Instructure PCI Responsibility Matrix	Responsibility		
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		x	
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	x	x	
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	x	
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.	x	x	
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.	x	x	
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	x	x	
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.	x	x	
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	x	x	
1.3.5 Permit only “established” connections into the network.	x	x	
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.	x	x	
1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties.	x	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.		x	
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.).	x	x	
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).	x	x	
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.)	x	x	
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	x	x	
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.	x	x	
2.2.4 Configure system security parameters to prevent misuse.	x	x	
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	x	x	
2.3 Encrypt all non-console administrative access using strong cryptography.	x	x	
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	x	x	
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	x	
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.	x	x	
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.		x	

Instructure PCI Responsibility Matrix	Responsibility		
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. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:		x	
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.		x	
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.		x	
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.		x	
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.		x	
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.		x	
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.		x	
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		x	
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.		x	
3.6 Fully document and implement all key- management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:			
3.6.1 Generation of strong cryptographic keys		x	
3.6.2 Secure cryptographic key distribution		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).		x	
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.		x	
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.		x	
3.6.7 Prevention of unauthorized substitution of cryptographic keys.		x	
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.		x	
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.		x	
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.	x	x	
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.		x	
4.2 Never send unprotected PANs by end- user messaging technologies (for example, e- mail, instant messaging, SMS, chat, etc.).		x	

Instructure PCI Responsibility Matrix	Responsibility		
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.	x	x	
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	x	x	
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	x	x	
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.	x	x	
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.	x	x	
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.	x	x	
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	x	x	
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.	x	x	
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.	x	x	
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, 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.	x	x	
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.	x	x	
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.	x	x	
6.4.2 Separation of duties between development/test and production environments	x	x	
6.4.3 Production data (live PANs) are not used for testing or development	x	x	
6.4.4 Removal of test data and accounts from system components before the system becomes active / goes into production.	x	x	
6.4.5 Change control procedures must include the following:	x	x	
6.4.5.1 Documentation of impact.	x	x	
6.4.5.2 Documented change approval by authorized parties.	x	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.	x	x	
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.	x	x	
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.	x	x	
6.5.2 Buffer overflows	x	x	
6.5.3 Insecure cryptographic storage	x	x	
6.5.4 Insecure communications	x	x	
6.5.5 Improper error handling	x	x	
6.5.6 All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 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	x	x	
6.5.7 Cross-site scripting (XSS)	x	x	
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).	x	x	
6.5.9 Cross-site request forgery (CSRF)	x	x	
6.5.10 Broken authentication and session management.	x	x	
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.	x	x	

Instructure PCI Responsibility Matrix	Responsibility		
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.	x	x	
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	x	x	
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.	x	x	
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	x	x	
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	x	
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:	x	x	
7.2.1 Coverage of all system components	x	x	
7.2.2 Assignment of privileges to individuals based on job classification and function.	x	x	
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.	x	x	
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:	x	x	
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	x	x	
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	x	x	
8.1.3 Immediately revoke access for any terminated users.	x	x	
8.1.4 Remove/disable inactive user accounts within 90 days.	x	x	
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.	x	x	
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	x	x	
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	x	x	
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.	x	x	
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	x	x	
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	x	x	
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.	x	x	
8.2.4 Change user passwords/passphrases at least once every 90 days.	x	x	
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.	x	x	
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.	x	x	
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	x	x	
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	x	x	
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.	x	x	
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.	x	x	
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.	x	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.	x	x	
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.	x	x	

Instructure PCI Responsibility Matrix	Responsibility		
Requirement	**AWS**	**Instructure**	**Customer**
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other 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).		x	
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	x	x	
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	x		
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 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.	x		
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.	x		
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	x		
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).	x		
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., are returned or disabled.	x		
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:	x		
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	x		
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	x		
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.	x		
9.5 Physically secure all media.	x	x	
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.	x	x	
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.	x	x	
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.	x	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).	x	x	
9.7 Maintain strict control over the storage and accessibility of media.	x	x	
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	x	x	
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:	x	x	
9.8.1 Shred, incinerate, or pulp hard- copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	x	x	
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) · Device serial number or other method of unique identification.		x	
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or 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.		x	
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	x	x	
10.1 Implement audit trails to link all access to system components to each individual user.	x	x	

Instructure PCI Responsibility Matrix	Responsibility		
Requirement	**AWS**	**Instructure**	**Customer**
10.2 Implement automated audit trails for all system components to reconstruct the following events:			
10.2.1 All individual user accesses to cardholder data	x	x	
10.2.2 All actions taken by any individual with root or administrative privileges	x	x	
10.2.3 Access to all audit trails	x	x	
10.2.4 Invalid logical access attempts	x	x	
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	x	x	
10.2.6 Initialization, stopping, or pausing of the audit logs	x	x	
10.2.7 Creation and deletion of system- level objects	x	x	
10.3 Record at least the following audit trail entries for all system components for each event:			
10.3.1 User identification	x	x	
10.3.2 Type of event	x	x	
10.3.3 Date and time	x	x	
10.3.4 Success or failure indication	x	x	
10.3.5 Origination of event	x	x	
10.3.6 Identity or name of affected data, system component, or resource.	x	x	
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	x	x	
10.4.1 Critical systems have the correct and consistent time.	x	x	
10.4.2 Time data is protected.	x	x	
10.4.3 Time settings are received from industry-accepted time sources.	x	x	
10.5 Secure audit trails so they cannot be altered.	x	x	
10.5.1 Limit viewing of audit trails to those with a job-related need.	x	x	
10.5.2 Protect audit trail files from unauthorized modifications.	x	x	
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	x	x	
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	x	x	
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	x	x	
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.	x	x	
10.6.1 Review the following at least daily: · All security events · Logs of all system components that store, process, or transmit CHD and/or SAD · 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.).	x	x	
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.	x	x	
10.6.3 Follow up exceptions and anomalies identified during the review process.	x	x	
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).	x	x	
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 · 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.	x	x	
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.	x	x	
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.	x	x	
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.	x		
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	x		
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.	x		

Instructure PCI Responsibility Matrix	Responsibility		
Requirement	**AWS**	**Instructure**	**Customer**
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).		x	
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities 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.	x	x	
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.	x	x	
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	x	x	
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.	x	x	
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).	x	x	
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).	x	x	
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	x	x	
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.	x	x	
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.	x	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.	x	x	
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.	x	x	
11.5.1 Implement a process to respond to any alerts generated by the change- detection solution.	x	x	
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	x	x	
12.1 Establish, publish, maintain, and disseminate a security policy.		x	
12.1.1 Review the security policy at least annually and update the policy when the environment changes.		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.		x	
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, tablets, removable electronic media, e-mail usage and Internet usage. Ensure these usage policies require the following:			
12.3.1 Explicit approval by authorized parties		x	
12.3.2 Authentication for use of the technology		x	
12.3.3 A list of all such devices and personnel with access		x	
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)		x	
12.3.5 Acceptable uses of the technology		x	
12.3.6 Acceptable network locations for the technologies		x	
12.3.7 List of company-approved products		x	
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity		x	
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use		x	
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. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.		x	
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.		x	
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		x	
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.		x	

Instructure PCI Responsibility Matrix	Responsibility		
Requirement	**AWS**	**Instructure**	**Customer**
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.		x	
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.		x	
12.5.4 Administer user accounts, including additions, deletions, and modifications.		x	
12.5.5 Monitor and control all access to data.		x	
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.		x	
12.6.1 Educate personnel upon hire and at least annually.		x	
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.		x	
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)		x	
12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:			
12.8.1 Maintain a list of service providers including a description of the service provided.		x	x
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.		x	x
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.		x	x
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.		x	x
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.		x	x
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 behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.		x	
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.		x	
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 · 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 · Reference or inclusion of incident response procedures from the payment brands.		x	
12.10.2 Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually.		x	
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.		x	
12.10.4 Provide appropriate training to staff with security breach response responsibilities.		x	
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.		x	
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.		x	
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 · 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.		x	
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.		x	
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.	x	x	
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 only.	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.	x	x	
A1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	x	x	
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.		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 Risk Mitigation and Migration Plan in place.		x	
A2.3 Additional Requirement for Service Providers Only: All service providers must provide a secure service offering by June 30, 2016.		x	