used to replace the truncated segment of PAN) Index tokens and pads (pads must be securely stored) Strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.		х	
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.		х	
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.		х	
3.5.1 Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date Description of the key usage for each key Inventory of any HSMs and other SCDs used for key management		х	
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.		x	
3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) As at least two full-length key components or key shares, in accordance with an industry- accepted method Note: It is not required that public keys be stored in one of these forms.		x	
3.5.4 Store cryptographic keys in the fewest possible locations. 3.6 Fully document and implement all key- management processes and procedures for cryptographic keys used for		X	
encryption of cardholder data, including the following:		,,	
3.6.1 Generation of strong cryptographic keys 3.6.2 Secure cryptographic key distribution		X X	
3.6.3 Secure cryptographic key storage		x	
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).		х	
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.		х	
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. Note: Examples of manual key- management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.		х	
3.6.7 Prevention of unauthorized substitution of cryptographic keys.		х	
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key- custodian responsibilities.		х	
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.		Х	
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: Only trusted keys and certificates are accepted. The protocol in use only supports secure versions or configurations. The encryption strength is appropriate for the encryption methodology in use.	х	х	
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.		х	
4.2 Never send unprotected PANs by end- user messaging technologies (for example, e- mail, instant messaging, SMS, chat, etc.).		х	

Instructure PCI Responsibility Matrix	R	Responsibilit	:y
Requirement	AWS	Instructure	Customer
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	х	х	
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	х	х	
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	х	х	
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	х	х	
5.2 Ensure that all anti-virus mechanisms are maintained as follows: Are kept current, Perform periodic scans Generate audit logs which are retained per PCI DSS Requirement 10.7.	х	х	
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	х	х	
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	х	х	
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.	х	х	
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release.	х	х	
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely,	х	x	
as follows: In accordance with PCI DSS (for example, secure authentication and logging) Based on industry standards and/or best practices. Incorporating information security throughout the software-development life cycle Note: this applies to all software developed internally as well as bespoke or custom software developed by a third party.			
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	x	x	
6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. Code reviews ensure code is developed according to secure coding guidelines Appropriate corrections are implemented prior to release. Code-review results are reviewed and approved by management prior to release.	х	х	
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:			
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.	х	х	
6.4.2 Separation of duties between development/test and production environments	х	х	
6.4.3 Production data (live PANs) are not used for testing or development	х	х	
6.4.4 Removal of test data and accounts from system components before the system becomes active / goes into production.	х	x	
6.4.5 Change control procedures must include the following:	х	х	
6.4.5.1 Documentation of impact.	х	x	
6.4.5.2 Documented change approval by authorized parties.	х	x	
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	x	x	
6.4.5.4 Back-out procedures.	х	х	
6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.	х	х	
6.5 Address common coding vulnerabilities in software-development processes as follows: Train developers at least annually in up- to-date secure coding techniques, including how to avoid common coding vulnerabilities. Develop applications based on secure coding guidelines.	X	x	
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	х	х	
6.5.2 Buffer overflows	х	х	
6.5.3 Insecure cryptographic storage	х	х	
6.5.4 Insecure communications	х	х	
6.5.5 Improper error handling	х	х	
6.5.6 All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement	х	х	
6.1). Web applications, both in Note: Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (public) facing, have uniq (internal or external): upon their architecture a and occurrence of compr			
6.5.7 Cross-site scripting (XSS)	х	х	
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	х	x	
6.5.9 Cross-site request forgery (CSRF)	x	х	
6.5.10 Broken authentication and session management.	x	х	
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Installing an automated technical solution that detects and prevents web- based attacks (for example, a web- application firewall) in front of public- facing web applications, to continually check all traffic.	х	х	

Instructure - Confidential

Instructure PCI Responsibility Matrix		Responsibilit	V
Requirement	AWS	Instructure	Customer
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	х	х	
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	Х	х	
7.1.1 Define access needs for each role, including: - System components and data resources that each role needs to access for their job function - Level of privilege required (for example, user, administrator, etc.) for accessing resources.	х	х	
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	Х	х	
7.1.3 Assign access based on individual personnel's job classification and function.	x	x	
7.1.4 Require documented approval by authorized parties specifying required privileges.	x	х	
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following:	х	х	
7.2.1 Coverage of all system components	х	х	
7.2.2 Assignment of privileges to individuals based on job classification and function.	х	х	
7.2.3 Default "deny-all" setting.	x	X	
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	Х	х	
8.1 Define and implement policies and procedures to ensure proper user identification management for non- consumer users and administrators on all system components as follows:	Х	X	
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	Х	х	
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	х	x	
8.1.3 Immediately revoke access for any terminated users.	x	х	
8.1.4 Remove/disable inactive user accounts within 90 days.	Х	х	
8.1.5 Manage IDs used by third parties 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.	х	х	
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	х	x	
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	х	х	
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	X	x	
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: Something you know, such as a password or passphrase Something you have, such as a token device or smart card Something you are, such as a biometric.	х	х	
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	х	х	
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	х	х	
8.2.3 Passwords/passphrases must meet the following: Require a minimum length of at least seven characters. Contain both numeric and alphabetic characters. Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.	х	х	
8.2.4 Change user passwords/passphrases at least once every 90 days.	х	х	
8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.	х	х	
8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	х	х	
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	х	х	
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	х	х	
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.	х	х	
8.4 Document and communicate authentication policies and procedures to all users including: Guidance on selecting strong authentication credentials Guidance for how users should protect their authentication credentials Instructions not to reuse previously used passwords Instructions to change passwords if there is any suspicion the password could be compromised.	х	х	
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.	Х	x	
8.5.1 Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.	х	х	
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: - Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. - Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	х	х	

Instructure PCI Responsibility Matrix	F	Responsibilit	У
Requirement	AWS	Instructure	Customer
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other		x	
users) is restricted as follows: All user access to, user queries of, and user actions on databases are through programmatic methods. Only database administrators have the ability to directly access or query databases.			
Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).			
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	х	х	
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	х		
9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by	х		
law. Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of- sale terminals are present, such as the cashier areas in a retail store.			
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.	х		
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	х		
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: Identifying onsite personnel and visitors (for example, assigning badges) Changes to access requirements Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).	х		
9.3 Control physical access for onsite personnel to sensitive areas as follows: Access must be authorized and based on individual job function. Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc.,	х		
are returned or disabled. 9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:	х		
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or	x		
maintained. 9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from participations are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from participations.	х		
onsite personnel. 9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	X		
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data	×		
centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.			
9.5 Physically secure all media.	х	х	
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	х	х	
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:			
9.6.1 Classify media so the sensitivity of the data can be determined.	х	x	
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.	х	x	
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	х	x	
9.7 Maintain strict control over the storage and accessibility of media.	х	x	
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	х	x	
9.8 Destroy media when it is no longer needed for business or legal reasons as follows: 9.8.1 Shred, incinerate, or pulp hard- copy materials so that cardholder data cannot be reconstructed. Secure storage	x x	X X	
containers used for materials that are to be destroyed. 9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	x	X	
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.	*	X	
9.9.1 Maintain an up-to-date list of devices. The list should include the following: - Make, model of device - Location of device (for example, the address of the site or facility where the device is located)		х	
Device serial number or other method of unique identification. 9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or		x	
substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or			
cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.			
 9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. Do not install, replace, or return devices without verification. Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). 		x	
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties	х	х	
10.1 Implement audit trails to link all access to system components to each individual user.	х	х	

Negative metals Negative m	Instructure PCI Responsibility Matrix		Responsibilit	V
19.2.1 All individual tuere accesses to carchivoler data 19.2.2 All address that by any individual with motor an administrative privileges 19.2.3 Access to all austif trails 19.2.3 Access to all austif trails 19.2.5 Uses of and changes to identification and subtentiation mechanism—including but not limited to dreation of new accounts and elevation of privilege—and all damages, additions, decidents by accounts with roof of administrative of privilege—and all damages, additions, decidents by accounts with roof of administrative of the subtiling o				
19.2.2 A fluctions taken by any redividual with root or administrative privileges 19.2.4 Insulis logical access a description 19.2.4 Insulis logical access a description 19.2.5 Uses of and charges to destrictions and authentication mechanisms—including but not limited to creation of new accounts and diversion of privileges—and all charges, additions, or deletions to accounts with not or administrative privileges 19.2.5 Uses of and charges to destrictions and authentication mechanisms—including but not limited to creation of new accounts and diversion of privileges—and all charges, additions, or deletions to accounts with not or administrative privileges 19.2.7 Executed the service of the subtilings of the subtilines o	•			
19.2.2 All cactions taken by any individual with roof or administrative privileges 19.2.4 forwards larged accesses attempties 19.2.4 forwards larged accesses attempties 19.2.4 forwards larged accesses attempties 19.2.4 forwards and accesses attempties 19.2.4 forwards and accesses attempties 19.2.4 forwards and accesses attempties 19.2.5 forwards and accesses attempting and it will antitions for all system components for each event: 19.3.1 forwards and accesses attempting and it will antitions for all system components for each event: 19.3.1 forwards and accesses attempting and it will antitions for all system components for each event: 19.3.1 forwards and accesses attempting and it will antitions for all system components for each event: 19.3.3 forwards and accesses attempting and it will antitions for all system components for each event: 19.3.3 forwards and accesses attempting and it will antitions for all system components for each event: 19.3.3 forwards and accesses attempting and it will antitions for all system components for each event: 19.3.4 forwards and accesses attempting and it will antitions for all system components for each event: 19.3.5 forwards and including a system component, or resource. 19.4.5 forwards and forwards and accesses attempting and accesses attempting, accesses and accesses attempting, a		х	x	
19.2.4 Invited logical access attempts 19.2.5 Invited and transports bedeficiation and authentication mechanisms—including but not intend to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges 19.2.6 Invited and advantages—and all changes, additions, or deletions to accounts with root or administrative privileges 19.2.6 Invited and advantages and the advantage and the author of the south tops 19.2.6 Invited and the following and the author of the south tops 19.3.7 User allers and times 19.3.7 User advantages 19.3.8 Invited and times 19.3.5 Invited invited and the author of the south tops 19.3.5 Invited invited and the author of the south tops 19.3.5 Invited invited and times 19.3.5 Invited invited and times 19.3.5 Outperform or fewert 19.3.5 Invited invited and times 19.3.5 Invited invited invited and times 19.3.5 Invited in	10.2.2 All actions taken by any individual with root or administrative privileges		х	
10.2.5 Used and changes to Gentification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privilegem—and changes, additions, or deletions to accounts with root or administrative privilegem. 10.2.7 Creations and disellors of system tend (displace). 10.2.8 Totalism and disellors of system tend (displace). 10.3.1 Used certification. 10.3.1 Used certification. 10.3.1 Used certification. 10.3.1 Used certification. 10.3.2 Typed or ever the following auth at an entire for all system components for each event. 10.3.2 Typed or event. 10.3.2 Typed or event. 10.3.3 Data and time. 10.3.5 Organization of event. 10.3.5 Data and time. 10.3.5 Organization of event. 10.3.5 Data and time. 10.3.5 Data	10.2.3 Access to all audit trails	х	х	
accounts and elevation of printinges—and all changes, additions, or deletions to accounts with root or administrative printings. 10.28 initialization, telepting, or pausing of the audit logis 10.28 record at least the following audit trail entries for all system components for each event: 10.38 record at least the following audit trail entries for all system components for each event: 10.38 record at least the following audit trail entries for all system components for each event: 10.38 record at least the following audit trail entries for all system components for each event: 10.38 record at least the following audit trail entries for all system components or record and trail to a system or any or event of the system of the sys	10.2.4 Invalid logical access attempts	х	х	
10.2.6 In Intelligation is speciment to plausing of the audit logs 10.3 Record at least the following audit trail entries for all system components for each event: 10.3 Record at least the following audit trail entries for all system components for each event: 10.3 For any of the system of the system components for each event: 10.3 For any of the system of the system components or each event: 10.3 For any of the system of the system of the system components or each event: 10.3 For any of the system of	accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative	х	х	
10.2.7 Consider and deletion of system. Invest displaces. 10.3.1 User identification 10.3.1 User identification 10.3.2 Type of event 10.3.2 Type of event 10.3.3 Date and time the following adult trail entries for all system components for each event: 10.3.5 Date and time 10.3.5 Date and time and		x	x	
10.3 Floored at least the following audit trail entries for all system components for each event: 10.3.1 User identification 10.3.2 Type of event 10.3.2 Type of event 10.3.3 Date and time 10.3.4 Success or failure indication 10.3.4 Success or failure indication 10.3.5 Date and time 10.3.5 Serial principle in the failure indication 10.3.6 Serial principle in the failure indication 10.4 Lings principle in the failure in the failure indication 10.4 Lings principle in the failure indication 10.4 Lings principle in the failure indication				
10.3.1 User identification 10.3.2 Type of event 10.3.2 Type of event 10.3.3 Discardations 10.3.5 Origination of event 10.3.5 Origination of event 10.3.6 Origination of event 10.3.7 Origination of event 10.3.8 Origination of event 10.3.8 Origination of event 10.3.8 Origination of event 10.3.9 Origination of event 10.3.1 Origination of event 10.3.1 Origination of event 10.3.2 Origination of event 10.3.3 Origination of event 10.3.4 Origination of event 10.3.4 Origination of event 10.3.4 Origination of event 10.3.5 Origination of event 10.5 Origination of e	·			
19.3.2 Type of event 19.3.3 Date and time 19.3.4 Success or failure indication 19.3.6 Success or failure indication 19.4 London systems have the correct and consideration from the process of the correct and consideration for the correct and correct and consideration for the correct and co		х	x	
10.3.3 December of the medication	10.3.2 Type of event		_	
19.3.5 (gingalation of event 19.3.6 (gingalation of event 19.3.6 (gingalation of event 19.4 (Using time synthionization technology, synthronization technology, synthronization, synthr			_	
19.3.5 (gingalation of event 19.3.6 (gingalation of event 19.3.6 (gingalation of event 19.4 (Using time synthionization technology, synthronization technology, synthronization, synthr			+	
19.3.5 likelinity or name of effected data, system component, or resource. 10.4 Liking time-system/contraction technology, synchronized intellinity, and stating time. 10.4.2 Time data is protected. 10.4.2 Time data is protected. 10.4.3 Time settings are received from industry-accepted time sources. 10.5.1 Limit viewing of audit trails to those with a pid related need. 10.5.1 Limit viewing of audit trails to those with a pid related need. 10.5.1 Limit viewing of audit trails to those with a pid related need. 10.5.1 Limit viewing of audit trails to those with a pid related need. 10.5.1 Limit viewing of audit trails to those with a pid related need. 10.5.2 Protect a utility at files to a centralized log server or media device. 10.5.3 Limit viewing of audit trails files from understood modifications. 10.5.3 Promotify back up audit trail files to a centralized log server or media device. 10.5.4 Write logs for extermal-kaing technologies onto a secure, centralized, internal log server or media device. 10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that textisting log data cannot be changed without generating electralization, events for all system components to identify anomalies or suspicious activity. 10.5 Review logs and security events for all system components to identify anomalies or suspicious activity. 10.5 Ferview the following at least daily: 10.5 Ferview the following at least daily: 10.5 Ferview the following at least daily: 10.5 Ferview the following the resource of the protection servers, etc.): 10.5 Ferview the following the resource of the protection servers, etc.): 10.5 Ferview the poly of all direct grytam components that perform security functions (for example, frewalls, intrusion-detection example, frewalls, intrusion-detection exceptions and anomalies identified during the review process. 10.5 Ferview flogs of all critical system components that perform security functions (for example, follow): 10.5 Ferview flogs of a control of the secur				
19.4 Listing time-synchronization technology, synchronize all critical system docks and times and ensure that the following is members and example, and storing time. 19.4.1 Critical systems have the correct and consistent time. 19.4.2 Time deating are received from industry-accepted time sources. 19.4.3 Time settings are received from industry-accepted time sources. 19.5.3 Time settings are received from industry-accepted time sources. 19.5.4 Time settings are received from industry-accepted time sources. 19.5.5 Time settings are received from industry-accepted time sources. 19.5.5 Protect audit trail fiels from unauthorized modifications. 19.5.5 Protect audit trail fiels from unauthorized modifications. 19.5.5 Protect and trail fiels from unauthorized modifications. 19.5.5 Protect and trail fiels from unauthorized modifications. 19.5.5 Protect and trail fiels from unauthorized modifications. 19.5.5 Fromptly bedu pault trail fiels from unauthorized modifications. 19.5.5 Fromptly bedu pault trail fiels from unauthorized modifications. 19.5.5 Fromptly bedu pault trail field from unauthorized modifications. 19.5.5 Fromptly bedu pault trail field from unauthorized modifications. 19.5.5 Fromptly bedu pault trail field from unauthorized modifications. 19.5.5 Fromptly bedu pault trail field from unauthorized modifications. 19.5.5 Fromptly bedu pault trail field from unauthorized modifications. 19.5.5 Fromptly bedu pault trail field from unauthorized model and unauthorized modifications. 19.5.6 Review to gas a Security events for all system components to identify anomalies or suspicious activity. 19.5.6 Review logs of all other system components periodically based on the organization's polices and risk management strategy and trail from unauthorized modification servers, e-choice on the control of the security failure. 19.5.6 From the unauthory of a table story process, or transmit CHD and/or SAD 19.5.7 Fromptly and the security of the security failure. 19.5.8 Additional requirement for service	- ·		_	
19.4.2 Time data is protected. X	10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is		_	
10.4.3 Time settings are received from industry-accepted time sources. 10.5 Secure audit trails so they cannot be altered. 10.5 Four of the other of the property of part trails to they cannot be altered. 10.5 Four of the other other of the other other of the other other of the other		х	x	
10.5 Secure audit trails so they cannot be altered. 10.5.1 Limit viewing of audit trails to those with a job-related need. 10.5.2 Protect audit trail files from unauthorized modifications. 10.5.2 Protect audit trail files from unauthorized modifications. 10.5.2 Protect audit trail files from unauthorized modifications. 10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter. 10.5.4 Write logs for external-fecing technologies onto a secure, centralized, internal log server or media device. 10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating aetic (although reveal as leave). 10.5.6 Neview logs and sociuty events for all system components to identify anomalises or suspicious activity. 10.6.1 Review the following at least daily: 10.6.1 Review the following at least daily: 10.6.2 Review logs and sociuty events for all system components to identify anomalises or suspicious activity. 10.6.3 Review the following at least daily: 10.6.3 Petal security events 10.6.3 Petal security events 10.6.3 Petal security events 10.6.4 Security events 10.6.5 Petal security control systems (IDS/IPS), authentication servers, etc.): 10.6.7 Petal security the province of the security failure events in the province of the province providers only: Implement a process for the timely detection and reporting of failures 10.6.5 Petal security functions 10.6.5 Petal security control systems, including but not limited to failure of: 10.6.6 Petal security functions 10.6.7 Petal security functions 10.6.7 Petal security functions 10.6.7 Petal security functions 10.6.7	·	х	х	
10.5.1 Limit viewing of audit trails to those with a job-related need. 10.5.2 Promptly back up audit trail files from unauthorized modifications. 10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter. 10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device. 10.5.5 Uses file-integrity monitoring or change-detection software on logs to be ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert). 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement. 10.6.1 Review the following a least daily: All security events 1.0.gs of all system components that store, process, or transmit CHD and/or SAD 1.0.gs of all critical system components that store, process, or transmit CHD and/or SAD 1.0.gs of all critical system components that perform security functions (for example, frewalls, intrusion-detection systems/intrusion-prevention systems/(IDS/IPS), authentication servers, e-commerce redirection servers, etc.]. 10.7 Relain audit trail history for all least one year, with a minimum of three months immediately available for analysis (for example, or internal systems or anomalies identified during the review process. 10.7 Relain audit trail history for all least one year, with a minimum of three months immediately available for analysis (for example, or internal expertive, or restorable for ma backup; and the properties of critical security control systems, including but not limited to failure of: 10.8 Flowing internal processes for responding to failures so for reporting of failures of any critical security controls in a timely manufactor of failures of any critical security controls in a timely manufactor of failures in security controls in a timely manufactor of failures in controls or pr	10.4.3 Time settings are received from industry-accepted time sources.	х	х	
10.5.1 Limit viewing of audit trails to those with a job-related need. 10.5.2 Promptly back up audit trail files from unauthorized modifications. 10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter. 10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device. 10.5.5 Uses file-integrity monitoring or change-detection software on logs to be ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert). 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement. 10.6.1 Review the following a least daily: All security events 1.0.gs of all system components that store, process, or transmit CHD and/or SAD 1.0.gs of all critical system components that store, process, or transmit CHD and/or SAD 1.0.gs of all critical system components that perform security functions (for example, frewalls, intrusion-detection systems/intrusion-prevention systems/(IDS/IPS), authentication servers, e-commerce redirection servers, etc.]. 10.7 Relain audit trail history for all least one year, with a minimum of three months immediately available for analysis (for example, or internal systems or anomalies identified during the review process. 10.7 Relain audit trail history for all least one year, with a minimum of three months immediately available for analysis (for example, or internal expertive, or restorable for ma backup; and the properties of critical security control systems, including but not limited to failure of: 10.8 Flowing internal processes for responding to failures so for reporting of failures of any critical security controls in a timely manufactor of failures of any critical security controls in a timely manufactor of failures in security controls in a timely manufactor of failures in controls or pr				
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter. 10.5.4 Who logs for external-racing technologies onto a secure, centralized, internal log server or media device. 10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (elthough new data being added should not cause an alert). 10.6 Review log and security events for all system components to identify anomalies or suspicious activity. 10.6.1 Review the following at least daily: 10.6.2 Review logs of all critical system components that store, process, or transmit CHD and/or SAD 1.0gs of all system components that store, process, or transmit CHD and/or SAD 1.0gs of all critical system components that perform security functions (for example, firewalls, intrusion-detection systems firms on the components of	10.5.1 Limit viewing of audit trails to those with a job-related need.	x	х	
10.5 S Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating idents (although new data being added should not cause an alterty.) 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. 10.6.1 Review the following at least daily: 10.6.2 In Review the following at least daily: 10.6.3 Review logs of all system components that perform security functions (for example, frewalls, intrusion-detection systems/intrusion-prevention systems (IDSIPS), authentication servers, e-commerce redirection servers, etc.). 10.6.2 Review logs of all other system components periodically based on the organization's animal risk assessment. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.4 Follow up exceptions and anomalies identified during the re	10.5.2 Protect audit trail files from unauthorized modifications.	x	х	
10.5 S Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating idents (although new data being added should not cause an alterty.) 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. 10.6.1 Review the following at least daily: 10.6.2 In Review the following at least daily: 10.6.3 Review logs of all system components that perform security functions (for example, frewalls, intrusion-detection systems/intrusion-prevention systems (IDSIPS), authentication servers, e-commerce redirection servers, etc.). 10.6.2 Review logs of all other system components periodically based on the organization's animal risk assessment. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.4 Follow up exceptions and anomalies identified during the re	10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	х	х	
10.5 5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generaling alerts (although new data being added should not cause an alert). 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. 10.6.1 Review the following at least daily: 10.6.1 Review the following at least daily: 10.6.2 Review he following at least daily: 10.6.3 Review the following at least daily: 10.6.3 Review he following at least daily: 10.6.3 Review he following at least daily: 10.6.3 Perview the following at least daily: 10.6.3 Perview he following he		х	х	
without generating alerts (although new data being added should not cause an alert). 10.16 Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement. 10.61 Review logs and security events Logs of all system components that store, process, or transmit CHD and/or SAD Logs of all critical system components that store, process, or transmit CHD and/or SAD Logs of all critical system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/PS), authentication servers, e-commerce redirection servers, etc.). 10.62 Review logs of all other system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/PS), authentication servers, e-commerce redirection servers, etc.). 10.63 Pollow up exceptions and anomalies identified during the review process. 10.63 Follow up exceptions and anomalies identified during the review process. 10.63 Follow up exceptions and anomalies identified during the review process. 10.63 Follow up exceptions and anomalies identified during the review process. 10.63 Follow up exceptions and anomalies identified for mackup). 10.63 Follow up exceptions and anomalies identified for mackup. 10.63 Follow up exceptions and anomalies identified for mackup. 10.64 Event and the province of the security control systems, including but not limited to failure of: 10.65 Follow up exceptions and anomalies identified and province of the timely detection and reporting of failures 10.65 Follow up exceptions and anomalies in exception of the security control systems, including but not limited to failure of: 10.65 Follow up exceptions are service providers only. Respond to failures of any critical security controls in a timely 10.65 Follow up exception and addressing any security issues that are eduring the failure 10.65 Follow				
Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement. All security events Logs of all system components that store, process, or transmit CHD and/or SAD Logs of all critical system components that perform security functions (for example, firewalls, intrusion-detection systems/tiposal post of the transmit CHD and/or SAD Logs of all critical systems components that perform security functions (for example, firewalls, intrusion-detection systems/tiposal) Logs of all critical systems components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment. X	without generating alerts (although new data being added should not cause an alert).			
All security events Logs of all system components that store, process, or transmit CHD and/or SAD Logs of all critical system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (DIS/IPS), authentication servers, e-commerce redirection servers, etc.). 10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.4 Review of the regular process of the security control systems (for example, online, archived, or restorable from backup). 10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: 10.6.1 Film Additional requirement for service providers only: Respond to failures of any critical security controls (if used). 10.8.1 Additional requirement in security controls must include: 10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: 10.8.1 Additional requirement in security controls must include: 10.8.1 Additional requirement in security controls must include: 10.8.1 Additional requirement in a best practice until January 31, 2018, after which it becomes a requirement. 10.8.1 Additional requirement in a best practice until January	Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.			
Logs of all critical system components Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). 10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment. 10.6.3 Follow up exceptions and anomalies identified during the review process. x x x x X 10.6.3 Follow on exceptions and anomalies identified during the review process. x x x x X 10.6.3 Follow on exceptions and anomalies identified during the review process. x x x x x x x x 10.6.3 Follow on exceptions and anomalies identified during the review process. x x x x x x x x x x x x x x x		^	^	
systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). 10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.6.3 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: 10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: 10.8 Firewalls 10.8 Individual organization on the security control systems, including but not limited to failure of: 10.8 Firewalls 10.8 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely and controls (if used) 10.8 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: 10.8 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failure, including root cause, and documenting remediation required to address root cause 10.8 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder and anomaly and addressing any security issues that arose during the failure 10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder and accountented, in use	Logs of all critical system components			
strategy, as determined by the organization's annual risk assessment. 10.6.3 Follow up exceptions and anomalies identified during the review process. 10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). 10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: Firewalls. IDSI/IPS FIM Anti-virus Physical access controls Logical access controls Audit logging mechanisms Segmentation controls (if used) Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: Restoring security functions Identifying and documenting the duration (date and time start to end) of the security failure Identifying and addressing any security issues that arose during the failure Performing a risk assessment to determine whether further actions are required as a result of the security failure Inflementing controls to prevent cause of failure for meoccurring Resuming monitoring of security controls Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties. 11.1 Implement processes to to lest for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.	systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).			
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). 10.8 Additional requirement for service providers only. Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: Firewalls IDS/IPS FIMI Anti-virus - Physical access controls - Logical access controls - Audit logging mechanisms Segmentation controls (if used) Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: - Restoring security functions Identifying and documenting the duration (date and time start to end) of the security failure Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause Identifying an addressing any security issues that arose during the failure Performing a risk assessment to determine whether further actions are required as a result of the security failure Implementing controls to prevent cause of failure from reoccurring Resuming monitoring of security controls Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties. 11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components		х	Х	
example, online, archived, or restorable from backup). 10.8 Additional requirement for service providers only. Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: - Firewalls - IDS/IPS - FIM - Anti-virus - Physical access controls - Audit logging mechanisms - Segmentation controls (if used) - Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely - Restoring security functions - Identifying and documenting the duration (date and time start to end) of the security failure - Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause - Identifying and addressing any security issues that arcose during the failure - Performing a risk assessment to determine whether further actions are required as a result of the security failure - Implementing controls to prevent cause of failure from reoccurring - Resuming monitoring of security controls - Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder - Restorming and addressing any security issues that arcose during the failure - Performing a best practice until January 31, 2018, after which it becomes a requirement. 10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder - Restorming and addressing any security security and the security policies and operational procedures for monitoring all access to network resources and cardholder - Restorming and addressing and procedures for monitoring all access to network resources and cardholder - Restorming and the security policies and operational proc	10.6.3 Follow up exceptions and anomalies identified during the review process.	х	х	
of critical security control systems, including but not limited to failure of: Firewalls IDS/IPS FIRM LOS/IPS FIRM Anti-virus Physical access controls Logical access controls Audit logging mechanisms Segmentation controls (if used) Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: Restoring security functions Identifying and documenting the duration (date and time start to end) of the security failure Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause Identifying and addressing any security issues that arose during the failure Performing a risk assessment to determine whether further actions are required as a result of the security failure Implementing controls to prevent cause of failure from recocurring Resuming monitoring of security controls Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder ada are documented, in use, and known to all affected parties. 11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and an anuthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Note: Methods that may be used, they must be sufficient to detect and identify both authorized and unauthorized devices.		х	х	
- Audit logging mechanisms - Segmentation controls (if used) Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: - Restoring security functions - Identifying and documenting the duration (date and time start to end) of the security failure - Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause - Identifying and addressing any security issues that arose during the failure - Performing a risk assessment to determine whether further actions are required as a result of the security failure - Implementing controls to prevent cause of failure from reoccurring - Resuming monitoring of security controls - Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder - data are documented, in use, and known to all affected parties. 11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Welthods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices. 11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	of critical security control systems, including but not limited to failure of: - Firewalls - IDS/IPS - FIM - Anti-virus - Physical access controls	х	×	
manner. Processes for responding to failures in security controls must include: Restoring security functions Identifying and documenting the duration (date and time start to end) of the security failure Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause Identifying and addressing any security issues that arose during the failure Performing a risk assessment to determine whether further actions are required as a result of the security failure Implementing controls to prevent cause of failure from reoccurring Resuming monitoring of security controls Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties. 11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices. 11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	Audit logging mechanisms Segmentation controls (if used) Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.			
Identifying and addressing any security issues that arose during the failure Performing a risk assessment to determine whether further actions are required as a result of the security failure Implementing controls to prevent cause of failure from reoccurring Resuming monitoring of security controls Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties. 11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices. 11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	manner. Processes for responding to failures in security controls must include: Restoring security functions Identifying and documenting the duration (date and time start to end) of the security failure Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address	x	x	
data are documented, in use, and known to all affected parties. 11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices. 11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	Identifying and addressing any security issues that arose during the failure Performing a risk assessment to determine whether further actions are required as a result of the security failure Implementing controls to prevent cause of failure from reoccurring Resuming monitoring of security controls			
and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices. 11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.		x	х	
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.	х		
			+	

AVS Instructure AVS Instructure Custor	Instructure PCI Responsibility Matrix		Responsibilit	V
such as new system component intelliations, changes in network topology, firmwall null emotifications, product agrophes). 1.2 Perform quantify internal vulnerabilities and perform accesses to writing all pith tail. 1.2 Perform quantify internal vulnerabilities are profrom accesses to writing all pith tail. 1.2 Perform quantify described from the control of the	Requirement	AWS		Customer
12.1 Perform quarterity internal wulercality scans. Address vulnerabilities are revolved in accordance with earthry a vulnerabilities are revolved in accordance with the entity's vulnerabilities are revolved in accordance with the entity's vulnerability revolved process. The entity of the entity's vulnerability revolved by the Payment valor of the entity's vulnerability scans, via an Approvad Scanning Vindor (ASV) approvad by the Payment V. X. X. 1. 2.2 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed via a second vindors and valority of the entity of the entit	11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network		х	
indicated specially Siturations Council (PCI SSC). Perform interest and receives as needed, until passing scans are achieved: 1.2.3 Perform interest and endernal scans, and receives as needed, after any significant change. Scans must be performed: x	reference to the system companies inflammations, what we have the system companies and perform rescans to verify all "high risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.	х	х	
y qualified personnel. I Independent a methodology for penetration testing approaches (for example, NIST SP800-115) Is based on industry acception penetration testing approaches (for example, NIST SP800-115) Includes testing from both inside and outdate the network Includes testing from both inside and outdate the network Includes testing from both inside and outdate the network Includes testing from both inside and outdate the network Includes testing from both inside and outdate the network Includes testing from the penetration testing is obtained to the inside outdate the network includes review and consideration of threats and vulnerabilities separationed in the last 12 months. Includes review and consideration of threats and vulnerabilities expenienced in the last 12 months. Includes review and consideration of threats and vulnerabilities expenienced in the last 12 months. In 12 Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or oxidification (such as in operating systems upgrade, as sub-involved added to the environment). In 2 Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or oxidification (such as an operating system) and upgrade, as sub-involved added to the environment). In 3 Exportation below vulnerabilities found during penetration testing are corrected and testing is repeated to verify the x x constitution of the penetration of the	11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.	х	х	
1.3 Implement a methodology for penetration testing plan includes the following: Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) Includes coverage for the entire CDC perimeter and official systems Includes Setting to violation and sooper-feed of the control of the company of the control of th	11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	х	х	
indification (such as an operating system juggrade, a sub-network added to the environment, or a web server added to the vironment). 13.2 Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or x voidification (such as an operating system juggrade, a sub-network added to the environment, or a web server added to the environment). 13.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the x x voidification (such as a penetration testing are corrected and testing is repeated to verify the x x voidification (such as a penetration testing on the penetration testing on segmentation controls at least every six months and after any changes to segmentation and effective, and olate all sut-of-scope systems from systems in the CDE. 13.4 I.4 Additional requirement for service providers only. If segmentation is used, confirm PCI DSS scope by performing entertain testing on segmentation controls at least every six months and after any changes to segmentation or to segment the segmentation or to segment the segmentation or to segment the segmentation of the s	11.3 Implement a methodology for penetration testing that includes the following: Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) Includes coverage for the entire CDE perimeter and critical systems Includes testing from both inside and outside the network Includes testing to validate any segmentation and scope-reduction controls Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 Defines network-layer penetration tests to include components that support network functions as well as operating systems Includes review and consideration of threats and vulnerabilities experienced in the last 12 months Specifies retention of penetration testing results and remediation activities results.	х	х	
indification (such as air operating system upgrade, a sub-network added to the environment). 1.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the microchons. 1.3.4 Insploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the microchons. 1.3.4 Insploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the microchons. 1.3.4 Insploitable vulnerabilities of the CDE. If from other networks, perform penetration tests at least annually and after x y changes to segmentation controls with the companies of the control of the c	11.3.1 Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	х	х	
orrections. 1.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after ny changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and oldate all out-of-scope systems from systems in the CDE. 1.3.4 I Additional requirement for service providers only. If segmentation is used, confirm PCI DSS scope by performing enertation testing on segmentation controls at least servey six months and after any changes to segmentation on ontrols/methods. 1.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Intrusion-detection and/or intrusion-prevention engines and after any changes to segmentation on ontrols/methods. 1.5 Deploy a change-detection mechanism (for example, fle-integrity monitoring tools) to afer personnel to unauthorized configuration (including changes, additions, and deletions) of critical system files, configuration files, or content files; and orifique the software to perform critical fle comparisons at least weekly. 1.5.1 Implement a process to respond to any alerts generated by the change-detection solution. 1.5.1 Ensure that security policies and operational procedures for security monitoring and festing are documented, in use, and vown to all affected parties. 1.5.1 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and vown to all affected parties. 1.5.1 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and vown to all affected parties. 1.5.2 Implement a rich assessment process that: 1.5.3 performed at least annually and update the policy when the environment changes. 2.5 Implement an individual process that: 1.5 performed at least annually and upon significant changes to the environment (for example, acquisition, merger, society) and the security policies and environment and proc	11.3.2 Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	х	х	
ny changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and oldet all out-of-scope systems from systems in the CDE. 1.3.4.1 Additional requirement for service providers only: if segmentation is used, confirm PCI DSS scope by performing enteration testing on segmentation controls at least every six months and after any changes to segmentation on ontrols and prevention controls and least every six months and after any changes to segmentation on ontrols and prevention controls at least every six months and after any changes to segmentation on ontrols and prevention controls and prevention techniques to detect and/or prevent intrusions into the network. In Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. In Septial proposed to suspected compromises. In Septial proposed to any alerts generated by the change on suspected compromises. In Septial proposed to perform critical file comparisons of least veeling. In Septial proposed to any alerts generated by the change configuration files, or content files, and ordination in the control of the c	11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	х	х	
enertation testing on segmentation controls at least every six months and after any changes to segmentation ontorios/methods. 1.4 Use influsion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Including the provided of the cardioider data environment as well as at critical points in the cardioider data environment as well as at critical points in the cardioider data environment, and alert personnel to suspected compromises. 1.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to after personnel to unauthorized notification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and onligure the software to perform critical file comparisons at least weekly. 1.5 Implement a process to respond to any alerts generated by the change- detection solution. 1.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and now to all affected parties. 2.1 Establish, publish, maintain, and disseminate a security policy. 2.1.1 Review the security policy at least annually and update the policy when the environment changes. 2.1.1 Review the security policy at least annually and update the policy when the environment changes. 2.1.1 Review the security policy and upon significant changes to the environment (for example, acquisition, merger, adoctor), etc.). 2.1.1 Review the security and upon significant changes to the environment (for example, acquisition, merger, adoctor), etc., and any unique and	11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	х	x	
Intortior all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data mixronment, and aller personnel to suspected compromises. keep all intrusion-detection and prevention engines, baselines, and signatures up to date. 15. El pelly of a hange-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized outlined provided to the provided of the p	11.3.4.1 Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.	х	x	
nodification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and onliquer the software to perform critical file comparisons at least weekly. 1.5.1 Implement a process to respond to any alerts generated by the change- detection solution. x	11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	х	X	
1.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and 2.1 Establish, publish, maintain, and disseminate a security policy. 2.1.1 Review the security policy at least annually and update the policy when the environment changes. 2.2 Implement a risk-assessment process that: 3.2 Experiment of test least annually and upon significant changes to the environment (for example, acquisition, merger, slocation, etc.), identifies critical assets, threats, and vulnerabilities, and Results in a formal, documented analysis of risk. 2.3 Experiment of the translation of critical technologies and define proper use of these technologies. 3.3 Experiment of critical technologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30. 3.4 Experiment of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, abbets, removable electronic media, e-mail usage and Internet usage. 3.4 Experiment of the following: 4.2 Security of the technology 4.2 Security of the technology 5.2 Security of the technology 5.2 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices) 4.2 Security of the technology 5.2 Security of the technologies 5.2 Security of the technologies 6.2 Security of the 6.2 Security of th	11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	х	х	
nown to all affected parties. 2.1 Establish, publish, maintain, and disseminate a security policy. 2.1.1 Review the security policy at least annually and update the policy when the environment changes. 2.1 Inglement a risk-assessment process that: 1 sperformed at least annually and upon significant changes to the environment (for example, acquisition, merger, slocation, etc.). 1 dentifies critical assets, threats, and vulnerabilities, and 2 results in a formal, documented analysis of risk. 2 samples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30. 2.3 Develop usage policies for critical technologies and define proper use of these technologies, laptops, slote; Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, slote; sexual period of the remote access and wireless technologies, laptops, slotes, removable electronic media, e-mail usage and Internet usage. 2.3 Explicit approval by authorized parties 2.3.1 Explicit approval by authorized parties 2.3.2 Authentication for use of the technology 2.3.3 A list of all such devices and personnel with access 2.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and of inventorying of devices) 2.3.5 Acceptable uses of the technology 2.3.6 Acceptable network locations for the technologies 2.3.7 List of company-approved products 2.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and usiness partners, with immediate deactivation after use 2.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage (cardholder data on local hard drives and removable electronic media, unless explicitly authorized for a defined business ed. 2.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. 2.4 Ensure that the	11.5.1 Implement a process to respond to any alerts generated by the change- detection solution.	х	х	
2.1.1 Review the security policy at least annually and update the policy when the environment changes. 2.2 Implement a risk-assessment process that:	11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	х	х	
2.2 Implement a risk-assessment process that: Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, alcoration, etc.). Identifies critical assets, threats, and vulnerabilities, and Results in a formal, documented analysis of risk. Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30. 2.3 Develop usage policies for critical technologies and define proper use of these technologies. Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, albets, removable electronic media, e-mail usage and Internet usage. Insure these usage policies require the following: 2.3.1 Explicit approval by authorized parties 2.3.2 Authentication for use of the technology 2.3.3 A list of all such devices and personnel with access 2.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices) 2.3.5 Acceptable uses of the technology 2.3.6 Acceptable uses of the technology 2.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity 2.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and usiness partners, with immediate deactivation after use 2.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business end. A cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business end. A cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business end. A cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business	12.1 Establish, publish, maintain, and disseminate a security policy.		х	
Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, blocation, etc.), Identifies critical assets, threats, and vulnerabilities, and Research (and successed to the control of the contro	12.1.1 Review the security policy at least annually and update the policy when the environment changes.		х	
Ensure these usage policies require the following: 2.3.1 Explicit approval by authorized parties x 2.3.2 Authentication for use of the technology x 2.3.3 A list of all such devices and personnel with access 2.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, nd/or inventorying of devices) 2.3.5 Acceptable uses of the technology 2.3.6 Acceptable network locations for the technologies 2.3.7 List of company-approved products 2.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity 2.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and usiness partners, with immediate deactivation after use 2.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage for cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business each. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all pplicable PCI DSS Requirements. 2.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. x x x x x x x x x x x x x	12.2 Implement a risk-assessment process that: Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), Identifies critical assets, threats, and vulnerabilities, and Results in a formal, documented analysis of risk. Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30. 12.3 Develop usage policies for critical technologies and define proper use of these technologies. Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, technologies and laterate transport to the second of the		x	
2.3.2 Authentication for use of the technology 2.3.3 A list of all such devices and personnel with access 2.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, nd/or inventorying of devices) 2.3.5 Acceptable uses of the technology 2.3.6 Acceptable network locations for the technologies 2.3.7 List of company-approved products 2.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity 2.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and usiness partners, with immediate deactivation after use 2.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage for cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business ed. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all pplicable PCI DSS Requirements. 2.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. x to retection of cardholder data and a PCI DSS compliance program to include: Overall accountability for maintaining PCI DSS compliance program to include:	Ensure these usage policies require the following:			
2.3.3 A list of all such devices and personnel with access 2.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, nd/or inventorying of devices) 2.3.5 Acceptable uses of the technology 2.3.6 Acceptable network locations for the technologies 2.3.7 List of company-approved products 2.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity 2.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and usiness partners, with immediate deactivation after use 2.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage for dardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business eded. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all pplicable PCI DSS Requirements. 2.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. x rote that the security policy and procedures clearly define information security responsibility for the rotection of cardholder data and a PCI DSS compliance program to include: Overall accountability for maintaining PCI DSS compliance	,			
2.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, nd/or inventorying of devices) 2.3.5 Acceptable uses of the technology 2.3.6 Acceptable network locations for the technologies 2.3.7 List of company-approved products 2.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity 2.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and usiness partners, with immediate deactivation after use 2.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage for cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business eed. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all pplicable PCI DSS Requirements. 2.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. 2.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the rotection of cardholder data and a PCI DSS compliance program to include: Overall accountability for maintaining PCI DSS compliance	••			
2.3.5 Acceptable uses of the technology x 2.3.6 Acceptable network locations for the technologies x 2.3.7 List of company-approved products x 2.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity x 2.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and usiness partners, with immediate deactivation after use x 2.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage for cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business ead. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all pplicable PCI DSS Requirements. 2.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. 2.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the rotection of cardholder data and a PCI DSS compliance program to include: Overall accountability for maintaining PCI DSS compliance	12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding,			
2.3.6 Acceptable network locations for the technologies x 2.3.7 List of company-approved products x 2.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity x 2.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and usiness partners, with immediate deactivation after use 2.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage for cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business ead. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all pplicable PCI DSS Requirements. 2.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. 2.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the rotection of cardholder data and a PCI DSS compliance program to include: Overall accountability for maintaining PCI DSS compliance	, ,			
2.3.7 List of company-approved products 2.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity 2.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and usiness partners, with immediate deactivation after use 2.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage for cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business ead. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all pplicable PCI DSS Requirements. 2.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. 2.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the rotection of cardholder data and a PCI DSS compliance program to include: Overall accountability for maintaining PCI DSS compliance			+	
2.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity 2.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and usiness partners, with immediate deactivation after use 2.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage for cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business eed. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all pplicable PCI DSS Requirements. 2.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. 2.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the rotection of cardholder data and a PCI DSS compliance program to include: Overall accountability for maintaining PCI DSS compliance	· •			
2.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and usiness partners, with immediate deactivation after use 2.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage for cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business ead. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all pplicable PCI DSS Requirements. 2.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. 2.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the rotection of cardholder data and a PCI DSS compliance program to include: Overall accountability for maintaining PCI DSS compliance	12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity			
2.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage f cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business eed. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all pplicable PCI DSS Requirements. 2.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. x 2.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the rotection of cardholder data and a PCI DSS compliance program to include: Overall accountability for maintaining PCI DSS compliance	12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and		+	
pplicable PCI DSS Requirements. 2.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. 2.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the rotection of cardholder data and a PCI DSS compliance program to include: Overall accountability for maintaining PCI DSS compliance	12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.		х	
2.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the rotection of cardholder data and a PCI DSS compliance program to include: Overall accountability for maintaining PCI DSS compliance	Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.			
rotection of cardholder data and a PCI DSS compliance program to include: Overall accountability for maintaining PCI DSS compliance	12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.		х	
	12.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: Overall accountability for maintaining PCI DSS compliance Defining a charter for a PCI DSS compliance program and communication to executive management		х	
	12.5 Assign to an individual or team the following information security management responsibilities:		x	
	12.5.1 Establish, document, and distribute security policies and procedures.			

Instructure - Confidential

Requirement List 2.5 Albertion is and analyses escurity sleets and information, and distribute to appropriate personnel. 2.5 Albertion is additional distribute oscurity incident reagones and sealation procedures to ensure timely and definition of albertions. 2.5 Albertion analyses of albertions. 2.5 Albertion and of albertions. 2.5 Albertion analyses of albertions. 2.5 Albertion and control albertion. 2.5 Albertio	Instructure PCI Responsibility Matrix	R	esponsibility	у
12.5.5 Exablation, document students distribute security incident response and escalation procedures to ensure timely and distribute security incidents, including additions, deletions, and modifications. 12.6.4 Animation incident security solicity and procedures to the control of a security policy and procedures. 12.6 Simplement a formal security awareness program to make all personnel awaren of the carbinder data security policy and procedures. 12.6 Simplement and provide security awareness program to make all personnel awaren of the carbinder data security policy and procedures. 12.7 Simplement and provide provide the security policy and procedures are provided to advantage and the security policy and procedures. 12.7 Simplement policities personnel prior to his to maintaine the first of attacks from internal sources. (Examples of background A. X. Decembers	Requirement	AWS	Instructure	Customer
effective handling of all shabotoms. 2.6.3.6.4.4.6.minion tear accounts, including additions, deletions, and modifications. 2.6.1.2.6.4.4.6.minion tear accounts, including additions, deletions, and modifications. 2.6.1.2.6.1.2.6.f. replaced is characteristic and success to data. 2.6.2.6.1.2.6.f. replaced is characteristic and success to data. 2.6.2.6.6.1.2.6.6.1.2.2.6.1.2.6.1.2.2.2.2	12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.		x	
12.5 S Mortion and control all access to data.	effective handling of all situations.		х	
12.6 In classical personnel for him all security power and an extension of the certification	•			
Jackedures. 12.6.2 Education personnel to achievale an autually that they have read and understood the security policy and procedures. 12.7.3 Common potential personnel to achievale get at least annually. That they have read and understood the security policy and procedures. 12.7.3 Common potential personnel procedures from the procedure of a common potential personnel procedure from the procedure of a common potential personnel procedures from the procedure of a common potential personnel procedure from the procedure of the				
12.6.2 Require personnel to achinovelogie at least annually that they have read and understood the security policy and procedures. 12.7. Stores potential personnel prior to his to minimize the risk of attacks from internal sound checks. 12.8. Marinan a interplement profices and procedures to manage service provides with whom candidated data is shared, or 12.8. Marinan a interplement profices and procedures to manage service provides with whom candidated data is shared, or 12.8. Marinan a interplement profices and procedures to manage service provides. 12.8. A Marinan a virtical appearance that includes an automotecogeneous that the service provides are responsible for the secondary of candidated data the service provides possess or or invention at the service provides and responsible of the secondary of candidated data the service provides possess or or invention to the service to the secondary of the secondary of candidated data the service provides responsible for the secondary of the seco	procedures.		X	
Jacobs in vision is previous employment history, oriminal to the risk of attacks from internal sources. (Examples of background concide include previous employment history, oriminal record, ored history, and reference oriceks.) 12.8 I Mariana an emplement policies and procedures to manage service providers with whom carbodier data is shared, or least the provider of the providers of the provid	•			
checks include previous employment history, original record, oredit history, and reference checks.) 2.8 Almaham an implement protices and procedures to manage service provided. 3. X X X X X X X X X X X X X X X X X X X			х	
that could affect the security of cardholder data, as follows: 12.8 at Maintain a list of service provides including a description of the service provider provider are responsible for the security of cardholder data the service providers possess or of trained in the half of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. 12.3 at Finantian in Impact the security of the customer's cardholder data environment. 12.3 at Finantian in Impact the security of the customer's cardholder data environment. 12.3 at Finantian in Impact the security of the customer's cardholder data environment. 12.3 at Finantian in Impact the security of the customer's cardholder data environment. 12.4 at Finantian in Impact the security of the customer's cardholder data environment. 12.5 at Finantian in Impact the security of the customer's cardholder data the service provider and the service of the service provider and the service provider			х	
12.2.2 Maintain a written agreement that includes an acknowledgment that the service providers are responsible for the security of carthoder data the service providers passes or otherwise store, process or framents to be best of the customer, or to the extent that they could impact the security of the customer's carcholder data environment. 12.3.8 Tensur there is an established process for engaging service providers including proper due diligence prior to engagement. 12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually. 12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually. 12.9 Additional requirement for service providers only. Service providers acknowledge in writing to customers that they are responsible for the service providers only. Service providers acknowledge in writing to customers that they are responsible for the service providers only. Service providers acknowledge in writing to customers that they are responsible for the service providers acknowledge in writing to customers that they are responsible for the service providers acknowledge in writing to customers that they are responsible for the service providers acknowledge in writing to customers that they are responsible for the service providers acknowledge in writing to customers that they are responsible for the service providers acknowledge in writing to customers that they are responsible for the service providers acknowledge in writing to customers and they are responsible for the service providers acknowledge in writing to customers and they are responsible for the service providers and they are responsible for the service providers acknowledge in writing to customers acknowledge in writing to customers and they are responsible for the payment branch. 12.10 a Cheeving responsible providers on the payment branch. 12.10 a Deciginate requirements for reporting compromises acknowledge in writing to customers and acknowledge in writing to customer				
security of cardinoter data the service providers possess or otherwise store, process or inament on behalf of the customer, or to the electent that they could impact the security of the customer's cardinoted rotte environment. 12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagingenient. 12.8.4 Maintain in program to monitor service providers' PCI DSS compliance status at least annually. 12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. 12.8.6 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. 12.8.6 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. 12.8.7 Maintain and the entity of the entity. 12.8.7 Maintain and entity of the entity of t	12.8.1 Maintain a list of service providers including a description of the service provided.		х	х
engagement. 12.8.4 Maintain a program to monitor service providers PCI DSS compliance status at least annually. 2.8.4 Maintain information about which PCI DSS requirements are managed by each service provider; and which are managed by the entity. 12.9 Additional requirement for service providers only. Service providers acknowleds in writing to customers that they are responsible for the security of arthody draft are service; provider possesses or otherwise stores, processes, or thransition to behalf of the customer, or to the extent that they could impact the security of the customer's carchoder data environment. 12.10 in Implement in incident response plan. Be prepared to responditure protects. 12.10 in Ingeneral in incident response plan is the prepared to responditure protects. 12.10 Ingeneral in incident response plan is the prepared to responditure protects. 12.10 Ingeneral in incident response plan is the prepared to responditure protects. 12.10 Ingeneral response proceeds. 12.10 Ingeneral response protection and communication and contact strategies in the event of a compromise including notification of the Specific incident response procedures. 12.10 Ingeneral response processes. 12.10 Ingeneral	security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or		х	х
12.8.4 Meintain a program to monitor service providers PCI DSS compliance status at least annually. 2.8.5 Seharita information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. 2.9.4 Seharita incident response providers only. Service providers acknowledge in writing to customers that they are responsible for the security of cardinolder data the service providers providers only. Service providers expresses or otherwise stores, processes, or transmits on behalf of the customer's cardinolder data or work or the security of cardinolder data entity that the service provider provider possesses or otherwise stores, processes, or transmits on behalf of the customer's cardinolder data environment. 2.10 Implement an incident response plan. Be prepared to respond immediately to a system breach. 2.11 12.10 Termital incident response plan. Be prepared to respond immediately to a system breach. 2.12 10.11 Create the incident response plan. Be prepared to respond immediately to a system breach. 2.13 10.11 Create the incident response plan. Be prepared to respond immediately to a system breach. 2.14 10.11 Create the response procedures 3.15 Seporide incident response procedures 3.16 Seporide incident response procedures 3.16 Several possesses 3.17 Seporide incident response procedures 3.18 Seporide incident response procedures 3.18 Seporide incident response procedures from the payment brands. 2.19 Seporide proteins processes 3.19 Seporide incident response procedures from the payment brands. 2.19 Seporide proteins of response procedures from the payment brands. 2.19 Seporide proteins from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, freewalts, and file-integrity monitoring systems. 3.19 Seporide processes incident from service providers only. Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following process			х	X
managed by the entity. 12.9 Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardiholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customers cardiholder data environment. 12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach. 12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach. 12.10 Implement in incident response plan to be implemented in the event of a system breach. 12.10 Implement an incident response plan to be implemented in the event of system breach. 12.10 Implement an incident response plan to be implemented in the event of system breach. 12.10 Implement an incident response plan to be implemented in the event of system breach. 12.10 Implementation of the payment branch, at a minimum district substance in the control of the payment branch, at a minimum district substance in the payment branch, at a minimum district substance in control of the payment branch. 12.10 Implementation of incident response procedures from the payment branch. 12.10 Implementation of incident response procedures from the payment branch. 12.10 Implementation of incident response plan of the payment branch. 12.10 Implementation of incident responses procedures from the payment branch. 12.10 Implementation of incident responses plan of the payment branch. 12.10 Implementation of incident responses plan of the payment branch. 12.10 Implementation of incident prepared to the payment branch. 12.10 Implementation of incident responses plan of the payment branch. 12.10 Implementation of the plan incident payment branch. 12.10 Implementation of t			x	Х
12.9 Additional requirement for service providers only. Service providers acknowledge in writing to customers that they are responsible for the security of cardiodider data the service provider possesses or otherwise stores, processes. or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. 12.10.1 Create the incident response plan. Be prepared to respond immediately to a system breach. 12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum. 13.01.1 Create the incident response plan to be implemented in the event of a compromise including notification of the payment brands, at a minimum. 13.01.1 Create the incident response procedures 13.01.1 Create the incident response procedures from the payment brands. 13.01.1 Create the incident response procedures from the payment brands. 13.01.1 Create the incident response procedures from the payment brands. 13.01.1 Create the incident response procedures from the payment brands. 13.01.1 Create the incident response procedures from the payment brands. 13.01.1 Create the incident response procedures from security monitoring systems. Including but not limited to intrusion-detection, intrusion-prevention, for a process to modify and evolve the incident response plan according to lessons learned and to incorporate incident response procedures from security monitoring systems. 13.01.1 Create the incident requirement for service providers only. Perform reviews at least quarterly to confirm personnel are following a create from security and procedures. Review			х	х
12.10 Inglement an incident response plan. Be prepared to respond immediately to a system breach. 2.10.11 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the Rolley, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum specific microbilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum specific microbility procedures - Business recovery and continuity procedures - Analysis of legal requirement fall critical system compromes - Analysis of legal requirement fall critical system compromes - Analysis of legal requirement fall critical system compromes - Analysis of legal requirement fall critical system compromes - Analysis of legal requirement fall critical system compromes - Analysis of legal requirement fall critical system compromes - Analysis of legal requirement fall critical system compromes - Analysis of legal requirement by a system system and the system of the system	12.9 Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on		х	
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum in Specific incident response procedures Business recovery and continuity procedures Business recovery and continuity procedures Business recovery and continuity procedures Coverage and responses of all critical system components Coverage and responses of all critical system components Coverage and response of all critical systems coverage and response of all critical systems Coverage and response of all critical systems coverage and response of all critical systems Coverage and response of all critical systems coverage and cove			х	
Specific incident response procedures Data backup processes Justianes recovery and continuity procedures Data backup processes Justianes recovery and continuity procedures Coverage and responses of all critical system components Reference or inclusion of incident response procedures from the payment brands. 12.10.2 Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually. 12.10.3 Designate specific personnel to be available on a 24/T basis to respond to elerts. 12.10.4 Provide appropriate training to staff with security breach response responsibilities. 12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, freewalls, and file-integrity monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, freewalls, and file-integrity monitoring systems. 12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. 12.11.4 Additional requirement for service providers only. Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: Daily log reviews Firewall rule-set reviews Applying configuration standards to new systems Responding to security alerts Change management processes Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 12.11.1 Additional requirement for service providers only. Maintain documentation of quarterly review process to include: Documenting results of the reviews Review and sign-off results by personnel assigned responsibility for the PCI DSS compliance program Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. Al Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A1.1 through A1.4: A hosting provi	12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the			
12.10.2 Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually. 12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts. 12.10.4 Provide appropriate training to staff with security breach response responsibilities. 12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. 12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. 12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. 12.11.1 Additional requirement for service providers only. Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: 1. Designation of the service of the service providers only. Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: 1. Designation of the service of the service providers only. Maintain documentation of quarterly review process to include: 1. Designation of the service providers only. Maintain documentation of quarterly review process to include: 1. Documenting results of the reviews 1. Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program 1. Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 1. Al Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A1.1 through A1.4: 1. A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. 1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data envi	Specific incident response procedures Business recovery and continuity procedures Data backup processes Analysis of legal requirements for reporting compromises Coverage and responses of all critical system components			
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts. 12.10.4 Provide appropriate training to staff with security breach response responsibilities. 12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. 12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. 12.11 Additional requirement for service providers only. Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: 12.11 Additional requirement for service providers only. Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: 12.11.1 Additional requirement for service providers only. Maintain documentation of quarterly review process to include: 12.11.1 Additional requirement for service providers only. Maintain documentation of quarterly review process to include: 12.11.1 Additional requirement for service provider only. Maintain documentation of quarterly review process to include: 12.11.1 Additional requirement for service provider only. Maintain documentation of quarterly review process to include: 12.11.1 Additional requirement for service provider only. Maintain documentation of quarterly review process to include: 12.11.1 Additional requirement for service provider only. Maintain documentation of quarterly review process to include: 12.11.1 Additional requirement is a best practice until January 31, 2018, after which it becomes a requirement. 12.11.1 Additional requirement is a best practice until January 31, 2018, after which it becomes a requirement. 12.11.1 Additional requirement is a best practice until January 31, 2018, after which it becomes a requirement. 12.11.1 Additional requi				
12.10.4 Provide appropriate training to staff with security breach response responsibilities. 12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. 12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. 12.11.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. 12.11.1 Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: 12.11.1 Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: 12.11.1 Additional requirement for service providers only: Maintain documentation of quarterly review process to include: 12.11.1 Additional requirement for service providers only: Maintain documentation of quarterly review process to include: 12.11.1 Additional requirement for service provider sonly: Maintain documentation of quarterly review process to include: 12.11.1 Additional requirement for service provider sonly: Maintain documentation of quarterly review process to include: 12.11.1 Additional requirement for service provider, or other entity in becomes a requirement. 13.1.1 Ensure that each entity is (that is, merchant, service provider, or other entity) is cardholder data environment. 14.1.2 Restrict each entity only runs processes that have access to that entity's cardholder data environment. 15.1.2 Restrict each entity is access and privileges to its own cardholder data environment and consistent with processes. 16.1.3 Restrict each entity's access and privileges to its own cardholder data environment an				
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. 12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. 12.11 Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: - Daily log reviews - Polly log reviews - Firewall rule-set reviews - Applying configuration standards to new systems - Responding to security alerts - Change management processes Note: This requirement for service providers only: Maintain documentation of quarterly review process to include: - Documenting results by personnel assigned responsibility for the PCI DSS compliance program Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 12.11.1 Additional requirement is a best practice until January 31, 2018, after which it becomes a requirement. 12.11.1 Additional requirement is a best practice until January 31, 2018, after which it becomes a requirement. 12.11.1 Additional requirement is a best practice until January 31, 2018, after which it becomes a requirement. 12.11.1 Additional requirement is a best practice until January 31, 2018, after which it becomes a requirement. 12.11.1 Additional requirement is a best practice until January 31, 2018, after which it becomes a requirement. 12.11.1 Additional requirement is a best practice until January 31, 2018, after which it becomes a requirement. 12.11.1 Additional requirement is a best practice until January 31, 2018, after which it becomes a requirement. 12.11.1 Additional requirement is a best practice until January 31, 2018, after which it becomes a requirement. 12.11.1 Additional requirement is a best practice until January 31, 2018, after which it becomes a requ				
industry developments. 12.11 Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: Daily log reviews Applying configuration standards to new systems Responding to security alerts Change management processes Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 12.11.1 Additional requirement for service providers only: Maintain documentation of quarterly review process to include: Documenting results of the reviews Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. A1 Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A1.1 through A1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. A1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment. X X X A1.2 Restrict each entity's access and privileges to its own cardholder data environment and consistent with PCI DSS Requirement 10. A1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider. A2.1 Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either: Confirm the devices are not susceptible to any known exploits for those protocols. Or: Have a formal Risk Mitigation and Migration Plan in place. A2.2 Entities with existing implementations (other than as allowed in A2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.	12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention,			
security policies and operational procedures. Reviews must cover the following processes: Daily log reviews Firewall rule-set reviews Firewall rule-set reviews Perponding to security alerts Change management processes Note: This requirement a best practice until January 31, 2018, after which it becomes a requirement. 12.11.1 Additional requirement for service providers only: Maintain documentation of quarterly review process to include: Documenting results of the reviews Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. Al Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A1.1 through A1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. A1.1 Ensure that each entity's access and privileges to its own cardholder data environment. X X A1.2 Restrict each entity's access and privileges to its own cardholder data environment and consistent with PCI DSS Requirement 10. A1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider. A2.1 Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either: Confirm the devices are not susceptible to any known exploits for those protocols. Or. Have a formal Risk Mitigation and Migration Plan in place. A2.2 Entities with existing implementations (other than as allowed in A2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.			х	
Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. 12.11.1 Additional requirement for service providers only: Maintain documentation of quarterly review process to include: Documenting results of the reviews Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. A1 Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A1.1 through A1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. A1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment. X X A1.2 Restrict each entity's access and privileges to its own cardholder data environment and consistent with PCI DSS Requirement 10. A1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10. A1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider. A2.1 Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either: Confirm the devices are not susceptible to any known exploits for those protocols. Or: Have a formal Risk Mitigation and Migration Plan in place. A2.2 Entities with existing implementations (other than as allowed in A2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. A2.3 Additional Requirement for Service Providers Only: All service providers must provide a secure service offering by June X	security policies and operational procedures. Reviews must cover the following processes: Daily log reviews Firewall rule-set reviews Applying configuration standards to new systems Responding to security alerts		х	
Documenting results of the reviews Review and sign-off or results by personnel assigned responsibility for the PCI DSS compliance program Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. A1 Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A1.1 through A1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. A1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment. X	Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.			
A1 Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A1.1 through A1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. A1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment. X X X A1.2 Restrict each entity's access and privileges to its own cardholder data environment only. X X X A1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10. A1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider. A2.1 Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either: Confirm the devices are not susceptible to any known exploits for those protocols. Or: Have a formal Risk Mitigation and Migration Plan in place. A2.2 Entities with existing implementations (other than as allowed in A2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. A2.3 Additional Requirement for Service Providers Only: All service providers must provide a secure service offering by June	Documenting results of the reviews Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program		х	
A1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment. A1.2 Restrict each entity's access and privileges to its own cardholder data environment only. A1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10. A1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider. A2.1 Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either: Confirm the devices are not susceptible to any known exploits for those protocols. Or: Have a formal Risk Mitigation and Migration Plan in place. A2.2 Entities with existing implementations (other than as allowed in A2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. A2.3 Additional Requirement for Service Providers Only: All service providers must provide a secure service offering by June	A1 Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A1.1 through	х	х	
A1.2 Restrict each entity's access and privileges to its own cardholder data environment only. A1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10. A1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider. A2.1 Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either: Confirm the devices are not susceptible to any known exploits for those protocols. Or: Have a formal Risk Mitigation and Migration Plan in place. A2.2 Entities with existing implementations (other than as allowed in A2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. A2.3 Additional Requirement for Service Providers Only: All service providers must provide a secure service offering by June	A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS.			
A1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10. A1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider. A2.1 Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either: Confirm the devices are not susceptible to any known exploits for those protocols. Or: Have a formal Risk Mitigation and Migration Plan in place. A2.2 Entities with existing implementations (other than as allowed in A2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. A2.3 Additional Requirement for Service Providers Only: All service providers must provide a secure service offering by June		Х	х	
PCI DSS Requirement 10. A1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider. A2.1 Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either: Confirm the devices are not susceptible to any known exploits for those protocols. Or: Have a formal Risk Mitigation and Migration Plan in place. A2.2 Entities with existing implementations (other than as allowed in A2.1) that use SSL and/or early TLS must have a formal Risk Mitigation Plan in place. A2.3 Additional Requirement for Service Providers Only: All service providers must provide a secure service offering by June				
service provider. A2.1 Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either: Confirm the devices are not susceptible to any known exploits for those protocols. Or: Have a formal Risk Mitigation and Migration Plan in place. A2.2 Entities with existing implementations (other than as allowed in A2.1) that use SSL and/or early TLS must have a formal Risk Mitigation Plan in place. A2.3 Additional Requirement for Service Providers Only: All service providers must provide a secure service offering by June x		Х	х	
entity must either: Confirm the devices are not susceptible to any known exploits for those protocols. Or: Have a formal Risk Mitigation and Migration Plan in place. A2.2 Entities with existing implementations (other than as allowed in A2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. A2.3 Additional Requirement for Service Providers Only: All service providers must provide a secure service offering by June x		х	х	
Or: Have a formal Risk Mitigation and Migration Plan in place. A2.2 Entities with existing implementations (other than as allowed in A2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. A2.3 Additional Requirement for Service Providers Only: All service providers must provide a secure service offering by June	A2.1 Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either:		х	
A2.2 Entities with existing implementations (other than as allowed in A2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. A2.3 Additional Requirement for Service Providers Only: All service providers must provide a secure service offering by June	Or:			
A2.3 Additional Requirement for Service Providers Only: All service providers must provide a secure service offering by June x	A2.2 Entities with existing implementations (other than as allowed in A2.1) that use SSL and/or early TLS must have a formal		х	
	·		х	