Citrix Cloud-based Services

Overview

This responsibility matrix has been created to clarify the PCI compliance responsibilities for Citrix and the customers of Citrix Cloud-based Services to support Citrix customers implementing security controls for their use of Citrix Cloud-based Services.

Citrix is a global software company providing server, application and desktop virtualization, networking, software-as-a-service (SaaS), and cloud computing technologies. Compliance to PCI DSS is dependent on which Citrix Cloud-based Services are being utilized and how they are being implemented by the customer. Customers may use these services to store, process, or transmit cardholder data however the method of use is not known to Citrix.

For a list of the services covered in the assessment please refer to the Attestation of Compliance available through the Citrix Trust Center.

Responsibility

Customers of Citrix are ultimately responsible for their own PCI DSS compliance while utilizing Citrix Cloud-based Services. This matrix describes the various responsibilities of Citrix, its customers, and those shared by both to achieve PCI DSS compliance.

As a service provider, Citrix provides this matrix for customers to satisfy specific PCI DSS requirements in conjunction with the Attestation of Compliance for the Cloud-based Service. Most requirements require an understanding of the relationship of responsibilities between Citrix as the service provider and its customer as the administrator of the application. Alternatively, some requirements are the sole responsibility of the customer.

Attestation of Compliance

Citrix Systems Inc.'s 2022 PCI DSS 3.2.1 Attestation of Compliance can be downloaded for customer use at https://www.citrix.com/about/trust-center/

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
Install and maintain a firewall configuration to protect cardholder data							
1.1.1	Establish and implement firewall and router configuration standards that include the following: A formal process for approving and testing all network connections and changes to the firewall and router configurations.				X	Citrix is responsible for establishing firewall and router configuration standards for Citrix Cloud-based Services infrastructure.	Customer is responsible for establishing and implementing firewall and router configuration standards for devices and networks that are managed by them.
1.1.2	Establish and implement firewall and router configuration standards that include the following: Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.				X	Citrix is responsible for documenting all connections between the Citrix Cloud-based Services infrastructure and other networks including the customer network. This documentation includes a network diagram.	Customer is responsible for having a network diagram that depicts use of Citrix Cloud-based Services including all connections between Citrix Cloud-based services and the customer's cardholder data environment (CDE).
1.1.3	Establish and implement firewall and router configuration standards that include the following: Current diagram that shows all cardholder data flows across systems and networks.			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data transmitted within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for documenting all cardholder data flows across systems and networks. This documentation should be included in a form of a diagram.
1.1.4	Establish and implement firewall and router configuration standards that include the following: Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network.				X	Citrix is responsible for establishing firewall requirements at each internet connection and between any demilitarized zone (DMZ) and internal networks within the Citrix Cloud-based Services infrastructure.	Customer is responsible for establishing firewall requirements at each internet connection and between any demilitarized zone (DMZ) and internal networks managed by them.
1.1.5	Establish and implement firewall and router configuration standards that include the following: Description of groups, roles, and responsibilities for management of network components.				X	Citrix is responsible for establishing descriptions of groups, roles, and responsibilities for the management of network components within the Citrix Cloud-based Services infrastructure.	Customer is responsible for establishing descriptions of groups, roles, and responsibilities for the management of network components managed by them.
1.1.6	Establish and implement firewall and router configuration standards that include the following: Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.				X	Citrix is responsible for documenting the business justification for all services, protocols, and ports allowed within in the Citrix Cloud-based Services infrastructure. This documentation includes security features implemented for any protocols considered to be insecure.	Customer is responsible for documenting the business justification for all services, protocols, and ports allowed that are managed by them. This documentation should include security features implemented for any protocols considered to be insecure.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
1.1.7	Establish and implement firewall and router configuration standards that include the following: Requirement to review firewall and router rule sets at least every six months				X	Citrix is responsible for reviewing network security controls at least every six months within the Citrix Cloud-based Services infrastructure.	Customer is responsible for reviewing firewall and router rule sets at least every six months managed by them.
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.				X	Citrix is responsible for ensuring firewall and router configurations restrict connections between untrusted networks and system components within Citrix Cloud-based Services infrastructure.	Customer is responsible for ensuring firewall and router configurations managed by them restrict connections between untrusted networks and system components in their 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	Citrix is responsible for preventing inbound and outbound traffic to that which is necessary within the Citrix Cloud-based Services infrastructure. All other traffic is denied.	Customer is responsible for preventing inbound and outbound traffic managed by them to that which is necessary for their cardholder data environment. All other traffic should be denied.
1.2.2	Secure and synchronize router configuration files.				X	Citrix is responsible for securing router configuration files and ensuring the most current configuration is used at start-up for the Citrix Cloud-based Services infrastructure.	Customer is responsible for securing router configuration files managed by them and ensuring the most current configuration is used at start-up.
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		N/A for the Citrix Cloud-based Services infrastructure. Customer data transmitted within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for configuring firewalls that are managed by the customer between any on-premise wireless environments and their cardholder data environment.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data transmitted within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for ensuring no direct access exists between the public Internet and cardholder data environment system components managed by them.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.				X	Citrix is responsible for implementing a demilitarized zone (DMZ) that limits inbound traffic within the Citrix Cloud-based Services infrastructure. The DMZ is limited to system components that provide authorized, publicly accessible services, protocols, and ports.	Customer is responsible for implementing a demilitarized zone (DMZ) that limits inbound traffic managed by them. The DMZ must be limited to system components that provide authorized, publicly accessible services, protocols, and ports.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.				X	Citrix is responsible for ensuring that all inbound Internet traffic is limited to IP addresses within the demilitarized zone (DMZ) for the Citrix Cloud-based Services infrastructure.	Customer is responsible for ensuring that all inbound Internet traffic is limited to IP addresses within the demilitarized zone (DMZ) managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
1.3.3	Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.				X	Citrix is responsible for implementing anti-spoofing measures for the Citrix Cloud-based Services infrastructure.	Customer is responsible for implementing anti-spoofing measures for networks managed by them.
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.				X	Citrix is responsible for preventing unauthorized outbound traffic from the Citrix Cloud-based Services infrastructure to the internet.	Customer is responsible for preventing unauthorized outbound traffic from the cardholder data environment to the internet managed by them.
1.3.5	Permit only “established” connections into the network.				X	Citrix is responsible for ensuring that only established connections are permitted into Citrix Cloud-based Services infrastructure.	Customer is responsible for ensuring that only established connections into the network managed by them are permitted.
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		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for the placement of customer managed storage components in an internal network zone for systems managed by them.
1.3.7	Do not disclose private IP addresses and routing information to unauthorized parties. Note: Methods to obscure IP addressing may include, but are not limited to: - Network Address Translation (NAT) - Placing servers containing cardholder data behind proxy servers/firewalls, - Removal or filtering of route advertisements for private networks that employ registered addressing, - Internal use of RFC1918 address space instead of registered addresses.				X	Citrix is responsible for ensuring private IP address and routing information is not disclosed to unauthorized parties for Citrix Cloud-based Services infrastructure.	Customer is responsible for ensuring private IP address and routing information is not disclosed to unauthorized parties for systems managed by them.
1.4	Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the cardholder environment. Firewall configurations include: - Specific configuration settings are defined for personal firewall software. - Personal firewall software is actively running. - Personal firewall software is not alterable by users of mobile and/or employee-owned devices.			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for the protection of any mobile and/or employee-owned devices with access to the network(s) and cardholder data environment managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
1.5	Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.				X	Citrix is responsible for the security policies and operational procedures related to managing firewalls internally for the Citrix Cloud-based Services infrastructure. These policies and procedures should be disseminated and known to all associated parties.	Customer is responsible for documenting security policies and operational procedures of firewall management for systems managed by them. These policies and procedures should be disseminated and known to all associated parties.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
Do not use vendor-supplied defaults for system passwords and other security parameters							
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, Simple Network Management Protocol (SNMP) community strings, etc.).				X	Citrix is responsible for changing all default passwords and removing or disabling any unnecessary accounts and settings within the Citrix Cloud-based Services infrastructure.	Customer is responsible for changing all default passwords and removing or disabling any unnecessary accounts and settings for systems managed by them.
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		N/A for the Citrix Cloud-based Services infrastructure. Customer data transmitted within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for management of any wireless environment connected to the cardholder data environment managed by them.
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	Citrix is responsible for developing secure configuration standards for all system components within Citrix Cloud-based Services infrastructure. Citrix ensures these configurations address all known vulnerabilities and adhere to industry-accepted hardening standards.	Customer is responsible for developing secure configuration standards for all customer-deployed system components. It is also the responsibility of Customer to ensure these configurations address all known vulnerabilities and adhere to industry-accepted hardening standards.
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	Citrix is responsible for ensuring only one primary function is in use per server within Citrix Cloud-based Services infrastructure.	Customer is responsible for ensuring only one primary function is in use per server managed by them.
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.				X	Citrix is responsible for ensuring only necessary services, protocols, daemons, etc., are enabled on systems within Citrix Cloud-based Services infrastructure.	Customer is responsible for ensuring only necessary services, protocols, daemons, etc., are enabled on systems managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.				X	Citrix is responsible for ensuring industry-accepted additional security features are implemented for all insecure services, daemons and protocols that may be present on systems within the Citrix Cloud-based Services infrastructure.	Customer is responsible for ensuring industry-accepted additional security features are implemented for all insecure services, daemons and protocols for systems managed by them.
2.2.4	Configure system security parameters to prevent misuse.				X	Citrix is responsible for ensuring system configurations are established to prevent misuse of all systems within Citrix Cloud-based Services infrastructure.	Customer is responsible for ensuring system configurations are established to prevent misuse of all customer-deployed resources.
2.2.5	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.				X	Citrix is responsible for removing all unnecessary functionality. These functions may include scripts, drivers, web servers within Citrix Cloud-based Services infrastructure.	Customer is responsible for removing all unnecessary functionality. These functions may include scripts, drivers, web servers managed by them.
2.3	Encrypt all non-console administrative access using strong cryptography.				X	Citrix is responsible for ensuring industry-accepted cryptography is applied to all non-console administrative access for systems within the Citrix Cloud-based Services infrastructure.	Customer is responsible for ensuring industry-accepted cryptography is applied to all non-console administrative access for system managed by them.
2.4	Maintain an inventory of system components that are in scope for PCI DSS.				X	Citrix is responsible for maintaining an inventory of the system components within the Citrix Cloud-based Services infrastructure.	Customer is responsible for maintaining an accurate inventory of PCI relevant system components managed by them.
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	Citrix is responsible for documenting security policies and operational procedures for managing vendor default security parameters for systems within the Citrix Cloud-based Services infrastructure. These policies and procedures are disseminated and known to all associated parties.	Customer is responsible for documenting security policies and operational procedures for managing vendor default security parameters managed by them. These policies and procedures are disseminated and known to all associated parties.
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 A: Additional PCI DSS Requirements for Shared Hosting Providers.			X		N/A - Citrix is not a shared hosting provider	Where customer is a service provider they are responsible to ensure adherence to PCI DSS regarding shared hosting provider requirements.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
Protect stored cardholder data							
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 business requirements - Processes for secure deletion of data when no longer needed - Specific retention requirements for cardholder data - A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for implementing data retention and disposal on the systems managed by them.
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	Citrix is responsible for ensuring customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for ensuring that sensitive authentication data is not stored after authentication on the systems managed by them.
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	Citrix is responsible for ensuring customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for ensuring that track data is not stored after authentication on systems they manage.
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	Citrix is responsible for ensuring customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for ensuring that card verification data is not stored after authentication on systems managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.				X	Citrix is responsible for ensuring customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for ensuring that PIN card verification data is not stored after authentication on systems managed by them.
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 the full PAN.			X			Customer is responsible for ensuring that their configurations for using Citrix Cloud-based services appropriately masks the PANs within the Citrix Cloud-based Service.
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.			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for rendering PAN unreadable anywhere it is stored on systems managed by them.
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		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for proper implementation of disk encryption on systems that they manage.
3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for encryption implementation and key management on systems managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
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		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customers acting as service providers are responsible for key management responsibilities for maintaining PCI compliance of the systems managed by them.
3.5.2	Restrict access to cryptographic keys to the fewest number of custodians necessary.			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customers are responsible for key management responsibilities for maintaining PCI compliance of the systems managed by them.
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			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customers are responsible for key management responsibilities for maintaining PCI compliance of the systems managed by them.
3.5.4	Store cryptographic keys in the fewest possible locations			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customers are responsible for key management responsibilities for maintaining PCI compliance of the systems managed by them.
3.6.1	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: Generation of strong cryptographic keys			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customers are responsible for key management responsibilities for maintaining PCI compliance of the systems managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
3.6.2	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: Secure cryptographic key distribution			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customers are responsible for key management responsibilities for maintaining PCI compliance of the systems managed by them.
3.6.3	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: Secure cryptographic key storage			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customers are responsible for key management responsibilities for maintaining PCI compliance of the systems managed by them.
3.6.4	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: Cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines.			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customers are responsible for key management responsibilities for maintaining PCI compliance of the systems managed by them.
3.6.5	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: Retirement or replacement of keys as deemed necessary when the integrity of the key has been weakened, or keys are suspected of being compromised.			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customers are responsible for key management responsibilities for maintaining PCI compliance of the systems managed by them.
3.6.6	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customers are responsible for key management responsibilities for maintaining PCI compliance of the systems managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
3.6.7	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: Prevention of unauthorized substitution of cryptographic keys.			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customers are responsible for key management responsibilities for maintaining PCI compliance of the systems managed by them.
3.6.8	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customers are responsible for key management responsibilities for maintaining PCI compliance of the systems managed by them.
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	Citrix is responsible for documenting security policies and operational procedures for customer meta data in Citrix Cloud-based Services. These policies and procedures are disseminated to all associated parties.	Customer is responsible for documenting security policies and operational procedures for protecting stored cardholder data with customer managed encryption keys. These policies and procedures should be disseminated to all associated parties.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
Encrypt transmission of cardholder data across open, public networks							
4.1	Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) 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		N/A for the Citrix Cloud-based Services infrastructure. Customer data transmitted by the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for implementing strong cryptography and security protocols managed by them to safeguard card holder data in-transit.
4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data transmitted by the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for implementation of strong encryption for authentication and transmission of wireless networks transmitting cardholder data in their environment.
4.2	Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).			X		N/A for the Citrix Cloud-based Services infrastructure. Customer data transmitted by the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for never sending PANs using Citrix Cloud-based Services and systems managed by them.
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	Citrix is responsible for documenting security policies and operational procedures for encrypting in-transit customer data for the Citrix Cloud-based Services infrastructure. These policies and procedures are disseminated and known to all associated parties.	Customer is responsible for documenting security policies and operational procedures for encrypting in-transit cardholder data for systems they manage. These policies and procedures should be disseminated and known to all associated parties.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
Protect all systems against malware and regularly update anti-virus software or programs							
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).				X	Citrix is responsible for deploying anti-virus software on systems within the Citrix Cloud-based Services infrastructure.	Customer is responsible for deploying anti-virus software on systems managed by them.
5.1.1	Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.				X	Citrix is responsible for ensuring anti-virus software is capable of detecting, removing, and protecting against all known malware within Citrix Cloud-based Services infrastructure.	Customer is responsible for ensuring anti-virus software is capable of detecting, removing, and protecting against all known malware on systems managed by them.
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	Citrix is responsible for performing periodic evaluations to identify malware threats on systems not commonly affected by malware within Citrix Cloud-based Services infrastructure.	Customer is responsible for performing periodic evaluations to identify malware threats on systems not commonly affected by malware and managed by them.
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	Citrix is responsible for maintaining anti-virus software with regular updates and scan for the Citrix Cloud-based Services infrastructure.	Customer is responsible for maintaining anti-virus software with regular updates and scans for systems managed by them.
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	Citrix is responsible for ensuring anti-virus software runs actively and cannot be disabled except where authorized and for a limited time only within Citrix Cloud-based Services infrastructure.	Customer is responsible for ensuring anti-virus software runs actively and cannot be disabled except where authorized and only for a limited time on systems managed by them.
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	Citrix is responsible for the security policies and procedures related to malware protection internally for the Citrix Cloud-based Services infrastructure. These policies and procedures are disseminated to all associated internal parties.	Customer is responsible for documenting security policies and operational procedures for protecting systems managed by them against malware. These policies and procedures should be disseminated to all associated parties.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
Develop and maintain secure systems and applications							
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	Citrix is responsible for identifying security vulnerabilities using information sourced from a reputable third-party within Citrix Cloud-based Services infrastructure. This information is used for assigning risk rankings to new security vulnerabilities.	Customer is responsible for identifying security vulnerabilities using information sourced from a reputable third-party for systems managed by them. This information is used for assigning risk rankings to new security vulnerabilities.
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	Citrix is responsible for installing applicable vendor-supplied security patches in a timely manner for systems within the Citrix Cloud-based Services infrastructure.	The customer is responsible for installing applicable vendor-supplied security patches in a timely manner for customer-deployed resources on systems managed by them.
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		X			Citrix is responsible for securely developing applications following our SDLC standards for Citrix Cloud-based Services.	
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	Citrix is responsible for removing test accounts, user IDs and passwords within Citrix Cloud-based Services infrastructure before being released to customers.	Customers that have subscriptions for testing or development are responsible for removing test accounts, user IDs and passwords before it becomes an active production environment.
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			Citrix is responsible for code review of Citrix Cloud-based Services code before release to production on Citrix Cloud-based Services infrastructure.	

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
6.4.1	Follow change control processes and procedures for all changes to system components. The processes must include the following: Separate development/test environments from production environments, and enforce the separation with access controls.				X	Citrix is responsible for implementing change control processes and procedures including separation of development/test environments from production environments by enforceable access controls for Citrix Cloud-based Services infrastructure.	Customers that have subscriptions for testing or development are responsible for enforcing separation from production with access controls.
6.4.2	Follow change control processes and procedures for all changes to system components. The processes must include the following: Separation of duties between development/test and production environments.				X	Citrix is responsible for implementing change control and the adoption of the processes and procedures for Citrix Cloud-based Services infrastructure. This includes the separation of duties between development/test and production environments.	Customers that have subscriptions for testing or development are responsible for enforcing separation of duties from production.
6.4.3	Follow change control processes and procedures for all changes to system components. The processes must include the following: Production data (live PANs) are not used for testing or development.				X	Citrix Cloud-based Services functionality tests do not use live PANs for testing or development.	Customers that have subscription for testing or development are responsible for not using live PANs with those environments.
6.4.4	Follow change control processes and procedures for all changes to system components. The processes must include the following: Removal of test data and accounts before production systems become active.				X	Citrix is responsible for implementing change control processes and procedures which includes the removal of test accounts and data before release to production on Citrix Cloud-based Services infrastructure.	Customers that have subscriptions for testing or development are responsible for removal of test data and accounts for those environments before release to production.
6.4.5.1	Change control procedures for the implementation of security patches and software modifications must include the following: Documentation of impact.				X	Citrix is responsible for implementing change control processes and procedures which includes documentation of change impact for changes to Citrix Cloud-based Services infrastructure.	Customer is responsible for implementing change control processes and procedures including documenting impact for customer administered changes.
6.4.5.2	Change control procedures for the implementation of security patches and software modifications must include the following: Documented change approval by authorized parties.				X	Citrix is responsible for implementing change control processes and procedures that include documented change approval for changes to Citrix Cloud-based Services infrastructure.	Customer is responsible for implementing change control processes and procedures including documented approval for customer administered changes.
6.4.5.3	Change control procedures for the implementation of security patches and software modifications must include the following: Functionality testing to verify that the change does not adversely impact the security of the system.				X	Citrix is responsible for implementing change control processes and procedures that include functionality testing to verify for no adverse impact to Citrix Cloud-based Services infrastructure.	Customer is responsible for implementing change control processes and procedures that include functionality testing to verify for no adverse impact for customer administered changes.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
6.4.5.4	Change control procedures for the implementation of security patches and software modifications must include the following: Back-out procedures.				X	Citrix is responsible for implementing change control processes and procedures that include documented back-out procedures for changes to Citrix Cloud-based Services infrastructure.	Customer is responsible for implementing change control processes and procedures that include documented back-out procedures for customer administered changes.
6.4.6	Follow change control processes and procedures for all changes to system components. The processes must include the following: 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	Citrix is responsible for implementing change control processes and procedures that include documented processes for significant changes to Citrix Cloud-based Services infrastructure.	Customer is responsible for implementing change control processes and procedures that include processes for significant changes for customer administered changes.
6.5.1	Address common coding vulnerabilities in software-development processes as follows: - Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. - Develop applications based on secure coding guidelines. Vulnerabilities include: Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.		X			Citrix is responsible for developing applications based on secure coding practices by addressing common coding vulnerabilities for Citrix Cloud-based Services on Citrix Cloud-based Services infrastructure.	
6.5.2	Address common coding vulnerabilities in software-development processes as follows: - Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. - Develop applications based on secure coding guidelines. Vulnerabilities include: Buffer overflows.		X			Citrix is responsible for developing applications based on secure coding practices by addressing common coding vulnerabilities for Citrix Cloud-based Services on Citrix Cloud-based Services infrastructure.	

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
6.5.3	Address common coding vulnerabilities in software-development processes as follows: - Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. - Develop applications based on secure coding guidelines. Vulnerabilities include: Insecure cryptographic storage.		X			Citrix is responsible for developing applications based on secure coding practices by addressing common coding vulnerabilities for Citrix Cloud-based Services on Citrix Cloud-based Services infrastructure.	
6.5.4	Address common coding vulnerabilities in software-development processes as follows: - Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. - Develop applications based on secure coding guidelines. Vulnerabilities include: Insecure communications.		X			Citrix is responsible for developing applications based on secure coding practices by addressing common coding vulnerabilities for Citrix Cloud-based Services on Citrix Cloud-based Services infrastructure.	
6.5.5	Address common coding vulnerabilities in software-development processes as follows: - Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. - Develop applications based on secure coding guidelines. Vulnerabilities include: Improper error handling.		X			Citrix is responsible for developing applications based on secure coding practices by addressing common coding vulnerabilities for Citrix Cloud-based Services on Citrix Cloud-based Services infrastructure.	
6.5.6	Address common coding vulnerabilities in software-development processes as follows: - Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. - Develop applications based on secure coding guidelines. Vulnerabilities include: All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).		X			Citrix is responsible for developing applications based on secure coding practices by addressing common coding vulnerabilities for Citrix Cloud-based Services on Citrix Cloud-based Services infrastructure.	

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
6.5.7	Address common coding vulnerabilities in software-development processes as follows: - Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. - Develop applications based on secure coding guidelines. Vulnerabilities include: Cross-site scripting (XSS).		X			Citrix is responsible for developing applications based on secure coding practices by addressing common coding vulnerabilities for Citrix Cloud-based Services on Citrix Cloud-based Services infrastructure.	
6.5.8	Address common coding vulnerabilities in software-development processes as follows: - Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. - Develop applications based on secure coding guidelines. Vulnerabilities include: 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			Citrix is responsible for developing applications based on secure coding practices by addressing common coding vulnerabilities for Citrix Cloud-based Services on Citrix Cloud-based Services infrastructure.	
6.5.9	Address common coding vulnerabilities in software-development processes as follows: - Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. - Develop applications based on secure coding guidelines. Vulnerabilities include: Cross-site request forgery (CSRF).		X			Citrix is responsible for developing applications based on secure coding practices by addressing common coding vulnerabilities for Citrix Cloud-based Services on Citrix Cloud-based Services infrastructure.	
6.5.10	Address common coding vulnerabilities in software-development processes as follows: - Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. - Develop applications based on secure coding guidelines. Vulnerabilities include: Broken authentication and session management.		X			Citrix is responsible for developing applications based on secure coding practices by addressing common coding vulnerabilities for Citrix Cloud-based Services on Citrix Cloud-based Services infrastructure.	

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
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			Citrix is responsible for developing applications based on secure coding practices by addressing common coding vulnerabilities for Citrix Cloud-based Services on Citrix Cloud-based Services infrastructure.	
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	Citrix is responsible for the security policies and procedures related to managing firewalls internally for the Citrix Cloud-based Services infrastructure. These policies and procedures are disseminated and known to all associated parties.	Customer is responsible for documenting security policies and operational procedures for protecting systems managed by them against malware. These policies and procedures should be disseminated and known to all associated parties.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
Restrict access to cardholder data by business need to know							
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.				X	Citrix is responsible for limiting access to system components and customer metadata to only those individuals whose job requires such access within Citrix Cloud-based Services infrastructure.	The customer is responsible for limiting access to system components and cardholder data to only those individuals whose job requires such access. Refer to Citrix Cloud Identity and Access Management product documentation for capabilities.
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	Citrix is responsible for defining access requirements for data resources and system components taking into consideration least privilege for Citrix Cloud-based Services infrastructure.	The customer administrator is responsible for defining access requirements to system components and cardholder data to only those individuals whose job requires such access. Refer to Citrix Cloud Identity and Access Management product documentation for capabilities.
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.				X	Citrix is responsible for restricting privileged access for development and support of the Citrix Cloud-based Services infrastructure.	The customer administrator is responsible for restricting privileged access to system components and cardholder data to only those individuals whose job requires such access. Refer to Citrix Cloud Identity and Access Management product documentation for capabilities.
7.1.3	Assign access based on individual personnel's job classification and function.				X	Citrix is responsible for assigning access based on job classification for the development and support of the Citrix Cloud-based Services infrastructure.	The customer administrator is responsible for assigning access within the Citrix Cloud-based Services based on job classification. Refer to Citrix Cloud Identity and Access Management product documentation for capabilities.
7.1.4	Require documented approval by authorized parties specifying required privileges.				X	Citrix is responsible for requiring documented approval by authorized parties specifying required privileges when granting access to the Citrix Cloud-based Services infrastructure.	The customer is responsible for requiring documented approval by authorized parties specifying required privileges when granting access to the Citrix Cloud-based Services.
7.2.1	Establish an access control system 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 must include the following: Coverage of all system components.				X	Citrix is responsible for establishing a secure access control system for development and support of Citrix Cloud-based Services infrastructure covering all system components.	The customer administrator is responsible for selecting the appropriate Identity Provider for Citrix Cloud-based Services and a secure access control system for system components managed by them. Refer to Citrix Cloud Identity and Access Management product documentation for capabilities.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
7.2.2	Establish an access control system 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 must include the following: Assignment of privileges to individuals based on job classification and function.				X	Citrix is responsible for establishing a secure access control system for development and support of Citrix Cloud-based Services infrastructure with the ability to assign privileges based on job function.	The customer administrator is responsible for selecting the appropriate Identity Provider for Citrix Cloud-based Services and a secure access control system for system components managed by them. Refer to Citrix Cloud Identity and Access Management product documentation for capabilities.
7.2.3	Establish an access control system 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 must include the following: Default "deny-all" setting.				X	Citrix is responsible for establishing a secure access control system for development and support of Citrix Cloud-based Services infrastructure with a default "deny-all" setting in the access control system.	The customer administrator is responsible for selecting the appropriate Identity Provider for Citrix Cloud-based Services and a secure access control system for system components managed by them. Refer to Citrix Cloud Identity and Access Management product documentation for capabilities.
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	Citrix is responsible for the security policies and operational procedures for restricting development and support access for the Citrix Cloud-based Services infrastructure. These policies and procedures are disseminated and known to all associated parties.	Customer must ensure that security policies and operational procedures for restricting access to their subscribed Citrix Cloud-based Services and systems managed by them. These policies and procedures should be disseminated and known to all associated parties.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
Identify and authenticate access to system components							
8.1.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: Assign all users a unique ID before allowing them to access system components or cardholder data.				X	Citrix is responsible for assigning unique account IDs to users before allowing them access to the system components in the Citrix Cloud-based Services infrastructure.	Customer is responsible for assigning all users a unique account ID before allowing them to access their subscribed Citrix Cloud-based Services and systems they administer.
8.1.2	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.				X	Citrix is responsible for controlling the addition, deletion, and modification of user ID accounts, credentials, and other identifier objects for Citrix Cloud-based Services infrastructure.	Customer is responsible for controlling addition, deletion, and modification of user ID accounts, credentials, and other identifier objects for subscribed Citrix Cloud-based Services and systems they administer.
8.1.3	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: Immediately revoke access for any terminated users.				X	Citrix is responsible for immediately revoking access by terminated personnel to the Citrix Cloud-based Services infrastructure.	Customer is responsible for immediately revoking access to the subscribed Citrix Cloud-based Services by terminated personnel for subscribed Citrix Cloud-based Services and systems they administer.
8.1.4	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: Remove/disable inactive user accounts within 90 days.				X	Citrix is responsible for removing/disabling within 90 days their inactive user ID accounts for Citrix Cloud-based Services infrastructure.	Customers are responsible for removing/disabling within 90 days their inactive user ID accounts for subscribed Citrix Cloud-based Services and systems they administer.
8.1.5	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: - Enabled only during the time period needed and disabled when not in use. - Monitored when in use.			X		N/A - Citrix does not grant vendors access to Citrix Cloud-based Services infrastructure.	Customer is responsible for managing vendor access to their subscribed Citrix Cloud-based Services and systems they administer.
8.1.6	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: Limit repeated access attempts by locking out the user ID after not more than six attempts.				X	Citrix is responsible for locking customer administrators using Citrix Identity accounts on Citrix Cloud-based services after not more than 6 attempts. Citrix is responsible for locking accounts after not more than 6 attempts for user ID accounts for Citrix Cloud-based Services infrastructure.	Customer is responsible for locking accounts after not more than 6 attempts by non-Citrix Identity administrator accounts and user ID accounts for subscribed Citrix Cloud-based Services and systems they administer.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
8.1.7	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.				X	Citrix is responsible for locking accounts for minimum of 30 min or until an administrator unlocks the account for user ID accounts of Citrix Cloud-based Services infrastructure.	Customer is responsible for locking user ID accounts for minimum of 30 min or until an administrator unlocks the user ID accounts for subscribed Citrix Cloud-based Services and systems they administer. Customer Administrators using Citrix Identity accounts on Citrix Cloud-based services are subject to a soft lock of 5 min after 5 bad attempts. No passwords are accepted during the 5 min soft lock and after 5 consecutive soft locks the customer administrator must call Citrix support. Customer is responsible for providing a compensating control for this requirement or enforce the use of Azure Active Directory for their access.
8.1.8	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: 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	Citrix is responsible for forcing reactivation if a session has been idle for more than 15 minutes for user ID accounts of Citrix Cloud-based Services infrastructure.	Customer is responsible for forcing reactivation if a session has been idle for more than 15 minutes by user ID accounts for Citrix Cloud-based services and systems administered by them.
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	Citrix is responsible for forcing user authentication to require more than a unique ID for Citrix Cloud-based Services infrastructure. Citrix is responsible for forcing user authentication via Citrix Identity by Customer Administrators to require more than a unique ID for access.	Customer is responsible for selecting the appropriate Identity Provider for Citrix Cloud-based Services and access control system that forces user authentication to require more than a unique ID for subscribed Citrix Cloud-based Services and systems administered by them.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.				X	Citrix is responsible for strong cryptography to make all customer administrators (with using Citrix Identity accounts) authentication information unreadable for Citrix Cloud-based Services. Citrix is responsible for strong cryptography to make all support and development authentication information unreadable for Citrix Cloud-based Services infrastructure.	Customer is responsible for strong cryptography of authentication credentials by selecting the appropriate Identity Provider for Citrix Cloud-based Services and access control system for system components managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
8.2.2	Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.				X	Citrix is responsible for verification of requestors identity for modification of authentication credentials used by customer administrators for Citrix Cloud-based Services. Citrix is also responsible for verification of requestors identity for modification of authentication credentials used by support and development for Citrix Cloud-based Services infrastructure.	Customer is responsible for verification of the identity of customer administrators and customer subscribers for password, token and key provisioning tasks for subscribed Citrix Cloud-based Services and systems they administer.
8.2.3	Passwords/phrases must meet the following: - Require a minimum length of at least seven characters. - Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.				X	Citrix is responsible for password length and complexity for customer administrator accounts using Citrix Identity for Citrix Cloud-based Services. Citrix is also responsible for password length and complexity for accounts held by support and development personnel user accounts for Citrix Cloud-based Services infrastructure.	Customer is responsible for password length and complexity by selecting the appropriate Identity Provider for Citrix Cloud-based Services and access control system for Citrix Cloud based systems and system components managed by them.
8.2.4	Change user passwords/passphrases at least once every 90 days.				X	Citrix is responsible for password duration for accounts held by support and development personnel for Citrix Cloud-based Services infrastructure.	Customer is responsible for managing password duration of accounts used by customer administrators and subscribers selecting the appropriate Identity Provider for subscribed Citrix Cloud-based Services and systems they administer.
8.2.5	Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.				X	Citrix is responsible for password history for customer administrator accounts using Citrix Identity for Citrix Cloud-based Services. Citrix is also responsible for password history for accounts held by support and development personnel for Citrix Cloud-based Services infrastructure.	Customer is responsible for password history of accounts used by customer administrators and subscribers by selecting the appropriate Identity Provider for Citrix Cloud-based services and systems administered by them.
8.2.6	Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.				X	Citrix is responsible for ensuring passwords have unique values for user accounts held by support and development personnel for Citrix Cloud-based Services infrastructure.	Customer is responsible for using unique values for accounts used by customer administrators and subscribers for subscribed Citrix Cloud-based Services and systems administered by them.
8.3	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.				X	Citrix is responsible for using multi-factor authentication for non-console administration with accounts held by support and development personnel for Citrix Cloud-based Services infrastructure.	Customer is responsible for using multi-factor authentication for accounts used by customer administrators accessing Citrix Cloud and the CDE systems that they administer.
8.3.1	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.				X	Citrix is responsible for using multi-factor authentication for non-console administration with accounts held by support and development personnel for Citrix Cloud-based Services infrastructure.	Customer is responsible for using multi-factor authentication for accounts used by customer administrators accessing Citrix Cloud and their CDE systems that they administer.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
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	Citrix is responsible for using multi-factor authentication for remote network access with accounts held by support and development personnel for Citrix Cloud-based Services infrastructure.	Customer is responsible for using multi-factor authentication for remote network access for systems administered by them.
8.4	Document and communicate authentication procedures and policies 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	Citrix is responsible for documenting and distributing security policies and procedures for authentication for support and development personnel for Citrix Cloud-based Services infrastructure.	The customer is responsible for documenting and distributing security policies and procedures for authentication to all associated parties managed by them.
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	Citrix is responsible for assigning unique authentication methods for user accounts held by support and development personnel for the Citrix Cloud-based Services infrastructure.	Customer is responsible for assigning unique authentication methods for user account on the systems they administer.
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		N/A - Citrix does not have remote access to customer premises.	Customers acting as service provider are responsible to ensure adherence to PCI DSS regarding remote access to customer premises.
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	Citrix is responsible for assigning unique authentication methods for user accounts held by support and development personnel for the Citrix Cloud-based Services infrastructure.	Customer is responsible for assigning unique authentication methods for user account on the systems they administer.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
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		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for restricting access to databases containing their cardholder data managed by them.
8.8	Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.				X	Citrix is responsible for the security policies and procedures related to identification and authentication internally for the Citrix Cloud-based Services infrastructure. Citrix provides information on Citrix Identity on citrix.com website. These policies and procedures are disseminated and known to all associated internal parties.	Customer is responsible for documenting security policies and operational procedures for protecting systems managed by them against malware. These policies and procedures should be disseminated and known to all associated parties.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
Restrict physical access to cardholder data							
9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.			X		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for the physical and environmental protection controls for systems managed by them.
9.1.1	Use video cameras and/or access control mechanisms 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.			X		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for the physical and environmental protection controls for systems managed by them.
9.1.2	Implement physical and/or logical controls to restrict access to publicly accessible network jacks.			X		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for the physical and environmental protection controls for systems managed by them.
9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.			X		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for the physical and environmental protection controls for systems managed by them.
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		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for the physical and environmental protection controls for systems managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
9.3	Control physical access for onsite personnel to the 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		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for the physical and environmental protection controls for systems managed by them.
9.4	Implement procedures to identify and authorize visitors.			X		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for the physical and environmental protection controls for systems managed by them.
9.4.1	Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.			X		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for the physical and environmental protection controls for systems managed by them.
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		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for the physical and environmental protection controls for systems managed by them.
9.4.3	Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.			X		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for the physical and environmental protection controls for systems managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
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		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for the physical and environmental protection controls for systems managed by them.
9.5	Physically secure all media.			X		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for physically securing all media with cardholder data for systems managed by them.
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		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for physically securing all media including backup media with cardholder data for systems managed by them.
9.6.1	Maintain strict control over the internal or external distribution of any kind of media, including the following: Classify media so the sensitivity of the data can be determined.			X		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for controlling and classifying all media with cardholder data for systems managed by them.
9.6.2	Maintain strict control over the internal or external distribution of any kind of media, including the following: Send the media by secured courier or other delivery method that can be accurately tracked.			X		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for controlling and sending all media with cardholder data for systems managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
9.6.3	Maintain strict control over the internal or external distribution of any kind of media, including the following: Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).			X		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for controlling and approving movement of all media with cardholder data for systems managed by them.
9.7	Maintain strict control over the storage and accessibility of media.			X		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for controlling the storage and accessibility of all media with cardholder data for systems managed by them.
9.7.1	Properly maintain inventory logs of all media and conduct media inventories at least annually.			X		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for maintaining inventory logs of all media with cardholder data for systems managed by them.
9.8	Destroy media when it is no longer needed for business or legal reasons as follows:			X		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for destroying media with cardholder data for systems managed by them.
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		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for securely destroying media with cardholder data for systems managed by them.
9.8.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.			X		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customers are responsible for securely destroying media with cardholder data for systems managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
9.9	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.			X		N/A - Citrix Cloud-based Services infrastructure does not have any systems in which devices that capture payment card data are to be connected.	Customers are responsible for protecting devices that capture payment card data by systems managed by them.
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		N/A - Citrix Cloud-based Services infrastructure does not have any systems in which devices that capture payment card data are to be connected.	Customers are responsible for protecting devices that capture payment card data by systems managed by them.
9.9.2	Periodically inspect device surfaces to detect tampering, or substitution.			X		N/A - Citrix Cloud-based Services infrastructure does not have any systems in which devices that capture payment card data are to be connected.	Customers are responsible for protecting devices that capture payment card data by systems managed by them.
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		N/A - Citrix Cloud-based Services infrastructure does not have any systems in which devices that capture payment card data are to be connected.	Customers are responsible for protecting devices that capture payment card data by systems managed by them.
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		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. All physical and environmental protection controls are implemented and managed by Citrix engaged third party service providers for Citrix Cloud-based infrastructure.	Customer is responsible for security policies and operational procedures restricting physical access to locations managed by them. These policies and procedures should be disseminated to all associated parties.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
Track and monitor all access to network resources and cardholder data							
10.1	Implement audit trails to link all access to system components to each individual user.				X	Citrix is responsible for auditing individual user access for support and development of Citrix Cloud-based Services infrastructure.	Customer is responsible for auditing access for their Citrix Cloud-based services accounts and for systems managed by them.
10.2.1	Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data.			X		N/A - Customer data within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. Citrix does have automation of audit trails to capture access to customer data configured within Citrix Cloud-based Services infrastructure.	Customer is responsible for the automation of audit trails to capture user access to all cardholder data managed by them.
10.2.2	Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges.				X	Citrix is responsible for the automation of audit trails to capture actions taken by users with administrative privilege access within Citrix Cloud-based Services infrastructure.	Customer is responsible for the automation of audit trails to capture actions taken by their users with administrative privilege access for their Citrix Cloud-based services accounts and for systems managed by them.
10.2.3	Implement automated audit trails for all system components to reconstruct the following events: Access to all audit trails.				X	Citrix is responsible for the automation of audit trails to capture access to all audit trails within Citrix Cloud-based Services infrastructure.	Customer is responsible for the automation of audit trails to capture access to all audit trails for their Citrix Cloud-based services accounts and for systems managed by them.
10.2.4	Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts.				X	Citrix is responsible for the automation of audit trails to capture invalid access attempts within Citrix Cloud-based Services infrastructure.	Customer is responsible for the automation of audit trails to capture access to all audit trails by their Citrix Cloud-based service accounts and for systems managed by them.
10.2.5	Implement automated audit trails for all system components to reconstruct the following events: 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	Citrix is responsible for the automation of audit trails to capture use of and changes to identification and authentication mechanisms within Citrix Cloud-based Services infrastructure.	Customer is responsible for the automation of audit trails to capture use of and changes to identification and authentication mechanisms by their Citrix Cloud-based service accounts and for systems managed by them.
10.2.6	Implement automated audit trails for all system components to reconstruct the following events: Initialization, stopping, or pausing of the audit logs.				X	Citrix is responsible for the automation of audit trails to capture starting, stopping and pausing of audit logs within Citrix Cloud-based Services infrastructure.	Customer is responsible for the automation of audit trails to capture starting, stopping and pausing of audit logs by their Citrix Cloud-based service accounts and for systems managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
10.2.7	Implement automated audit trails for all system components to reconstruct the following events: Creation and deletion of system-level objects.				X	Citrix is responsible for the automation of audit trails to capture invalid access attempts within Citrix Cloud-based Services infrastructure.	Customer is responsible for the automation of audit trails to capture access to all audit trails by their Citrix Cloud-based service accounts and for systems managed by them.
10.3.1	Record at least the following audit trail entries for all system components for each event: User identification.				X	Citrix is responsible for recording audit trail entries and capture user IDs for events for Citrix Cloud-based services infrastructure.	Customer is responsible for recording audit trail entries and capture user IDs for events on their subscribed Citrix Cloud-based Services and for systems managed by them.
10.3.2	Record at least the following audit trail entries for all system components for each event: Type of event.				X	Citrix is responsible for recording audit trail entries and capture type of event for events for Citrix Cloud- based services infrastructure.	Customer is responsible for recording audit trail entries and capture type of event for events on their subscribed Citrix Cloud-based Services and for systems managed by them.
10.3.3	Record at least the following audit trail entries for all system components for each event: Date and time.				X	Citrix is responsible for recording audit trail entries and capture data and time for events for Citrix Cloud-based Services infrastructure.	Customer is responsible for recording audit trail entries and capture data and time for events on their subscribed Citrix Cloud-based Services and for systems managed by them.
10.3.4	Record at least the following audit trail entries for all system components for each event: Success or failure indication.				X	Citrix is responsible for recording audit trail entries and capture success or failure for events for Citrix Cloud-based infrastructure.	Customer is responsible for recording audit trail entries and capture success or failure for events on their subscribed Citrix Cloud-based Services and for systems managed by them.
10.3.5	Record at least the following audit trail entries for all system components for each event: Origination of event.				X	Citrix is responsible for recording audit trail entries and capture origination of event for events for Citrix Cloud-based infrastructure.	Customer is responsible for recording audit trail entries and capture origination of event for events on their subscribed Citrix Cloud-based Services and for systems managed by them.
10.3.6	Record at least the following audit trail entries for all system components for each event: Identity or name of affected data, system component, or resource.				X	Citrix is responsible for recording audit trail entries and capture system name for events for Citrix Cloud-based Services infrastructure.	Customer is responsible for recording audit trail entries and capture system name for events on their subscribed Citrix Cloud-based Services and for systems managed by them.
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	Citrix is responsible for ensuring all time services are synchronized within the Citrix Cloud-based Services infrastructure.	Customer is responsible for ensuring all time services are synchronized for all systems managed by them.
10.4.1	Critical systems have the correct and consistent time.				X	Citrix is responsible for ensuring all systems have the correct and consistent time for Citrix Cloud-based Services infrastructure.	Customer is responsible for ensuring all systems have the correct and consistent time for systems managed by them.
10.4.2	Time data is protected.				X	Citrix is responsible for ensuring all systems have protected time data for Citrix Cloud-based Services infrastructure.	Customer is responsible for ensuring all systems have protected time data for systems managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
10.4.3	Time settings are received from industry-accepted time sources.				X	Citrix is responsible for ensuring all systems time settings are received from industry-accepted time sources for Citrix Cloud-based Services infrastructure.	Customer is responsible for ensuring all systems time settings are received from industry-accepted time sources for systems managed by them.
10.5	Secure audit trails so they cannot be altered.				X	Citrix is responsible for securing audit trails from alteration for Citrix Cloud-based Services infrastructure and for customer administrator enabled online audit trails Citrix Cloud-based services.	Customer is responsible for securing audit trails from alteration for downloaded Citrix Cloud-based Services logs and for systems managed by them.
10.5.1	Limit viewing of audit trails to those with a job-related need.				X	Citrix is responsible for limiting access to audit trails based on job function for Citrix Cloud-based Services infrastructure.	Customer is responsible for limiting access to audit trails based on job function on for their subscribed Citrix Cloud-based Services and for systems managed by them.
10.5.2	Protect audit trail files from unauthorized modifications.				X	Citrix is responsible for limiting access to audit trail files based on job function for Citrix Cloud-based Services infrastructure.	Customer is responsible for limiting access to audit trail files based on job function for their subscribed Citrix Cloud-based Services and for systems managed by them.
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.				X	Citrix is responsible for backing up audit trail files to a secure centralized log server for Citrix Cloud-based Services infrastructure.	Customer is responsible for backing up audit trail files to a secure centralized log server for their subscribed Citrix Cloud-based Services and for systems managed by them.
10.5.4	Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.				X	Citrix is responsible for writing logs for external-facing technologies to a secure centralized log server for Citrix Cloud-based Services infrastructure.	Customer is responsible for writing logs for external-facing technologies to a secure centralized log server for their subscribed Citrix Cloud-based Services and for systems managed by them.
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	Citrix is responsible for active monitoring of logs for Citrix Cloud-based Services infrastructure.	Customer is responsible for log file integrity according to PCI DSS for downloaded Citrix Cloud-based Services logs and systems managed by them.
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity.				X	Citrix is responsible for identifying anomalies or suspicious activity within logs for Citrix Cloud-based Services infrastructure.	Customer is responsible for daily review of logs to identify anomalies or suspicious activity according to PCI DSS within logs for subscribed Citrix Cloud-based Services and systems managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
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	Citrix is responsible for daily review of logs to identify anomalies or suspicious activity according to PCI DSS within logs for Citrix Cloud-based Services infrastructure.	Customer is responsible for daily review of logs to identify anomalies or suspicious activity according to PCI DSS within logs for subscribed Citrix Cloud-based Services and systems managed by them.
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	Citrix is responsible for daily review of logs to identify anomalies or suspicious activity according to PCI DSS within logs for Citrix Cloud-based Services infrastructure.	Customer is responsible for daily review of logs to identify anomalies or suspicious activity according to PCI DSS within logs for subscribed Citrix Cloud-based Services and systems managed by them.
10.6.3	Follow up exceptions and anomalies identified during the review process.				X	Citrix is responsible for follow-up of anomalies or suspicious activity within logs for Citrix Cloud-based Services infrastructure.	Customer is responsible for follow-up of identified anomalies or suspicious activity within logs for subscribed Citrix Cloud-based services and systems managed by them.
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	Citrix is responsible for retaining audit trail logs for at least one year for Citrix Cloud-based Services infrastructure. The most recent three months must be immediately available for analysis.	Customer is responsible for retaining audit trail logs for at least one year for subscribed Citrix Cloud-based Services and systems managed by them. The most recent three months must be immediately available for analysis.
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)				X	Citrix is responsible for the timely detection and reporting of failures to critical security control systems for Citrix Cloud-based Services infrastructure.	Customers that are service providers are responsible for the timely detection and reporting of failures to critical security control systems managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
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 of the security failure, cause(s) of failure and remediation required - Identifying and addressing any security issues that arose during the failure - Performing a risk assessment to determine whether further actions are required - Implementing controls to prevent cause of failure from reoccurring - Resuming monitoring of security controls				X	Citrix is responsible for responding to failures of critical security control systems for Citrix Cloud-based Services infrastructure.	Customers acting as service providers are responsible for responding to failures of critical security control systems managed by them.
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	Citrix is responsible for documenting security policies and operational procedures for monitoring access to network resources and cardholder data. These policies and procedures should be disseminated and known to all associated parties.	Customer is responsible for documenting security policies and operational procedures for monitoring access to network resources and card holder data for systems managed by them. These policies and procedures should be disseminated and known to all associated parties.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
Regularly test security systems and processes							
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. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.				X	Citrix is responsible for testing for the presence of wireless access points and unauthorized wireless access points are detected for the Citrix Cloud-based Services infrastructure environment.	Customer is responsible to implement a process to test for rogue access points on a quarterly basis for networks managed by them.
11.1.1	Maintain an inventory of authorized wireless access points including a documented business justification.				X	Citrix is responsible for maintaining an inventory of authorized wireless access points for Citrix Cloud-based Services infrastructure environment.	Customer is responsible to implement a process to maintain an inventory of authorized wireless access points for networks managed by them.
11.1.2	Implement incident response procedures in the event unauthorized wireless access points are detected.				X	Citrix is responsible for implementing an incident response process for unauthorized access points for the Citrix Cloud-based Services infrastructure.	Customer is responsible to implement an incident response for the presence of rogue access points for networks managed by them.
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	Citrix is responsible for internal and external network vulnerability scans at least quarterly and after any significant changes for Citrix Cloud-based Services infrastructure.	Customer is responsible for scanning of the environment managed by them and should only include customer IP addresses, not Citrix Cloud-based Services endpoints. Citrix Cloud-based Services endpoints are tested as part of Citrix compliance vulnerability scans.
11.2.1	Perform quarterly internal vulnerability scans and rescans as needed, until all “high-risk” vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.				X	Citrix is responsible for internal network vulnerability scans and rescans until all "high-risk" vulnerabilities for Citrix Cloud-based Services infrastructure are resolved.	Customer is responsible for scans and rescans for the environment managed by them until all "high-risk "vulnerabilities are resolved.
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	Citrix is responsible for quarterly external network vulnerability scans and rescans by ASV for Citrix Cloud-based Services infrastructure until passing scans are achieved.	Customer is responsible for quarterly external network vulnerability scans and rescans by ASV for environments managed by them until passing scans are achieved.
11.2.3	Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.				X	Citrix is responsible for performing vulnerabilities scans performed by qualified personnel on at least a quarterly basis for Citrix Cloud-based Services infrastructure.	Customer is responsible for performing vulnerabilities scans performed by qualified personnel on at least a quarterly basis for systems managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
11.3	Implement a methodology for penetration testing that includes all aspects covered in the PCI DSS v3.2.1 Requirment 11.3				X	Citrix is responsible for implementing a methodology for penetration tests for the Citrix Cloud-based Services infrastructure.	Customers are responsible for implementing a methodology for penetration testing for the environment managed by them.
11.3.1	Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification.				X	Citrix is responsible for performing external penetration test annually and after significant changes for the Citrix Cloud-based Services infrastructure.	Customers are responsible for performing external penetration tests annually and after significant changes for the environment managed by them.
11.3.2	Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification.				X	Citrix is responsible for performing internal penetration tests annually and after significant changes for the Citrix Cloud-based Services infrastructure.	Customers are responsible for performing internal penetration tests annually and after significant changes for the environment managed by them.
11.3.3	Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.				X	Citrix is responsible for performing penetration testing until all exploitable vulnerabilities for Citrix Cloud-based Services infrastructure are resolved.	Customer is responsible for performing penetration testing for the environment managed by them until all exploitable vulnerabilities are resolved.
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		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customer is responsible for performing penetration tests annually and after significant changes to verify segmentation controls tests in their environment managed by them.
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		N/A for the Citrix Cloud-based Services infrastructure. Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service.	Customers acting as service providers are responsible for performing penetration testing on segmentation controls for maintaining PCI compliance of their managed solution.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
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	Citrix is responsible for monitoring network traffic via logging and intrusion-detection systems (IDS) for Citrix Cloud-based Services infrastructure.	Customer is responsible for monitoring network traffic via logging and intrusion-detection systems (IDS) for systems managed by them.
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	Citrix is responsible for alerting personnel when an unauthorized modifications to critical objects is detected for Citrix Cloud-based Services infrastructure.	Customer is responsible for alerting personnel of unauthorized modifications to critical objects for systems managed by them.
11.5.1	Implement a process to respond to any alerts generated by the change-detection solution.				X	Citrix is responsible for responding to unauthorized modification to critical object alerts for Citrix Cloud-based Services infrastructure.	Customer is responsible for responding to unauthorized modification to critical object alerts for systems managed by them.
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	Citrix is responsible to ensure that security policies and operational procedures for security monitoring and testing are documented, distributed and known to all affected parties for Citrix Cloud-based Services infrastructure.	Customer is responsible to ensure that security policies and operational procedures for security monitoring and testing are documented, distributed and known to all affected parties for systems managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
Maintain a policy that addresses information security for all personnel							
12.1	Establish, publish, maintain, and disseminate a security policy.				X	Citrix is responsible for establishing, maintaining, and publishing security policies internally for Citrix Cloud-based Services infrastructure.	Customer is responsible for establishing, maintaining, and publishing security policies for systems managed by them.
12.1.1	Review the security policy at least annually and update the policy when the environment changes.				X	Citrix is responsible for reviewing security policies internally on an annual basis for Citrix Cloud-based Services infrastructure.	Customer is responsible for reviewing security policies internally on an annual basis for systems managed by them.
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.				X	Citrix is responsible to create and implement an internal risk-assessment process.	Customer is responsible to created and implement a risk-assessment process.
12.3.1	Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following: Explicit approval by authorized parties.				X	Citrix is responsible for developing internal policies ensuring proper usage of critical technologies within the Citrix Cloud-based Services infrastructure environment including authorization requirements.	Customer is responsible for developing policies ensuring proper usage of critical technologies within their cardholder data environment. Policies should include authorization requirements.
12.3.2	Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following: Authentication for use of the technology.				X	Citrix is responsible for developing internal policies ensuring proper usage of critical technologies within the Citrix Cloud-based Services infrastructure environment including authentication requirements.	Customer is responsible for developing policies ensuring proper usage of critical technologies within their cardholder data environment. Policies should include authentication requirements.
12.3.3	Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following: A list of all such devices and personnel with access.				X	Citrix is responsible for developing internal policies ensuring proper usage of critical technologies within the Citrix Cloud-based Services infrastructure environment including an inventory of devices and authorized personnel.	Customer is responsible for developing policies ensuring proper usage of critical technologies within their cardholder data environment. Policies should include an inventory of devices and authorized personnel.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
12.3.4	Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following: A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices).				X	Citrix is responsible for developing internal policies ensuring proper usage of critical technologies within the Citrix Cloud-based Services infrastructure environment including a method to determine ownership of technologies.	Customer is responsible for developing policies ensuring proper usage of critical technologies within their cardholder data environment. Policies should include a method to accurately determine ownership.
12.3.5	Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following: Acceptable uses of the technology.				X	Citrix is responsible for developing internal policies ensuring proper usage of critical technologies within the Citrix Cloud-based Services infrastructure environment including acceptable usage information.	Customer is responsible for developing policies ensuring proper usage of critical technologies within their cardholder data environment. Policies should include acceptable usage.
12.3.6	Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following: Acceptable network locations for the technologies.				X	Citrix is responsible for developing internal policies ensuring proper usage of critical technologies within the Citrix Cloud-based Services infrastructure environment including acceptable network locations.	Customer is responsible for developing policies ensuring proper usage of critical technologies within their cardholder data environment. Policies should include acceptable network locations.
12.3.7	Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following: List of company-approved products.				X	Citrix is responsible for developing internal policies ensuring proper usage of critical technologies within the Citrix Cloud-based Services infrastructure environment including list of company approved products.	Customer is responsible for developing policies ensuring proper usage of critical technologies within their cardholder data environment. Policies should list company-approved products.
12.3.8	Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following: Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.				X	Citrix is responsible for developing internal policies ensuring proper usage of critical technologies within the Citrix Cloud-based Services infrastructure environment including automatic session disconnection for remote access.	Customer is responsible for developing policies ensuring proper usage of critical technologies within their cardholder data environment. Policies should specify inactivity periods for automatic session closure.
12.3.9	Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following: Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.			X		N/A - Citrix does not have vendors that access the Citrix Cloud-based Services infrastructure.	Customer is responsible for developing policies ensuring proper usage of critical technologies within their cardholder data environment. Policies should include activation and immediate deactivation of remote-access for vendors.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
12.3.10	Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following: 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	Citrix is responsible for developing internal policies ensuring proper usage of critical technologies within the Citrix Cloud-based Services infrastructure environment including prohibiting copying, moving and storage of customer data outside of assigned locations.	Customer is responsible for developing policies ensuring proper usage of critical technologies within their cardholder data environment via remote-access technologies. Policies should prohibit the copying, moving, and storage of cardholder data outside the cardholder data environment.
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.				X	Citrix is responsible for developing internal policies defining information security responsibilities for all personnel for Citrix Cloud-based Services infrastructure.	Customer is responsible for ensuring their security policy and operating procedures define responsibilities for personnel.
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	Citrix responsible for acknowledging their responsibilities for maintaining PCI compliance of Citrix Cloud-based Services infrastructure.	Customers which are service providers are responsible for acknowledging their responsibilities for maintaining PCI compliance of their managed solution.
12.5.1	Assign to an individual or team the following information security management responsibilities: Establish, document, and distribute security policies and procedures.				X	Citrix is responsible for assigning security management responsibilities internally, including the establishment and dissemination of security policies and procedures for Citrix Cloud-based Services infrastructure.	Customer is responsible for assigning security management responsibilities, including the establishment and dissemination of security policies and procedures for their personnel.
12.5.2	Assign to an individual or team the following information security management responsibilities: Monitor and analyze security alerts and information, and distribute to appropriate personnel.				X	Citrix is responsible for assigning security management responsibilities internally, including monitoring, analysis and escalation of security alerts for Citrix Cloud-based Services infrastructure.	Customer is responsible for assigning security management responsibilities, including the monitoring of security alerts.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
12.5.3	Assign to an individual or team the following information security management responsibilities: Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.				X	Citrix is responsible for assigning security management responsibilities internally, including establishment and dissemination of incident response and escalation procedures for Citrix Cloud-based Services infrastructure.	Customer is responsible for assigning security management responsibilities, including the establishment and dissemination of incident response and escalation procedures.
12.5.4	Assign to an individual or team the following information security management responsibilities: Administer user accounts, including additions, deletions, and modifications.				X	Citrix is responsible for assigning security management responsibilities internally, including account administration for Citrix Cloud-based Services infrastructure.	Customer is responsible for customer user accounts utilizing the Citrix Cloud-based Services and systems managed by them.
12.5.5	Assign to an individual or team the following information security management responsibilities: Monitor and control all access to data.				X	Citrix is responsible for assigning security management responsibilities internally, including monitoring and controlling all access for Citrix Cloud-based Services infrastructure.	Customer is responsible for monitor and control of all access to data
12.6	Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.			X		N/A - Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. Citrix has an internal security awareness program addressing sensitive data for Citrix Cloud-based Services infrastructure personnel.	Customer is responsible for implementing a formal security awareness program for their personnel.
12.6.1	Educate personnel upon hire and at least annually.			X		N/A - Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. Citrix provides security awareness training for personnel upon hire and at least annually for Citrix Cloud-based Services infrastructure personnel.	Customer is responsible for delivery of a formal security awareness program upon hire and at least annually for their personnel.
12.6.2	Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.			X		N/A - Customer data stored within the Citrix Cloud-based Services infrastructure is limited to metadata for the operation of the service. Citrix requests personnel at least annually to acknowledge they understand the security policy and procedures for Citrix Cloud-based Services infrastructure personnel.	Customer is responsible for implementing a formal security awareness program. Their personnel should acknowledge current security policies and procedures.
12.7	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources.				X	Citrix is responsible for performing personnel screening prior to hire or personnel for Citrix Cloud-based Services infrastructure.	Customer is responsible for performing personnel screening prior to hiring of personnel.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
12.8.1	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: Maintain a list of service providers including a description of the service provided.				X	Citrix is responsible for policies and procedures to manage service providers with whom customer data is shared including maintaining a list of service providers and their services for Citrix Cloud systems.	Customer is responsible for policies and procedures to manage service providers with whom cardholder data is shared including the maintenance of a list of service providers and their provided services for their CDE.
12.8.2	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: 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	Citrix is responsible for policies and procedures to manage service providers with whom customer data is shared including maintaining written agreements acknowledging service provider responsibilities for Citrix Cloud systems.	Customer is responsible for policies and procedures to manage service providers with whom cardholder data is shared including maintaining written agreements acknowledging service provider responsibilities for systems managed by them.
12.8.3	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: Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.				X	Citrix is responsible for policies and procedures to manage service providers with whom customer data is shared including a process for engaging service providers for Citrix Cloud-based Services infrastructure.	Customer is responsible for policies and procedures to manage service providers with whom cardholder data is shared including a process for engaging service providers for systems managed by them.
12.8.4	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: Maintain a program to monitor service providers' PCI DSS compliance status at least annually.				X	Citrix is responsible for policies and procedures to manage service providers with whom customer data is shared including maintenance of a program to monitor service providers' PCI DSS compliance status at least annually.	Customer is responsible for policies and procedures to manage service providers with whom cardholder data is shared including maintenance of a program to monitor service providers' PCI DSS compliance status, at least annually for their CDE.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
12.8.5	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: Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.				X	Citrix is responsible for policies and procedures to manage service providers with whom customer data is shared including identification of PCI DSS responsibilities of their service providers.	Customer is responsible for policies and procedures to manage service providers with whom cardholder data is shared including identification of PCI DSS responsibilities of their service providers for their CDE.
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	Citrix is responsible for acknowledging their responsibilities for maintaining PCI compliance of the Citrix Cloud-based Services infrastructure.	Customers acting as service providers are responsible for acknowledging their responsibilities for maintaining PCI compliance of their managed solution.
12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach.				X	Citrix is responsible for implementing an incident response plan for Citrix Cloud-based Services infrastructure.	Customer is responsible for implementing an incident response plan for systems managed by them.
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	Citrix is responsible for creating an incident response plan to be implemented in the event of a Citrix Cloud-based Services infrastructure breach.	Customer is responsible for implementing an incident response plan to be implemented in the event of a breach of the systems and environment managed by them.
12.10.2	Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually.				X	Citrix is responsible for annually testing their incident response plan for a Citrix Cloud-based Services infrastructure breach.	Customer is responsible for annually testing their incident response plan for systems and environment managed by them.

Requirement Number	PCI DSS Requirement Description	N/A	Citrix	Customer	Joint	Citrix Responsibility Description	Customer Responsibility Description
12.10.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.				X	Citrix is responsible for designating personnel to be available on a 24/7 basis to respond to alerts for Citrix Cloud-based Services infrastructure.	Customer is responsible for designating personnel to be available on a 24/7 basis to respond to alerts for systems managed by them.
12.10.4	Provide appropriate training to staff with security breach response responsibilities.				X	Citrix is responsible for providing security breach response training for Citrix Cloud-based Services resources.	Customer is responsible for providing security breach response training for their resources.
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	Citrix is responsible for monitoring and responding to alerts from security monitoring systems for Citrix Cloud-based Services infrastructure.	Customer is responsible for monitoring and responding to alerts from security monitoring systems for systems managed by them.
12.10.6	Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.				X	Citrix is responsible for reviewing and modified appropriately their incident response plan, taking into account lessons learned and industry developments.	Customer is responsible for reviewing and modified appropriately their incident response plan, taking into account lessons learned and industry developments for their environment. Reporting of a breach to the payment brands is the responsibility of the customer.
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				X	Citrix is responsible for documenting their reviews of processes for confirming PCI compliance control performance for Citrix Cloud-based Services infrastructure.	Customers acting as service providers are responsible for documenting their reviews of processes for confirming PCI compliance control performance of their managed solution.
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				X	Citrix is responsible for documenting the quarterly review process and requiring PCI DSS compliance personnel to sign-off on the results for Citrix Cloud-based Services infrastructure.	Customers acting as service providers are responsible for documenting the quarterly review process and requiring PCI DSS compliance personnel to sign-off on the results.