DRAFT – Internal Skytap use only

PCI DSS 3.2 Responsibility Summary

Skytap Cloud

December 2018

TABLE OF CONTENTS

[TABLE OF CONTENTS 2](#_Toc526513322)

[1. Executive Summary 3](#_Toc526513323)

[2. Business Description 3](#_Toc526513324)

[3. Compliance Scope 3](#_Toc526513325)

[3.1. Management Environment 3](#_Toc526513326)

[3.2. In-Scope Systems 3](#_Toc526513327)

[3.2.1. Service 1 Description 4](#_Toc526513328)

[3.2.2. Service 2 Description 4](#_Toc526513329)

[3.2.3. Other Services (not in-scope) Description 4](#_Toc526513330)

[4. Customer Considerations 4](#_Toc526513331)

[5. Responsibility for PCI DSS Requirements 4](#_Toc526513332)

[5.1. PCI DSS 3.2 Shared Responsibility Matrix 4](#_Toc526513333)

[5.2. PCI DSS 3.2 Detailed Customer Responsibility Matrix 7](#_Toc526513334)

# Executive Summary

This Responsibility Summary is based on Skytap’s PCI DSS 3.2 Service Provider Attestation of Compliance (AOC) dated 12/15/2018.

# Business Description

Skytap provides cloud infrastructure services that enable customers to build enterprise IT applications. Customers may build applications on top of Skytap cloud infrastructure that store, process, or transmit cardholder data. Skytap does not directly store, transmit, or process cardholder data in providing its cloud infrastructure services. Skytap has no access to customer data except when explicitly provided access by the customer to assist with troubleshooting issues.

# Compliance Scope

Skytap Cloud’s PCI DSS Service Provider Attestation of Compliance (AOC) applies to the entire Skytap Cloud Platform, from the Skytap Cloud Management Console to all underlying people, processes and technology supporting the hosting infrastructure. An overview of the Skytap Cloud platform is maintained here: <https://www.skytap.com/product/how-skytap-is-built/>

# Customer Considerations

Extensive documentation and recommendations for customer application architecture and operations are included on Skytap Help site.

* <https://help.skytap.com>

# 

# Responsibility for PCI DSS Requirements

When selecting a Cloud Service Provider (CSP) for hosting regulated workloads, it is important to understand each entity’s role in maintaining compliance, often distinguished as compliance (and security reasonability) “of the cloud” vs. “in the cloud”. Security of the cloud is the responsibility of Skytap Cloud, for securing the platform itself (the Cloud Hosting Provider Service defined in the Scope section above). Security “in the cloud” is the responsibility of Customers to secure the workloads they deploy on the secure Skytap Cloud platform. Responsibility is said to be shared between Skytap Cloud and Customers when there is an implementation dependency for each entity to fully meet a give PCI DSS requirement on behalf of the customer. It is through the PCI DSS Service Provider Attestation of Compliance that Skytap Cloud demonstrates they have meet their responsibilities for the security platform itself (*“of the cloud”*). This document explains those responsibilities, as well as provides guidance on the responsibilities of Customers within their Skytap Cloud environments (*“in the cloud”*).

## PCI DSS 3.2 Shared Responsibility Matrix

The table below summarizes the responsibilities complying with the top-level PCI DSS requirements for both Skytap (*“of the cloud”*) and Customers’ (*“in the cloud”*) Skytap cloud environments.

| Requirement and Testing Procedure | Compliance Status | Skytap Responsibility | Customer Responsibility |
| --- | --- | --- | --- |
| **Requirement 1:** Install and maintain a firewall configuration to protect cardholder data. |  | Skytap is responsible for maintaining back-end isolation for customer environments and from the Skytap Management Network, including guest operating system, hypervisor and firewall and network configurations. | Skytap customers are responsible for all network configurations within their Skytap Cloud environments. |
| **Requirement 2:** Do not use Supplier- supplied defaults for system passwords and other security parameters. |  | Skytap is responsible for implementing security standards for the underlying systems and networks hosting the Skytap Cloud platform on behalf of the customer. | Skytap customers are responsible for implementing security standards for the systems and networks in their Skytap Cloud environments. |
| **Requirement 3:** Protect stored cardholder data. |  | Skytap is not responsible for any stored CHD in customer environments. | Skytap customers are responsible for implementing encryption on any CHD stored in their Skytap Cloud environments. |
| **Requirement 4:** Encrypt transmission of cardholder data across open, public networks. |  | Skytap is responsible for implementing transit encryption on all sensitive data within the networks hosting the Skytap Cloud platform. | Skytap customers are responsible for implementing encryption on any network traffic within or external from their Skytap Cloud environments. |
| **Requirement 5:** Use and regularly update anti-virus software or programs. |  | Skytap is responsible for implementing antivirus on all appropriate systems hosting the Skytap Cloud platform. | Skytap customers are responsible for implementing antivirus on any appropriate systems within their Skytap Cloud environments. |
| **Requirement 6:** Develop and maintain secure systems and applications |  | Skytap is responsible for implementing patch and vulnerability management for all systems hosting the Skytap Cloud platform.  Skytap is responsible for implementing change control and secure software development for all systems and software hosting the Skytap Cloud platform. | Skytap customers are responsible for implementing patch and vulnerability management on any systems within their Skytap Cloud environments.  Skytap customers are responsible for implementing change control and secure software development for all systems and software within their Skytap Cloud environments. |
| **Requirement 7:** Restrict access to cardholder data by business need-to- know. |  | Skytap is responsible for implementing access control on all systems and applications hosting the Skytap Cloud platform. | Skytap customers are responsible for implementing access control on any systems and applications within their Skytap Cloud environments. |
| **Requirement 8:** Assign a unique ID to each person with computer access. |  | Skytap is responsible for implementing identity management on all systems and applications hosting the Skytap Cloud platform. | Skytap customers are responsible for implementing identity management on any systems and applications within their Skytap Cloud environments. |
| **Requirement 9:** Restrict physical access to cardholder data. |  | Skytap is responsible for the physical security and media handling controls for all components hosting the Skytap Cloud platform. | Skytap customers are responsible for the media handling controls for any media external to their Skytap Cloud environments. |
| **Requirement 10:** Track and monitor all access to network resources and cardholder data. |  | Skytap is responsible for the logging and monitoring of all components hosting the Skytap Cloud platform. | Skytap customers are responsible for logging and monitoring of any systems and applications within their Skytap Cloud environments. |
| **Requirement 11:** Regularly test security systems and processes. |  | Skytap is responsible for implementing all required security testing and monitoring of the components hosting the Skytap Cloud platform, including rogue wireless access point detection, vulnerability and penetration testing, intrusion detection and file integrity monitoring | Skytap customers are responsible for vulnerability and penetration testing, intrusion detection and file integrity monitoring within their Skytap Cloud environments.  Customers must follow coordinate with Skytap processes for scanning and pen testing: https://help.skytap.com/Security\_Best\_Practices.html |
| **Requirement 12:** Maintain a policy that addresses information security for employees and contractors. |  | Skytap is responsible for implementing security governance of all components hosting the Skytap Cloud Platform, including security policies and procedures, risk management, security awareness, human resources, vendor management and incident response. | Skytap customers are responsible for all security governance of their Skytap Cloud environments, including security policies and procedures, risk management, security awareness, human resources, vendor management and incident response.   Skytap customers should include Skytap as a Shared Hosting Provider for Req. 12.8. |
| **Appendix A1:** Shared hosting providers must protect the cardholder data environment. |  | Skytap is responsible for implementing controls to ensure that Skytap customer instances and data are protected from other Skytap Cloud customer environment and the Skytap Management Environment. | Skytap customers may also be considered a Shared Hosting Provider, if they run applications or store data for their customers in their Skytap Cloud environments. In this case, customers are responsible for protecting their customers’ data within their Skytap Cloud environments. |
| **Appendix A2:** Additional PCI DSS Requirements for Entities Using SSL/Early TLS |  | Skytap is responsible for implementing TLS 1.1 or greater within the Skytap Management Environment, and for customer web management interfaces to Skytap Cloud. | Skytap customers are responsible for ensuring only secure versions of TLS are used within their Skytap Cloud environments. |

## PCI DSS 3.2 Detailed Customer Responsibility Matrix

The table below details the responsibilities for meeting each of the PCI DSS requirements for a customer’s environment. The requirements designated as “Skytap” or “Shared” indicate that the Customer is dependent on Skytap (either partially or fully) to implement the control on their behalf, as explained in the comments field, along with all customer responsibilities.

| Requirement and Testing Procedure | Skytap | Customer | Shared | Comments |
| --- | --- | --- | --- | --- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1.1** Establish and implement firewall and router configuration standards that include the following: |  |  |  |  |
| **1.1** Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows: |  |  |  |  |
| **1.1.1** A formal process for approving and testing all network connections and changes to the firewall and router configurations. |  |  |  |  |
| **1.1.1.a** Examine documented procedures to verify there is a formal process for testing and approval of all:   •  Network connections, and  •  Changes to firewall and router configurations. |  |  | X | Skytap maintains routers and firewalls used to deliver the Skytap Cloud platform.  Customers are responsible for configuration of network connections to customer managed VMs. Customers are responsible for testing and approving their network connectivity and configuration for storing cardholder data in Skytap Cloud services. |
| **1.1.1.b** For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested. |  |  | X |
| **1.1.1.c** Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested. |  |  | X |
| **1.1.2** Current diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks. |  |  |  |  |
| **1.1.2.a** Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to the cardholder data environment, including any wireless networks. |  | X |  | Customers are responsible for maintaining network diagrams for their Cardholder Data Environment (CDE). |
| **1.1.2.b** Interview responsible personnel to verify that the diagram is kept current. |  | X |  |
| **1.1.3** Current diagram that shows all cardholder data flows across systems and networks. |  |  |  |  |
| **1.1.3.a** Examine data flow diagram and interview personnel to verify the diagram:   • Shows all cardholder data flows across systems and networks.   •  Is kept current and updated as needed upon changes to the environment. |  | X |  | Customers are responsible for maintaining data flow diagrams for their Cardholder Data Environment (CDE). |
| **1.1.4** Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone. |  |  |  |  |
| **1.1.4.a** Examine thefirewall configuration standards and verify that they include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. |  |  | X | Skytap maintains routers and firewalls used to deliver the Skytap Cloud platform.  Customers are responsible for implementing perimeter firewalls on customer managed VMs. Customers are responsible for maintaining firewall and router configuration standards for customer managed firewalls along with developing appropriate firewall rules necessary to implement appropriate DMZ and internal networks.   * <https://help.skytap.com/Ips.html> * <https://help.skytap.com/IP_Addresses_and_Port_Ranges.html> |
| **1.1.4.b** Verify that the current network diagram is consistent with the firewall configuration standards. |  |  | X |
| **1.1.4.c** Observe network configurations to verify that a firewall is in place at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone, per the documented configuration standards and network diagrams. |  |  | X |
| **1.1.5** Description of groups, roles, and responsibilities for management of network components. |  |  |  |  |
| **1.1.5.a** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components. |  |  | X | Skytap maintains routers and firewalls used to deliver the Skytap Cloud platform.  Customers are responsible for maintaining firewall and router configuration standards for firewalls and routers running on customer managed VMs along with other network services used to filter traffic into the CDE including access controls for customer managed VMs and customer VPN configurations. Configuration standards should include appropriate descriptions of groups, roles, and responsibilities for managing customer managed routers and firewalls. |
| **1.1.5.b** Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented. |  |  | X |
| **1.1.6** Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. |  |  |  |  |
| **1.1.6.a** Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification and approval for each. |  |  | X | Skytap maintains routers and firewalls used to deliver the Skytap Cloud platform.  Customers are responsible for documenting ports, protocols, and services used by customer managed VMs; documenting business justifications and approvals; and identifying insecure services and implementing appropriate controls and security features to limit the risk of the protocols from being used. |
| **1.1.6.b** Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service. |  |  | X |
| **1.1.6.c** Examine firewall and router configurations to verify that the documented security features are implemented for each insecure service, protocol, and port. |  |  | X |
| **1.1.7** Requirement to review firewall and router rule sets at least every six months. |  |  |  |  |
| **1.1.7.a** Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months. |  |  | X | Skytap maintains routers and firewalls used to deliver the Skytap Cloud platform.  Customers are responsible for performing reviews of firewalls and router configurations for customer managed VMs. This includes but may not be limited to firewalls and routers running on customer managed VMs, access controls for customer managed VMs, and VPN configurations. |
| **1.1.7.b** Examine documentation relating to rule set reviews and interview responsible personnel to verify that the rule sets are reviewed at least every six months. |  |  | X |
| **1.2** Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.  Note: An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. |  |  |  |  |
| **1.2** Examine firewall and router configurations and perform the following to verify that connections are restricted between untrusted networks and system components in the cardholder data environment: |  |  |  |  |
| **1.2.1** Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic. |  |  |  |  |
| **1.2.1.a** Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cardholder data environment. |  |  | X | Skytap maintains routers and firewalls used to deliver the Skytap Cloud platform.  Customers are responsible for installing and configurating firewalls on customer managed VMs and developing appropriate firewall rules to protect customer cardholder data, including verifying inbound and outbound traffic for their cardholder data environment and configuring firewalls and routers to deny any traffic that is not explicitly required for customer service to function.   * <https://help.skytap.com/Ips.html> * <https://help.skytap.com/IP_Addresses_and_Port_Ranges.html> * <https://help.skytap.com/Routing_Between_Networks.html> * <https://help.skytap.com/Networking_Between_Environments.html> |
| **1.2.1.b** Examine firewall and router configurations to verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment. |  |  | X |
| **1.2.1.c** Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit “deny all” or an implicit deny after allow statement. |  |  | X |
| **1.2.2** Secure and synchronize router configuration files. |  |  |  |  |
| **1.2.2.a** Examine router configuration files to verify they are secured from unauthorized access. |  |  | X | Skytap maintains routers and firewalls used to deliver the Skytap Cloud platform.  Customers are responsible for configuration of routers running on customer managed VMs. |
| **1.2.2.b** Examine router configurations to verify they are synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted). |  |  | X |
| **1.2.3** Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment. |  |  |  |  |
| **1.2.3.a** Examine firewall and router configurations to verify that there are perimeter firewalls installed between all wireless networks and the cardholder data environment. |  |  | X | Skytap maintains perimeter firewalls used to deliver the Skytap Cloud platform and controls traffic between wireless networks and systems in Skytap Cloud data centers.  Customers that use wireless networks are responsible for isolating their cardholder data environment from those wireless networks. |
| **1.2.3.b** Verify that the firewalls deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment. |  |  | X |
| **1.3** Prohibit direct public access between the Internet and any system component in the cardholder data environment. |  |  |  |  |
| **1.3** Examine firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—and perform the following to determine that there is no direct access between the Internet and system components in the internal cardholder network segment: |  |  |  |  |
| **1.3.1** Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. |  |  |  |  |
| **1.3.1** Examine firewall and router configurations to verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. |  |  | X | Skytap maintains routers and firewalls used to deliver the Skytap Cloud platform.  Customers are responsible for implementing perimeter firewalls and configuring security groups and ACLs through the Skytap Cloud API and other user interfaces for their in-scope services.  Customers are responsible for developing appropriate firewall rules or using additional firewall technologies to develop appropriate DMZ and internal networks.   * <https://help.skytap.com/IP_Addresses_and_Port_Ranges.html> * <https://help.skytap.com/Routing_Between_Networks.html> * <https://help.skytap.com/Networking_Between_Environments.html> |
| **1.3.2** Limit inbound Internet traffic to IP addresses within the DMZ. |  |  |  |  |
| **1.3.2** Examine firewall and router configurations to verify that inbound Internet traffic is limited to IP addresses within the DMZ. |  |  | X | Skytap maintains routers and firewalls used to deliver the Skytap Cloud platform.  Customers are responsible for maintaining firewall and router configuration standards for firewalls and routers running on customer managed VMs along with other network services used to filter traffic into the CDE including access controls for customer managed VMs and customer VPN configurations. Customers are responsible for implementing appropriate DMZ and internal networks in customer environment.   * <https://help.skytap.com/IP_Addresses_and_Port_Ranges.html> * <https://help.skytap.com/Routing_Between_Networks.html> * <https://help.skytap.com/Networking_Between_Environments.html> |
| **1.3.3** Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.   (For example, block traffic originating from the Internet with an internal source address) |  |  |  |  |
| **1.3.3** Examine firewall and router configurations to verify that anti-spoofing measures are implemented, for example internal addresses cannot pass from the Internet into the DMZ**.** |  |  | X | Skytap maintains routers and firewalls used to deliver the Skytap Cloud platform.  Customers are responsible for maintaining firewall and router configuration standards for firewalls and routers running on customer managed VMs along with other network services used to filter traffic into the CDE including access controls for customer managed VMs and customer VPN configurations. Customers are responsible for implementing appropriate DMZ and internal networks in customer environment.   * <https://help.skytap.com/IP_Addresses_and_Port_Ranges.html> * <https://help.skytap.com/Routing_Between_Networks.html> * <https://help.skytap.com/Networking_Between_Environments.html> |
| **1.3.4** Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. |  |  |  |  |
| **1.3.4** Examine firewall and router configurations to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized. |  |  | X | Skytap maintains routers and firewalls used to deliver the Skytap Cloud platform.  Customers are responsible for maintaining firewall and router configuration standards for firewalls and routers running on customer managed VMs along with other network services used to filter traffic into the CDE including access controls for customer managed VMs and customer VPN configurations.   * <https://help.skytap.com/IP_Addresses_and_Port_Ranges.html> * <https://help.skytap.com/Routing_Between_Networks.html> * <https://help.skytap.com/Networking_Between_Environments.html> |
| **1.3.5** Permit only “established” connections into the network. |  |  |  |  |
| **1.3.5** Examine firewall and router configurations to verify that the firewall permits only established connections into internal network, and denies any inbound connections not associated with a previously established session. |  |  | X | Skytap maintains routers and firewalls used to deliver the Skytap Cloud platform.  Customers are responsible for maintaining firewall and router configuration standards for firewalls and routers running on customer managed VMs along with other network services used to filter traffic into the CDE including access controls for customer managed VMs and customer VPN configurations. Customers are responsible for ensuring the use of stateful inspection firewalls if any host- based or other firewalls are implemented in the VMs, and Management Console instances.   * <https://help.skytap.com/IP_Addresses_and_Port_Ranges.html> * <https://help.skytap.com/Routing_Between_Networks.html> * <https://help.skytap.com/Networking_Between_Environments.html> |
| **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. |  |  |  |  |
| **1.3.6** Examine firewall and router configurations to verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks. |  |  | X | Skytap maintains routers and firewalls used to deliver the Skytap Cloud platform.  Customers are responsible for maintaining firewall and router configuration standards for firewalls and routers running on customer managed VMs along with other network services used to filter traffic into the CDE including access controls for customer managed VMs and customer VPN configurations.   * <https://help.skytap.com/IP_Addresses_and_Port_Ranges.html> * <https://help.skytap.com/Routing_Between_Networks.html> * <https://help.skytap.com/Networking_Between_Environments.html> |
| **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. |  |  |  |  |
| **1.3.7.a** Examine firewall and router configurations to verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet. |  |  | X | Skytap maintains routers and firewalls used to deliver the Skytap Cloud platform. Skytap routers and firewalls are configured to avoid disclosing private IP space to the Internet  Network MAC addresses are dynamically assigned to Skytap customer instances by the Skytap network infrastructure. IP addresses are either dynamically assigned by the Skytap network infrastructure or statically assigned by a Skytap customer administrator through authenticated API requests. The Skytap network only allows customer VMs to send traffic from IP and MAC addresses specifically assigned to them, or the traffic will be dropped.  Customers are responsible for maintaining firewall and router configuration standards for firewalls and routers running on customer managed VMs along with other network services used to filter traffic into the CDE including access controls for customer managed VMs and customer VPN configurations.  Customers are responsible for developing appropriate configuration on customer managed VMs to prevent the disclosure of IP Addresses and routing information.   * <https://help.skytap.com/IP_Addresses_and_Port_Ranges.html> * <https://help.skytap.com/Routing_Between_Networks.html> * <https://help.skytap.com/Networking_Between_Environments.html> |
| **1.3.7.b** Interview personnel and examine documentation to verify that any disclosure of private IP addresses and routing information to external entities is authorized. |  |  | X |
| **1.4** Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee/owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include:   • Specific configuration settings are defined.   • Personal firewall (or equivalent functionality) is actively running.   • Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices. |  |  |  |  |
| **1.4.a** Examine policies and configuration standards to verify:   • Personal firewall software or equivalent functionality is required for all portable computing devices (including company and/or employee-owned) that connect to the  Internet when outside the network, (for example, laptops used by employees), and which are also used to access the CDE.  • Specific configuration settings are defined for personal firewall or equivalent functionality.  • Personal firewall or equivalent functionality is configured to actively run.  • Personal firewall or equivalent functionality is configured to not be alterable by users of the portable computing devices. |  | X |  | Customers are responsible for installing and maintaining personal firewalls on customer owned portable computing devices.  Customers are responsible for implementing firewall rules for systems with direct connectivity to the Internet for systems used to manage the CDE.  Skytap has no access to customer data. |
| **1.4.b I**nspect a sample of portable computing devices (including company and/or employee-owned) to verify that:   • Personal firewall (or equivalent functionality) is installed and configured per the organization’s specific configuration settings.  • Personal firewall (or equivalent functionality) is actively running.   • Personal firewall or equivalent functionality is not alterable by users of the portable computing devices. |  | X |  |
| **1.5** Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties. |  |  |  |  |
| **1.5** Examine documentation and interview personnel to verify that security policies and operational procedures for managing firewalls are:   • Documented,   • In use, and   • Known to all affected parties. |  |  | X | Skytap maintains routers and firewalls used to deliver the Skytap Cloud platform. Skytap security policies and procedures for managing Skytap firewalls are documented, in use, and communicated to all affected parties.  Customers are responsible for ensuring that their policies and procedures for managing firewalls running on customer managed VMs are documented, in use, and known to all affected parties. |
| **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, POS terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc. |  |  |  |  |
| **2.1.a** Choose a sample of system components, and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords (including those on operating systems, software that provides security services, application and system accounts, POS terminals, and Simple Network Management Protocol (SNMP) community strings) have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.) |  |  | X | Skytap maintains systems used to deliver the Skytap Cloud platform. Default passwords, vendor-accounts, etc. on these systems are changed, disabled, or removed as appropriate.  Customers are responsible for changing vendor-supplied defaults for all services running on customer managed VMs and customer managed services providing access to customer managed VMs.   * <https://help.skytap.com/users-create.html> |
| **2.1.b** For the sample of system components, verify that all unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled. |  |  | X |
| **2.1.c** Interview personnel and examine supporting documentation to verify that:  • All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple  Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network.  • Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or  disabled before a system is installed on the network. |  |  | X |
| **2.1.1** For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. |  |  |  |  |
| **2.1.1.a** Interview responsible personnel and examine supporting documentation to verify that:  • Encryption keys were changed from default at installation   • Encryption keys are changed anytime anyone with knowledge of the keys leaves the company or changes positions. |  | X |  | Skytap Cloud does not host any wireless networks that transmit cardholder data. Customers are responsible for management of their networks, including those with wireless connectivity. |
| **2.1.1.b** Interview personnel and examine policies and procedures to verify:   • Default SNMP community strings are required to be changed upon installation.  • Default passwords/phrases on access points are required to be changed upon installation. |  | X |  |
| **2.1.1.c** Examine vendor documentation and login to wireless devices, with system administrator help, to verify:   • Default SNMP community strings are not used.  • Default passwords/passphrases on access points are not used. |  | X |  |
| **2.1.1.d** Examine vendor documentation and observe wireless configuration settings to verify firmware on wireless devices is updated to support strong encryption for:   • Authentication over wireless networks  • Transmission over wireless networks |  | X |  |
| **2.1.1.e** Examine vendor documentation and observe wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable. |  | X |  |
| **2.2** Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.  Sources of industry-accepted system hardening standards may include, but are not limited to:   • Center for Internet Security (CIS)   • International Organization for Standardization (ISO)  • SysAdmin Audit Network Security (SANS) Institute  • National Institute of Standards Technology (NIST) |  |  |  |  |
| **2.2.a** Examine the organization’s system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards. |  |  | X | Skytap maintains configuration standards for systems used to deliver the Skytap Cloud platform.  Customers are responsible for documenting configuration standards for all services running on customer managed VMs and customer managed services providing access to customer managed VMs. These standards should begin with Skytap Cloud published security best practices.   * <https://help.skytap.com/Security_Best_Practices.html> |
| **2.2.b** Examine policies and interview personnel to verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.1. |  |  | X |
| **2.2.c** Examine policies and interview personnel to verify that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network. |  |  | X |
| **2.2.d** Verify that system configuration standards include the following procedures for all types of system components:   • Changing of all vendor-supplied defaults and elimination of unnecessary default accounts  • Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server  • Enabling only necessary services, protocols, daemons, etc., as required for the function of the system  • Implementing additional security features for any required services, protocols or daemons that are considered to be insecure  • Configuring system security parameters to prevent misuse  • Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers |  |  | X |
| **2.2.1** Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component. |  |  |  |  |
| **2.2.1.a** Select a sample of system components and inspect the system configurations to verify that only one primary function is implemented per server. |  |  | X | Skytap maintains systems used to deliver the Skytap Cloud platform. Services on these systems are limited to one primary function per server as appropriate.  Customers are responsible for ensuring that only one primary function is implemented per customer managed server instance. |
| **2.2.1.b I**f virtualization technologies are used, inspect the system configurations to verify that only one primary function is implemented per virtual system component or device. |  |  | X |
| **2.2.2** Enable only necessary services, protocols, daemons, etc., as required for the function of the system. |  |  |  |  |
| **2.2.2.a** Select a sample of system components and inspect enabled system services, daemons, and protocols to verify that only necessary services or protocols are enabled. |  |  | X | Skytap maintains systems used to deliver the Skytap Cloud platform. Unnecessary services on these systems are disabled as appropriate. Any insecure services in use are documented with appropriate restrictions and business justification.  Customers are responsible fordisabling any unnecessary services running on customer managed VMs and documenting any insecure services running on customer managed VMs. |
| **2.2.2.b** Identify any enabled insecure services, daemons, or protocols and interview personnel to verify they are justified per documented configuration standards. |  |  | X |
| **2.2.3** Implement additional security features for any required services, protocols, or daemons that are considered to be insecure **Note:** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.* |  |  |  |  |
| **2.2.3.a** Inspect configuration settings to verify that security features are documented and implemented for all insecure services, daemons, or protocols. |  |  | X | Skytap maintains systems used to deliver the Skytap Cloud platform. Any insecure services in use are documented with appropriate restrictions and business justification.  Customers are responsible fordocumenting any insecure services running on customer managed VMs. |
| **2.2.3.b** If SSL/early TLS is used, perform testing procedures in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS. |  |  | X |
| **2.2.4** Configure system security parameters to prevent misuse. |  |  |  |  |
| **2.2.4.a** Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components. |  |  | X | Skytap maintains systems used to deliver the Skytap Cloud platform. Security parameters on these systems are documented and configured as appropriate.  Customers are responsible for documenting the functional and security configuration standards of customer managed VMS and any Skytap Cloud services used within the CDE to ensure that the secure state designed for the service can be maintained. |
| **2.2.4.b** Examine the system configuration standards to verify that common security parameter settings are included. |  |  | X |
| **2.2.4.c** Select a sample of system components and inspect the common security parameters to verify that they are set appropriately and in accordance with the configuration standards. |  |  | X |
| **2.2.5** Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. |  |  |  |  |
| **2.2.5.a** Select a sample of system components and inspect the configurations to verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed. |  |  | X | Skytap maintains systems used to deliver the Skytap Cloud platform. Unnecessary functionality and services on these systems are disabled as appropriate.  Customers are responsible for documenting, developing and implementing configuration standards for the customer managed VMs within the CDE. |
| **2.2.5.b.** Examine the documentation and security parameters to verify enabled functions are documented and support secure configuration. |  |  | X |
| **2.2.5.c.** Examine the documentation and security parameters to verify that only documented functionality is present on the sampled system components. |  |  | X |
| **2.3** Encrypt all non-console administrative access using strong cryptography.  **Note:** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.* |  |  |  |  |
| **2.3** Select a sample of system components and verify that non-console administrative access is encrypted by performing the following: |  |  | X | Skytap enforces encrypted access to all systems used to deliver the Skytap Cloud platform.  Customers are responsible for ensuring secure communication for administrative access to all customer managed VMs including Windows Remote Desktop (RDP) using “High Encryption” or “FIPS compatible” encryption settings or SSH v2 or above and appropriate SSH keys.   * <https://help.skytap.com/Accessing_VM_Desktops.html>   Customers are responsible for developing their own Risk Mitigation and Migration Plan to support their own PCI compliance activities regarding early TLS use. |
| **2.3.a** Observe an administrator log on to each system and examine system configurations to verify that a strong encryption method is invoked before the administrator’s password is requested. |  |  | X |
| **2.3.b** Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access. |  |  | X |
| **2.3.c** Observe an administrator log on to each system to verify that administrator access to any web-based management interfaces is encrypted with strong cryptography. |  |  | X |
| **2.3.d** Examine vendor documentation and interview personnel to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations. |  |  | X |
| **2.3.e** If SSL/early TLS is used, perform testing procedures in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS. |  |  | X |
| **2.4** Maintain an inventory of system components that are in scope for PCI DSS. |  |  |  |  |
| **2.4.a** Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each. |  |  | X | Skytap maintains an inventory of systems components used to deliver the Skytap Cloud platform.  Customers are responsible for maintaining an inventory of all system components on customer managed VMs instances and any other Skytap Cloud services that are in scope for their compliance. |
| **2.4.b** Interview personnel to verify the documented inventory is kept current. |  |  | X |
| **2.5** Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. |  |  |  |  |
| **2.5** Examine documentation and interview personnel to verify 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 | Skytap maintains security policies and procedures used to deliver the Skytap Cloud platform that are documented, used, and known to all affected parties.  Customers are responsible for ensuring that their policies and procedures used to operate customer managed VMs and any other customer managed Skytap Cloud services are documented and known to all affected 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 A1: Additional PCI DSS Requirements for Shared Hosting Providers.* |  |  |  |  |
| **2.6** Perform testing procedures **A1.1** through **A1.4** detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers* for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities’ (merchants and service providers) hosted environment and data. |  |  | X | Customers may also be considered a shared hosting provider, if they run applications or store data for their customers. In this case, customers are responsible for protecting their customer’s data within Skytap Cloud services. |
| **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 CHD storage:  • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements.  • Specific retention requirements for cardholder data  • Processes for secure deletion of data when no longer needed.  • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention. |  |  |  |  |
| **3.1.a** Examine the data-retention and disposal policies, procedures and processes to verify they include the following for all cardholder data (CHD) storage:  • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements.   • Specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons).  • Processes for secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons  • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements. |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate data retention policies and procedures, and processes for maintaining PCI Data Security Standard requirements |
| **3.1.b** Interview personnel to verify that:  • All locations of stored cardholder data are included in the data-retention and disposal processes.  • Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data.  • The quarterly automatic or manual process is performed for all locations of cardholder data. |  | X |  |
| **3.1.c** For a sample of system components that store cardholder data:   • Examine files and system records to verify that the data stored does not exceed the requirements defined in the data-retention policy.  • Observe the deletion mechanism to verify data is deleted securely. |  | X |  |
| **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: |  |  |  |  |
| **3.2.a** For issuers and/or companies that support issuing services and store sensitive authentication data, review policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data. |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI Data Security Standard requirements. |
| **3.2.b** For issuers and/or companies that support issuing services and store sensitive authentication data, examine data stores and system configurations to verify that the sensitive authentication data is secured. |  | X |  |
| **3.2.c** For all other entities, if sensitive authentication data is received, review policies and procedures, and examine system configurations to verify the data is not retained after authorization.3.2.c For all other entities, if sensitive authentication data is received, review policies and procedures, and examine system configurations to verify the data is not retained after authorization. |  | X |  |
| **3.2.d** For all other entities, if sensitive authentication data is received, review procedures and examine the processes for securely deleting the data to verify that the data is unrecoverable. |  | X |  |
| **3.2.1** Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:   • The cardholder’s name   • Primary account number (PAN)   • Expiration date   • Service code  To minimize risk, store only these data elements as needed for business. |  |  |  |  |
| **3.2.1** For a sample of system components, examine data sources, including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization:  • Incoming transaction data  • All logs (for example, transaction, history, debugging, error)  • History files  • Trace files  • Several database schemas  • Database contents |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI Data Security Standard requirements. |
| **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. |  |  |  |  |
| **3.2.2** For a sample of system components, examine data sources, including but not limited to the following, and verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization:   • Incoming transaction data  • All logs (for example, transaction, history, debugging, error)  • History files  • Trace files  • Several database schemas  • Database contents |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI Data Security Standard requirements. |
| **3.2.3** Do not store the personal identification number (PIN) or the encrypted PIN block after authorization. |  |  |  |  |
| **3.2.3** For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored after authorization:   • Incoming transaction data  • All logs (for example, transaction, history, debugging, error)  • History files  • Trace files  • Several database schemas  • Database contents |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI Data Security Standard requirements. |
| **3.3** Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than first six/last four digits of the PAN.  ***Note:*** *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.* |  |  |  |  |
| **3.3.a** Examine written policies and procedures for masking the display of PANs to verify:  • A list of roles that need access to displays of more than first six/last four (includes full PAN) is documented, together with a legitimate business need for each role to  have such access.  • PAN must be masked when displayed such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.  • All roles not specifically authorized to see the full PAN must only see masked PANs. |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate policies and procedures for masking the display of PANs. |
| **3.3.b** Examine system configurations to verify that full PAN is only displayed for users/roles with a documented business need, and that PAN is masked for all other requests. |  | X |  |
| **3.3.c** Examine displays of PAN (for example, on screen, on paper receipts) to verify that PANs are masked when displaying cardholder data, and that only those with a legitimate business need are able to see more than first six/last four digits of the PAN. |  | X |  |
| 3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:  • One-way hashes based on strong cryptography, (hash must be of the entire PAN).  • Truncation (hashing cannot be used to replace the truncated segment of PAN).  • Index tokens and pads (pads must be securely stored).  • Strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity’s environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. |  |  |  |  |
| **3.4.a** Examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the following methods:  • One-way hashes based on strong cryptography,   • Truncation   • Index tokens and pads, with the pads being securely stored  • Strong cryptography, with associated key-management processes and procedures |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate data retention policies and procedures, encryption technologies and key management processes for maintaining PCI Data Security Standard requirements. |
| **3.4.b** Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text). |  | X |  |
| **3.4.c** Examine a sample of removable media (for example, backup tapes) to confirm that the PAN is rendered unreadable. |  | X |  |
| **3.4.d** Examine a sample of audit logs, including payment application logs, to confirm that PAN is rendered unreadable or is not present in the logs. |  | X |  |
| **3.4.e** If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. |  | X |  |
| **3.4.1** If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.  *Note: This requirement applies in addition to all other PCI DSS encryption and key management requirements.* |  |  |  |  |
| **3.4.1.a** If disk encryption is used, inspect the configuration and observe the authentication process to verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating system’s authentication mechanism (for example, not using local user account databases or general network login credentials). |  |  | X | Skytap provides full disk encryption storage services to customers with encryption keys managed by Skytap. Customers and operating systems running on customer managed VMs do not have any access to disk encryption keys.  Customers are responsible for management of any storage encryption running on customer managed VMs. |
| **3.4.1.b** Observe processes and interview personnel to verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls). |  |  | X |
| **3.4.1.c** Examine the configurations and observe the processes to verify that cardholder data on removable media is encrypted wherever stored. ***Note:*** *If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.* |  |  | X |
| **3.5** Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: ***Note:*** *This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.* |  |  |  |  |
| **3.5** Examine key-management policies and procedures to verify processes are specified to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following: • Access to keys is restricted to the fewest number of custodians necessary.  • Key-encrypting keys are at least as strong as the data-encrypting keys they protect  • Key-encrypting keys are stored separately from data-encrypting keys.  • Keys are stored securely in the fewest possible locations and forms. |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate encryption key management policies and procedures for maintaining PCI Data Security Standard requirements. |
| **3.5.1** Interview responsible personnel and review documentation to verify that a document exists to describe the cryptographic architecture, including:  • 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 |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate encryption key management policies and procedures for maintaining PCI Data Security Standard requirements. |
| **3.5.2** Restrict access to cryptographic keys to the fewest number of custodians necessary. |  |  |  |  |
| **3.5.2** Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary. |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate encryption key management policies and procedures for maintaining PCI Data Security Standard requirements. |
| **3.5.3** Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:  • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key.  • Within a secure cryptographic device (such as a hardware/host security module (HSM) or PTS-approved point-of-interaction device).  • As at least two full-length key components or key shares, in accordance with an industry-accepted method.  Note: It is not required that public keys be stored in one of these forms. |  |  |  |  |
| **3.5.3.a** Examine documented procedures to verify that cryptographic keys used to encrypt/decrypt cardholder data must only exist 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 key components or key shares, in accordance with an industry-accepted method. |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate encryption key management policies and procedures for maintaining PCI Data Security Standard requirements. |
| **3.5.3.b** Examine system configurations and key storage locations to verify that cryptographic keys used to encrypt/decrypt cardholder data exist in one, (or more), of the following form at all times.   • Encrypted with a key-encrypting key.   • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device).  • As key components or key shares, in accordance with an industry-accepted method. |  |  |  |
| **3.5.3.c** Wherever key-encrypting keys are used, examine system configurations and key storage locations to verify:  • Key-encrypting keys are at least as strong as the data-encrypting keys they protect.  • Key-encrypting keys are stored separately from data-encrypting key**s.** |  | X |  |
| **3.5.4** Store cryptographic keys in the fewest possible locations. |  |  |  |  |
| **3.5.4** Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations. |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate encryption key management policies and procedures for maintaining PCI Data Security Standard requirements. |
| **3.6** Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: ***Note:*** *Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.* |  |  |  |  |
| **3.6.a *Additional Procedure for service provider assessments only:*** If the service provider shares keys with their customers for transmission or storage of cardholder data, examine the documentation that the service provider provides to their customers to verify that it includes guidance on how to securely transmit, store, and update customers’ keys, in accordance with Requirements 3.6.1 through 3.6.8 below. |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate encryption key management policies and procedures for maintaining PCI Data Security Standard requirements. |
| **3.6.b** Examine the key-management procedures and processes for keys used for encryption of cardholder data and perform the following: |  |  |  |  |
| **3.6.1** Generation of strong cryptographic keys. |  |  |  |  |
| **3.6.1.a** Verify that key-management procedures specify how to generate strong keys. |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate encryption key management policies and procedures for maintaining PCI Data Security Standard requirements. |
| **3.6.1.b** Observe the procedures for generating keys to verify that strong keys are generated. |  | X |  |
| **3.6.2** Secure cryptographic key distribution. |  |  |  |  |
| **3.6.2.a** Verify that key-management procedures specify how to securely distribute keys. |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate encryption key management policies and procedures for maintaining PCI Data Security Standard requirements. |
| **3.6.2.b** Observe the method for distributing keys to verify that keys are distributed securely. |  | X |  |
| **3.6.3 S**ecure cryptographic key storage. |  |  |  |  |
| **3.6.3.a** Verify that key-management procedures specify how to securely store keys. |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate encryption key management policies and procedures for maintaining PCI Data Security Standard requirements. |
| **3.6.3.b** Observe the method for storing keys to verify that keys are stored securely. |  | X |  |
| **3.6.4** Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57). |  |  |  |  |
| **3.6.4.a** Verify that key-management procedures include a defined cryptoperiod for each key type in use and define a process for key changes at the end of the defined cryptoperiod(s). |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate encryption key management policies and procedures for maintaining PCI Data Security Standard requirements. |
| **3.6.4.b** Interview personnel to verify that keys are changed at the end of the defined cryptoperiod(s). |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate encryption key management policies and procedures for maintaining PCI Data Security Standard requirements. |
| **3.6.5** Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. ***Note:*** *If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.* |  |  |  |  |
| **3.6.5.a** Verify that key-management procedures specify processes for the following:  • The retirement or replacement of keys when the integrity of the key has been weakened.  • The replacement of known or suspected compromised keys.  • Any keys retained after retiring or replacing are not used for encryption operations. |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate encryption key management policies and procedures for maintaining PCI Data Security Standard requirements. |
| **3.6.5.b** Interview personnel to verify the following processes are implemented:  • Keys are retired or replaced as necessary when the integrity of the key has been weakened, including when someone with knowledge of the key leaves the company.  • Keys are replaced if known or suspected to be compromised.  • Any keys retained after retiring or replacing are not used for encryption operations. |  | X |  |
| **3.6.6** If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.  ***Note:*** *Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.* |  |  |  |  |
| **3.6.6.a** Verify that manual clear-text key-management procedures specify processes for the use of the following:  • Split knowledge of keys, such that key components are under the control of at least two people who only have knowledge of their own key components; AND  • Dual control of keys, such that at least two people are required to perform any key-management operations and no one person has access to the authentication materials (for example, passwords or keys) of another. |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate encryption key management policies and procedures for maintaining PCI Data Security Standard requirements. |
| **3.6.6 b** Interview personnel and/or observe processes to verify that manual clear-text keys are managed with:   • Split knowledge, AND  • Dual control |  | X |  |
| **3.6.7** Prevention of unauthorized substitution of cryptographic keys. |  |  |  |  |
| **3.6.7.a** Verify that key-management procedures specify processes to prevent unauthorized substitution of keys. |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate encryption key management policies and procedures for maintaining PCI Data Security Standard requirements. |
| **3.6.7.b** Interview personnel and/or observe process to verify that unauthorized substitution of keys is prevented. |  | X |  |
| **3.6.8** Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities. |  |  |  |  |
| **3.6.8.a** Verify that key-management procedures specify processes for key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities. |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including maintaining appropriate encryption key management policies and procedures for maintaining PCI Data Security Standard requirements. |
| **3.6.8.b** Observe documentation or other evidence showing that key custodians have acknowledged (in writing or electronically) that they understand and accept their key-custodian responsibilities. |  | X |  |
| **3.7** Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties. |  |  |  |  |
| **3.7** Examine documentation and interview personnel to verify that security policies and operational procedures for protecting stored cardholder data are:  • Documented,   • In use, and   • Known to all affected parties |  | X |  | Customers are responsible for all aspects of secure storage of cardholder data, including ensuring that their policies and procedures for protecting stored cardholder data are documented and known to all affected parties. |
| **4.1** Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:  • Only trusted keys and certificates are accepted.  • The protocol in use only supports secure versions or configurations.  • The encryption strength is appropriate for the encryption methodology in use. Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed . Examples of open, public networks include but are not limited to:  • The Internet  • Wireless technologies, including 802.11 and Bluetooth  • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)  • General Packet Radio Service (GPRS)  • Satellite communications |  |  |  |  |
| **4.1.a** Identify all locations where cardholder data is transmitted or received over open, public networks. Examine documented standards and compare to system configurations to verify the use of security protocols and strong cryptography for all locations. |  |  | X | Skytap is responsible for providing methods of secure access to the Skytap Cloud platform. In particular, Skytap provides the following services:   1. Authentication to cloud.skytap.com (via SSL) 2. Customer VPN termination endpoints are provided inside of the Skytap application. Skytap is responsible for providing VPN technologies that support strong cryptography. Customer is responsible for configuring the VPN correctly. 3. Remote desktop functionality. Skytap provides secure web based and VNC based remote desktop technologies to allow customers to connect to their VMs. 4. Data import services. Skytap provides SFTP and other secure data import tools.   Customers are responsible for properly configuring and using provided secure access methods including configuration of secure VPN connections, using secure data import services, and other secure services provided by Skytap.  Customers are responsible for securing all services running on customer managed VMs (SSL configs, SSH configs, key management, etc.).    Customers are responsible for developing their own Risk Mitigation and Migration Plan to support their own PCI compliance activities regarding early TLS use.   * <https://help.skytap.com/vpn-access-control.html> * <https://help.skytap.com/vpn-connecting-environments.html> * <https://help.skytap.com/Adding_Sharing_Files.html> |
| **4.1.b** Review documented policies and procedures to verify processes are specified for the following:  • For acceptance of only trusted keys and/or certificates.  • For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported).  • For implementation of proper encryption strength per the encryption methodology in use. |  |  | X |
| **4.1.c** Select and observe a sample of inbound and outbound transmissions as they occur (for example, by observing system processes or network traffic) to verify that all cardholder data is encrypted with strong cryptography during transit. |  |  | X |
| **4.1.d** Examine keys and certificates to verify that only trusted keys and/or certificates are accepted. |  |  | X |
| **4.1.e** Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations. |  |  | X |
| **4.1.f** Examine system configurations to verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.) |  |  | X |
| **4.1.g** For TLS implementations, examine system configurations to verify that TLS is enabled whenever cardholder data is transmitted or received.  For example, for browser-based implementations:  • “HTTPS” appears as the browser Universal Record Locator (URL) protocol; and   • Cardholder data is only requested if “HTTPS” appears as part of the URL. |  |  | X |
| **4.1.h** If SSL/early TLS is used, perform testing procedures in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS. |  |  | X |
| **4.1.1** Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission. |  |  |  |  |
| **4.1.1** Identify all wireless networks transmitting cardholder data or connected to the cardholder data environment. Examine documented standards and compare to system configuration settings |  | X |  | Skytap does not host any wireless networks that transmit cardholder data.  Customers are responsible for management of their networks, including those with wireless connectivity. |
| **4.2** Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.). |  |  |  |  |
| **4.2.a** If end-user messaging technologies are used to send cardholder data, observe processes for sending PAN and examine a sample of outbound transmissions as they occur to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. |  | X |  | Customers are responsible for the use of any end-user messaging technologies for transmitting PAN. |
| **4.2.b** Review written policies to verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies. |  | X |  |
| **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. |  |  |  |  |
| **4.3** Examine documentation and interview personnel to verify that security policies and operational procedures for encrypting transmissions of cardholder data are:  • Documented,   • In use, and   • Known to all affected parties. |  | X |  | Customers are responsible for ensuring that their policies and procedures for encrypting transmissions of cardholder data are documented and known to all affected parties. |
| **5.1** Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). |  |  |  |  |
| **5.1 For a sample** of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists. |  |  | X | Skytap deploys anti-virus software on systems used to manage the Skytap platform.  Customers are responsible for managing anti-virus to PCI requirements on customer managed VMs. |
| **5.1.1** Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. |  |  |  |  |
| **5.1.1** Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs;  • Detect all known types of malicious software,   • Remove all known types of malicious software, and   • Protect against all known types of malicious software.  (Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits). |  |  | X | Skytap deploys anti-virus software on systems used to manage the Skytap platform.  Customers are responsible for managing anti-virus to PCI requirements on customer managed VMs. |
| **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. |  |  |  |  |
| **5.1.2** Interview personnel to verify that evolving malware threats are monitored |  |  | X | Skytap monitors all systems used to operate the Skytap platform for evolving malware threats and the need for anti-virus software.  Customers are responsible for managing anti-virus to PCI requirements on customer managed VMs. |
| **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. |  |  |  |  |
| **5.2.a** Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up-to-date. |  |  | X | Skytap deploys anti-virus software on systems used to manage the Skytap platform. Configurations are managed in compliance with Skytap policies and procedures requiring automatic updates and periodic scanning.  Customers are responsible for managing anti-virus to PCI requirements on customer managed VMs. |
| **5.2.b** Examine anti-virus configurations, including the master installation of the software, to verify anti-virus mechanisms are:  • Configured to perform automatic updates, and   • Configured to perform periodic scans. |  |  | X |
| **5.2.c** Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that:   • The anti-virus software and definitions are current.  • Periodic scans are performed. |  |  | X |
| **5.2.d** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that:  • Anti-virus software log generation is enabled, and  • Logs are retained in accordance with PCI DSS Requirement 10.7 |  |  | X |
| **5.3** Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.  ***Note:*** *Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.* |  |  |  |  |
| **5.3.a** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify the anti-virus software is actively running. |  |  | X | Skytap deploys anti-virus software on systems used to manage the Skytap platform.  Customers are responsible for managing anti-virus to PCI requirements on customer managed VMs. |
| **5.3.b** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that the anti-virus software cannot be disabled or altered by users. |  |  | X |
| **5.3.c** Interview responsible personnel and observe processes to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. |  |  | X |
| **5.4** Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties. |  |  |  |  |
| **5.4** Examine documentation and interview personnel to verify that security policies and operational procedures for protecting systems against malware are:  • Documented,   • In use, and   • Known to all affected parties. |  |  | X | Skytap maintains anti-malware policies and procedures for systems used to manage the Skytap platform. These policies and procedures are documented, in use, and communicated to all affected parties.  Customers are responsible for managing anti-malware policies and procedures to PCI requirements on customer managed VMs. |
| **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.  ***Note:*** *Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.* |  |  |  |  |
| **6.1.a** Examine policies and procedures to verify that processes are defined for the following:  • To identify new security vulnerabilities.   • To assign a risk ranking to vulnerabilities that includes identification of all “high risk” and “critical” vulnerabilities.  • To include using reputable outside sources for security vulnerability information. |  |  | X | Skytap operates a vulnerability management program covering systems used to operate the Skytap platform. Skytap will notify customers when appropriate of emerging vulnerabilities on the Skytap platform.  Customers are responsible for maintaining a vulnerability management program for customer managed VMs.  Customers are responsible for reviewing all Skytap Cloud Security Notices and ensuring that any recommendations that are applicable to the customer’s environment are reviewed and implemented as necessary.   * https://help.skytap.com/Security\_Best\_Practices.html |
| **6.1.b** Interview responsible personnel and observe processes to verify that:   • New security vulnerabilities are identified.   • A risk ranking is assigned to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities.   • Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information. |  |  | X |
| **6.2** Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1. |  |  |  |  |
| **6.2.a** Examine policies and procedures related to security-patch installation to verify processes are defined for:  • Installation of applicable critical vendor-supplied security patches within one month of release.  • Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months). |  |  | X | Skytap maintains policies and procedures and associated security patching program covering systems used to operate the Skytap platform. Skytap will notify customers when appropriate of emerging vulnerabilities on the Skytap platform.  Customers are responsible for installing security patches on customer managed VMs.  Customers are responsible for reviewing all Skytap Cloud Security Notices and ensuring that any recommendations that are applicable to the customer’s environment are reviewed and implemented as necessary.   * <https://help.skytap.com/Security_Best_Practices.html> |
| **6.2.b** For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify the following:  • That applicable critical vendor-supplied security patches are installed within one month of release.  • All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months). |  |  | X |
| **6.3** Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:  • In accordance with PCI DSS (for example, secure authentication and logging).   • Based on industry standards and/or best practices.  • Incorporate information security throughout the software development life cycle.  Note: this applies to all software developed internally as well as bespoke or custom software developed by a third party. |  |  |  |  |
| **6.3.a** Examine written software-development processes to verify that the processes are based on industry standards and/or best practices. |  |  | X | Skytap utilizes secure software development procedures for all code used to operate the Skytap Cloud platform.  Customers are responsible for maintaining secure software development procedures for all customer developed applications deployed on customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **6.3.b** Examine written software development processes to verify that information security is included throughout the life cycle. |  |  | X |
| **6.3.c** Examine written software development processes to verify that software applications are developed in accordance with PCI DSS. |  |  | X |
| **6.3.d** Interview software developers to verify that written software development processes are implemented. |  |  | X |
| **6.3.1** Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers. |  |  |  |  |
| **6.3.1** Examine written software-development procedures and interview responsible personnel to verify that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers. |  |  | X | Skytap removes all development, test, and pre-production account credentials prior to production deployment of code used to operate the Skytap Cloud platform.  Customers are responsible for securing account credentials on customer managed VMs and Skytap account credentials managed through Skytap customer portal. Skytap Cloud IAM accounts and roles can be used to separate development and test environments. |
| 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. Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6. |  |  |  |  |
| **6.3.2.a** Examine written software development procedures and interview responsible personnel to verify that all custom application code changes must be reviewed (using either manual or automated processes) as follows:  • Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices.  • Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5).  • Appropriate corrections are implemented prior to release.  • Code-review results are reviewed and approved by management prior to release. |  |  | X | Skytap utilizes secure software development procedures for all code used to operate the Skytap Cloud platform.  Customers are responsible for maintaining secure software development procedures for all customer developed applications deployed on customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **6.3.2.b** Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.2.a, above. |  |  | X |
| **6.4** Follow change control processes and procedures for all changes to system components. The processes must include the following: |  |  |  |  |
| **6.4** Examine policies and procedures to verify the following are defined:   • Development/test environments are separate from production environments with access control in place to enforce separation.  • A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment.  • Production data (live PANs) are not used for testing or development.  • Test data and accounts are removed before a production system becomes active.  • Change control procedures related to implementing security patches and software modifications are documented. |  |  | X | Skytap follows documented change control procedures for all systems used to operate the Skytap Cloud platform. Skytap does not have access to any PAN data.  Customers are responsible for following change controls procedures for customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **6.4.1** Separate development/test environments from production environments, and enforce the separation with access controls. |  |  |  |  |
| **6.4.1.a** Examine network documentation and network device configurations to verify that the development/test environments are separate from the production environment(s). |  |  | X | Skytap maintains separate development, test, and production environments for systems used to operate the Skytap Cloud platform.  Customers are responsible for maintaining separate development, test, and production environments on customer managed VMs and for any other customer managed systems accessing Skytap Cloud services including Skytap APIs. |
| **6.4.1.b** Examine access controls settings to verify that access controls are in place to enforce separation between the development/test environments and the production environment(s). |  |  | X |
| **6.4.2** Separation of duties between development/test and production environments. |  |  |  |  |
| **6.4.2** Observe processes and interview personnel assigned to development/test environments and personnel assigned to production environments to verify that separation of duties is in place between development/test environments and the production environment. |  |  | X | Skytap maintains appropriate separation of duties for systems used to operate the Skytap Cloud platform.  Customers are responsible for maintaining separation of duties for access to customer managed VMs and for any other customer managed systems accessing Skytap Cloud services including Skytap APIs. |
| **6.4.3** Production data (live PANs) are not used for testing or development. |  |  |  |  |
| **6.4.3.a** Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development. |  |  | X | Skytap maintains separate development, test, and production environments for systems used to operate the Skytap Cloud platform. Skytap does not utilize production data in development or test environments. Skytap does not have any access to PAN data.  Customers are responsible for maintaining separate development, test, and production environments on customer managed VMs and for any other customer managed systems accessing Skytap Cloud services including Skytap APIs. Customers are responsible for ensuring that production data is not used in customer managed development or test environments. |
| **6.4.3.b** Examine a sample of test data to verify production data (live PANs) is not used for testing or development. |  |  | X |
| **6.4.4** Removal of test data and accounts from system components before the system becomes active / goes into production. |  |  |  |  |
| **6.4.4.a** Observe testing processes and interview personnel to verify test data and accounts are removed before a production system becomes active. |  |  | X | Skytap maintains separate development, test, and production environments for systems used to operate the Skytap Cloud platform. Skytap development and test account prior to production deployment.  Customers are responsible for maintaining separate development, test, and production environments on customer managed VMs and for any other customer managed systems accessing Skytap Cloud services including Skytap APIs. Customers are responsible for removing development and test accounts on these systems prior to production deployment. |
| **6.4.4.b** Examine a sample of data and accounts from production systems recently installed or updated to verify test data and accounts are removed before the system becomes active. |  |  | X |
| **6.4.5** Change control procedures must include the following: |  |  |  |  |
| **6.4.5.a** Examine documented change-control procedures and verify procedures are defined for:  • Documentation of impact.  • Documented change approval by authorized parties.  • Functionality testing to verify that the change does not adversely impact the security of the system.  • Back-out procedures. |  |  | X | Skytap follows documented change control procedures for all systems used to operate the Skytap Cloud platform.  Customers are responsible for following change controls procedures for customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **6.4.5.b** For a sample of system components, interview responsible personnel to determine recent changes. Trace those changes back to related change control documentation. For each change examined, perform the following: |  |  | X |
| **6.4.5.1** Documentation of impact. |  |  |  |  |
| **6.4.5.1** Verify that documentation of impact is included in the change control documentation for each sampled change. |  |  | X | Skytap follows documented change control procedures for all systems used to operate the Skytap Cloud platform.  Customers are responsible for following change controls procedures for customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **6.4.5.2** Documented change approval by authorized parties. |  |  |  |  |
| **6.4.5.2** Verify that documented approval by authorized parties is present for each sampled change. |  |  | X | Skytap follows documented change control procedures for all systems used to operate the Skytap Cloud platform.  Customers are responsible for following change controls procedures for customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **6.4.5.3** Functionality testing to verify that the change does not adversely impact the security of the system. |  |  |  |  |
| **6.4.5.3.a** For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system. |  |  | X | Skytap follows documented change control procedures for all systems used to operate the Skytap Cloud platform.  Customers are responsible for following change controls procedures for customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **6.4.5.3.b** For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production. |  |  | X |
| **6.4.5.4** Back-out procedures. |  |  |  |  |
| **6.4.5.4** Verify that back-out procedures are prepared for each sampled change. |  |  | X | Skytap follows documented change control procedures for all systems used to operate the Skytap Cloud platform.  Customers are responsible for following change controls procedures for customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **6.4.6** Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.   ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* |  |  |  |  |
| **6.4.6** For a sample of significant changes, examine change records, interview personnel and observe the affected systems/networks to verify that applicable PCI DSS requirements were implemented and documentation updated as part of the change. |  |  | X | Skytap follows documented change control procedures for all systems used to operate the Skytap Cloud platform.  Customers are responsible for following change controls procedures for customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **6.5** Address common coding vulnerabilities in software-development processes as follows:  • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities.  • Develop applications based on secure coding guidelines. Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements. |  |  |  |  |
| **6.5.a** Examine software development policies and procedures to verify that up-to-date training in secure coding techniques is required for developers at least annually, based on industry best practices and guidance. |  |  | X | Skytap operates a secure coding training program for the Skytap development team and follows secure coding guidelines for all code used to operate the Skytap Cloud platform.  Customers are responsible for following secure coding guidelines for all customer developed software interacting with Skytap services such as the Skytap Cloud API. Customers are responsible for conducting secure coding training for customer development teams. |
| **6.5.b** Examine records of training to verify that software developers receive up-to-date training on secure coding techniques at least annually, including how to avoid common coding vulnerabilities |  |  | X |
| **6.5.c.** Verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities: |  |  | X |
| ***Note:*** *Requirements 6.5.1 through 6.5.6, below, apply to all applications (internal or external):* |  |  |  |  |
| **6.5.1** Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. |  |  |  |  |
| **6.5.1** Examine software-development policies and procedures and interview responsible personnel to verify that injection flaws are addressed by coding techniques that include:  • Validating input to verify user data cannot modify meaning of commands and queries.  • Utilizing parameterized queries. |  |  | X | Skytap utilizes secure software development procedures for all code used to operate the Skytap Cloud platform.  Customers are responsible for maintaining secure software development procedures for all customer developed applications deployed on customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **6.5.2** Buffer overflow. |  |  |  |  |
| **6.5.2** Examine software-development policies and procedures and interview responsible personnel to verify that buffer overflows are addressed by coding techniques that include:  • Validating buffer boundaries.   • Truncating input strings. |  |  | X | Skytap utilizes secure software development procedures for all code used to operate the Skytap Cloud platform.  Customers are responsible for maintaining secure software development procedures for all customer developed applications deployed on customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **6.5.3** Insecure cryptographic storage. |  |  |  |  |
| **6.5.3** Examine software-development policies and procedures and interview responsible personnel to verify that insecure cryptographic storage is addressed by coding techniques that:  • Prevent cryptographic flaws.  • Use strong cryptographic algorithms and keys. |  |  | X | Skytap utilizes secure software development procedures for all code used to operate the Skytap Cloud platform.  Customers are responsible for maintaining secure software development procedures for all customer developed applications deployed on customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **6.5.4** Insecure communications. |  |  |  |  |
| **6.5.4** Examine software-development policies and procedures and interview responsible personnel to verify that insecure communications are addressed by coding techniques that properly authenticate and encrypt all sensitive communications. |  |  | X | Skytap utilizes secure software development procedures for all code used to operate the Skytap Cloud platform.  Customers are responsible for maintaining secure software development procedures for all customer developed applications deployed on customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **6.5.5** Improper error handling. |  |  |  |  |
| **6.5.5** Examine-software development policies and procedures and interview responsible personnel to verify that improper error handling is addressed by coding techniques that do not leak information via error messages (for example, by returning generic rather than specific error details). |  |  | X | Skytap utilizes secure software development procedures for all code used to operate the Skytap Cloud platform.  Customers are responsible for maintaining secure software development procedures for all customer developed applications deployed on customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **6.5.6** All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1). |  |  |  |  |
| **6.5.6** Examine software-development policies and procedures and interview responsible personnel to verify that coding techniques address any “high risk” vulnerabilities that could affect the application, as identified in PCI DSS Requirement 6.1. |  |  | X | Skytap utilizes secure software development procedures for all code used to operate the Skytap Cloud platform.  Customers are responsible for maintaining secure software development procedures for all customer developed applications deployed on customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| ***Note:*** *Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external):* |  |  |  |  |
| **Indicate whether** web applications and application interfaces are present**. (yes/no)**  *If “no,” mark the below 6.5.7-6.5.10 as “Not Applicable.” If “yes,”* ***complete the following:*** |  |  |  | **yes** |
| **6.5.7** Cross-site scripting (XSS). |  |  |  |  |
| **6.5.7** Examine software-development policies and procedures and interview responsible personnel to verify that cross-site scripting (XSS) is addressed by coding techniques that include:  • Validating all parameters before inclusion.  • Utilizing context-sensitive escaping. |  |  | X | Skytap utilizes secure software development procedures for all code used to operate the Skytap Cloud platform.  Customers are responsible for maintaining secure software development procedures for all customer developed applications deployed on customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **6.5.8** Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions). |  |  |  |  |
| **6.5.8** Examine software-development policies and procedures and interview responsible personnel to verify that improper access control—such as insecure direct object references, failure to restrict URL access, and directory traversal—is addressed by coding technique that include:  • Proper authentication of users.   • Sanitizing input.  • Not exposing internal object references to users.  • User interfaces that do not permit access to unauthorized functions. |  |  | X | Skytap utilizes secure software development procedures for all code used to operate the Skytap Cloud platform.  Customers are responsible for maintaining secure software development procedures for all customer developed applications deployed on customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **6.5.9** Cross-site request forgery (CSRF). |  |  |  |  |
| **6.5.9** Examine software development policies and procedures and interview responsible personnel to verify that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers. |  |  | X | Skytap utilizes secure software development procedures for all code used to operate the Skytap Cloud platform.  Customers are responsible for maintaining secure software development procedures for all customer developed applications deployed on customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **6.5.10** Broken authentication and session management. |  |  |  |  |
| **6.5.10** Examine software development policies and procedures and interview responsible personnel to verify that broken authentication and session management are addressed via coding techniques that commonly include:   • Flagging session tokens (for example cookies) as “secure.”  • Not exposing session IDs in the URL.  • Incorporating appropriate time-outs and rotation of session IDs after a successful login. |  |  | X | Skytap utilizes secure software development procedures for all code used to operate the Skytap Cloud platform.  Customers are responsible for maintaining secure software development procedures for all customer developed applications deployed on customer managed VMs and customer developed software interacting with Skytap services such as the Skytap Cloud API.   * <https://help.skytap.com/reference-architecture-ci-cd.html> * <https://help.skytap.com/developer-tools.html> |
| **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. Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2.  • 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. |  |  |  |  |
| **6.6** For public-facing web applications, ensure that either one of the following methods is in place as follows:   • Examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed—using either manual or automated vulnerability security assessment tools or methods—as follows: - At least annually. - After any changes. - By an organization that specializes in application security. - That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. - That all vulnerabilities are corrected. - That the application is re-evaluated after the corrections.  • Examine the system configuration settings and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place as follows:  - Is situated in front of public-facing web applications to detect and prevent web-based attacks. - Is actively running and up-to-date as applicable. - Is generating audit logs.  - Is configured to either block web-based attacks, or generate an alert that is immediately investigated. |  |  | X | Skytap conducts vulnerability assessments for public Internet facing Skytap Cloud services.  Customers are responsible for implementing security assessments or Web Application Filtering for web applications deployed on customer managed VMs. |
| **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. |  |  |  |  |
| **6.7** Examine documentation and interview personnel to verify 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 | Skytap maintains security policies and procedures covering systems and applications used to operate the Skytap Cloud platform. These policies and procedures are documented, in use, and communicated to all affected parties.  Customers are responsible for maintaining security policies and procedures covering all systems and applications on customer managed VMs and as well as customer developed software interacting with Skytap services such as the Skytap Cloud API. |
| **7.1** Limit access to system components and cardholder data to only those individuals whose job requires such access. |  |  |  |  |
| **7.1.a** Examine written policy for access control, and verify that the policy incorporates 7.1.1 through 7.1.4 as follows:   • Defining access needs and privilege assignments for each role.  • Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities.  • Assignment of access based on individual personnel’s job classification and function.   • Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> |
| **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. |  |  |  |  |
| **7.1.1** Select a sample of roles and verify access needs for each role are defined and include:  • System components and data resources that each role needs to access for their job function.  • Identification of privilege necessary for each role to perform their job function. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> |
| **7.1.2** Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. |  |  |  |  |
| **7.1.2.a** Interview personnel responsible for assigning access to verify that access to privileged user IDs is:  • Assigned only to roles that specifically require such privileged access.  • Restricted to least privileges necessary to perform job responsibilities. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> |
| **7.1.2.b** Select a sample of user IDs with privileged access and interview responsible management personnel to verify that privileges assigned are:  • Necessary for that individual’s job function.  • Restricted to least privileges necessary to perform job responsibilities. |  |  | X |
| **7.1.3** Assign access based on individual personnel’s job classification and function. |  |  |  |  |
| **7.1.3** Select a sample of user IDs and interview responsible management personnel to verify that privileges assigned are based on that individual’s job classification and function. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> |
| **7.1.4** Require documented approval by authorized parties specifying required privileges. |  |  |  |  |
| **7.1.4** Select a sample of user IDs and compare with documented approvals to verify that:  • Documented approval exists for the assigned privileges.  • The approval was by authorized parties.  • That specified privileges match the roles assigned to the individual. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> |
| **7.2** Establish an access control system(s) for systems components that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.  This access control system(s) must include the following: |  |  |  |  |
| **7.2** Examine system settings and vendor documentation to verify that an access control system(s) is implemented as follows: |  |  |  |  |
| **7.2.1** Coverage of all system components. |  |  |  |  |
| **7.2.1** Confirm that access control systems are in place on all system components. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> |
| **7.2.2** Assignment of privileges to individuals based on job classification and function. |  |  |  |  |
| **7.2.2** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> |
| **7.2.3** Default “deny-all” setting. |  |  |  |  |
| **7.2.3** Confirm that the access control systems have a default “deny-all” setting. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> |
| **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. |  |  |  |  |
| **7.3** Examine documentation and interview personnel to verify that security policies and operational procedures for restricting access to cardholder data are:  • Documented,   • In use, and   • Known to all affected parties. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> |
| **8.1** Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: |  |  |  |  |
| **8.1.a** Review procedures and confirm they define processes for each of the items below at 8.1.1 through 8.1.8. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> |
| **8.1.b** Verify that procedures are implemented for user identification management, by performing the following: |  |  |  |  |
| **8.1.1** Assign all users a unique ID before allowing them to access system components or cardholder data. |  |  |  |  |
| **8.1.1** Interview administrative personnel to confirm that all users are assigned a unique ID for access to system components or cardholder data. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> |
| **8.1.2** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. |  |  |  |  |
| **8.1.2** For a sample of privileged user IDs and general user IDs, examine associated authorizations and observe system settings to verify each user ID and privileged user ID has been implemented with only the privileges specified on the documented approval. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> |
| **8.1.3** Immediately revoke access for any terminated users. |  |  |  |  |
| **8.1.3.a** Select a sample of users terminated in the past six months, and review current user access lists*—*forbothlocal and remote access—to verify that their IDs have been deactivated or removed from the access lists. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> * <https://help.skytap.com/users-delete-deactivate.html> |
| **8.1.3.b** Verify all physical authentication methods—such as, smart cards, tokens, etc.—have been returned or deactivated. |  |  | X |
| **8.1.4** Remove/disable inactive user accounts within 90 days. |  |  |  |  |
| **8.1.4** Observe user accounts to verify that any inactive accounts over 90 days old are either removed or disabled. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> * <https://help.skytap.com/users-delete-deactivate.html> * <https://help.skytap.com/Password_Policy.html> |
| **8.1.5** Manage IDs used by third parties to access, support, or maintain system components via remote access as follows:  • Enabled only during the time period needed and disabled when not in use.   • Monitored when in use. |  |  |  |  |
| **8.1.5.a** Interview personnel and observe processes for managing accounts used by third parties to access, support, or maintain system components to verify that accounts used for remote access are:  • Disabled when not in use.  • Enabled only when needed by the third party, and disabled when not in use. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> * <https://help.skytap.com/users-delete-deactivate.html> |
| **8.1.5.b** Interview personnel and observe processes to verify that third party remote access accounts are monitored while being used. |  |  | X |
| **8.1.6** Limit repeated access attempts by locking out the user ID after not more than six attempts. |  |  |  |  |
| **8.1.6.a** For a sample of system components, inspect system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts. |  |  | X | Skytap maintains password policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing the creation of user accounts. Skytap Cloud IAM features include basic password management options for local accounts, such as password length and complexity requirements.  Additional password management controls can be provided by leveraging tools such as Multi- Factor Authentication (MFA) provided by Skytap Cloud or integrating with a corporate directory service.  Additionally, for password management on VMs instances, customers are responsible for establishing a policy for the servers that align with the applicable PCI requirements.   * <https://help.skytap.com/Password_Policy.html> |
| **8.1.6.b** Additional procedure for service provider assessments only: Review internal processes and customer/user documentation, and observe implemented processes to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts. |  |  | X |
| **8.1.7** Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. |  |  |  |  |
| **8.1.7** For a sample of system components, inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account. |  |  | X | Skytap maintains password policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing the creation of user accounts. Skytap Cloud IAM features include basic password management options for local accounts, such as password length and complexity requirements.  Additional password management controls can be provided by leveraging tools such as Multi- Factor Authentication (MFA) provided by Skytap Cloud or integrating with a corporate directory service.  Additionally, for password management on VMs instances, customers are responsible for establishing a policy for the servers that align with the applicable PCI requirements.   * <https://help.skytap.com/Password_Policy.html> |
| **8.1.8** If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. |  |  |  |  |
| **8.1.8** For a sample of system components, inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less. |  |  | X | Skytap maintains password policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing the creation of user accounts. Skytap Cloud IAM features include basic password management options for local accounts, such as password length and complexity requirements.  Additional password management controls can be provided by leveraging tools such as Multi- Factor Authentication (MFA) provided by Skytap Cloud or integrating with a corporate directory service.  Additionally, for password management on VMs instances, customers are responsible for establishing a policy for the servers that align with the applicable PCI requirements.   * <https://help.skytap.com/Password_Policy.html> |
| **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. |  |  |  |  |
| **8.2** To verify that users are authenticated using unique ID and additional authentication (for example, a password/phrase) for access to the cardholder data environment, perform the following:  • Examine documentation describing the authentication method(s) used.  • For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s). |  |  | X | Skytap maintains identity, access, and authorization policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing the creation of user accounts. Skytap Cloud IAM features include basic password management options for local accounts, such as password length and complexity requirements.  Additional password management controls can be provided by leveraging tools such as Multi- Factor Authentication (MFA) provided by Skytap Cloud or integrating with a corporate directory service.  Additionally, for password management on VMs instances, customers are responsible for establishing a policy for the servers that align with the applicable PCI requirements.   * <https://help.skytap.com/Password_Policy.html> |
| **8.2.1** Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. |  |  |  |  |
| **8.2.1.a** Examine vendor documentation and system configuration settings to verify that passwords are protected with strong cryptography during transmission and storage. |  |  | X | Skytap maintains identity, access, and authorization policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for the processes and creation of accounts using the various authentication mechanisms offered by Skytap Cloud with Skytap Cloud IAM. For accounts managed directly in Skytap Cloud IAM, passwords are rendered unreadable in storage and transmission. For customers connecting Skytap Cloud IAM to the corporate directory, customers are responsible for ensuring that the corporate directory configuration stores credentials in an unreadable and protected format as well as in transit for authentication to Skytap Cloud systems.    Customers are responsible for the processes and creation of accounts and access controls using the various authentication mechanisms offered by Skytap Cloud. This includes access controls to all Skytap Cloud Services included in scope as well as to the server instances and applications that customers may be hosting in VMs. Any applications or authentication such as corporate directories or applications hosted in VMs, customers are responsible for ensuring proper configuration of the authentication mechanisms to ensure that passwords are unreadable in storage and transmission. Authentication mechanisms managed by Skytap Cloud render the password unreadable in storage and transmission.   * <https://help.skytap.com/Sso_Policy.html> |
| **8.2.1.b** For a sample of system components, examine password files to verify that passwords are unreadable during storage. |  |  | X |
| **8.2.1.c** For a sample of system components, examine data transmissions to verify that passwords are unreadable during transmission. |  |  | X |
| **8.2.1.d** Additional procedure for service provider assessments only: Observe password files to verify that non-consumer customer passwords are unreadable during storage. |  |  | X |
| **8.2.1.e** Additional procedure for service provider assessments only: Observe data transmissions to verify that non-consumer customer passwords are unreadable during transmission. |  |  | X |
| **8.2.2** Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys. |  |  |  |  |
| **8.2.2** Examine authentication procedures for modifying authentication credentials and observe security personnel to verify that, if a user requests a reset of an authentication credential by phone, e-mail, web, or other non-face-to-face method, the user’s identity is verified before the authentication credential is modified. |  |  | X | Skytap maintains identity, access, and authorization policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing the creation of user accounts. Skytap Cloud IAM features include basic password management options for local accounts, such as password length and complexity requirements.  Additional password management controls can be provided by leveraging tools such as Multi- Factor Authentication (MFA) provided by Skytap Cloud or integrating with a corporate directory service.  Additionally, for password management on VMs instances, customers are responsible for establishing a policy for the servers that align with the applicable PCI requirements.   * <https://help.skytap.com/Password_Policy.html> |
| **8.2.3** Passwords/passphrases must meet the following:  • Require a minimum length of at least seven characters.  • Contain both numeric and alphabetic characters. Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above. |  |  |  |  |
| **8.2.3.a** For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require at least the following strength/complexity:  • Require a minimum length of at least seven characters.  • Contain both numeric and alphabetic characters. |  |  | X | Skytap maintains password policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing the creation of user accounts. Skytap Cloud IAM features include basic password management options for local accounts such as password length and complexity requirements.  Additional password management controls can be provided by leveraging tools such as Multi- Factor Authentication provided by Skytap Cloud or connecting Skytap Cloud IAM to a corporate directory service.  Additionally, for password management on VMs instances, customers are responsible for establishing a policy for the servers that align with the applicable PCI requirements.   * <https://help.skytap.com/Password_Policy.html> |
| **8.2.3.b** Additional procedure for service provider assessments only: Review internal processes and customer/user documentation to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity:  • Require a minimum length of at least seven characters.  • Contain both numeric and alphabetic characters. |  |  | X |
| **8.2.4** Change user passwords/passphrases at least once every 90 days. |  |  |  |  |
| **8.2.4.a** For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require users to change passwords/passphrases at least once every 90 days. |  |  | X | Skytap maintains password policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing the creation of user accounts. Skytap Cloud IAM features include basic password management options for local accounts, such as password length and complexity requirements.  Additional password management controls can be provided by leveraging tools such as Multi- Factor Authentication (MFA) provided by Skytap Cloud or integrating with a corporate directory service.  Additionally, for password management on VMs instances, customers are responsible for establishing a policy for the servers that align with the applicable PCI requirements.   * <https://help.skytap.com/Password_Policy.html> |
| **8.2.4.b** Additional procedure for service provider assessments only: Review internal processes and customer/user documentation to verify that:  • Non-consumer customer user passwords/passphrases are required to change periodically; and   • Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change. |  |  | X |
| **8.2.5** Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used. |  |  |  |  |
| **8.2.5.a** For a sample of system components, obtain and inspect system configuration settings to verify that password/passphrases parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases. |  |  | X | Skytap maintains password policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing the creation of user accounts. Skytap Cloud IAM features include basic password management options for local accounts, such as password length and complexity requirements.  Additional password management controls can be provided by leveraging tools such as Multi- Factor Authentication (MFA) provided by Skytap Cloud or integrating with a corporate directory service.  Additionally, for password management on VMs instances, customers are responsible for establishing a policy for the servers that align with the applicable PCI requirements.   * <https://help.skytap.com/Password_Policy.html> |
| **8.2.5.b** Additional Procedure for service provider assessments only: Review internal processes and customer/user documentation to verify that new non-consumer customer user passwords/passphrases cannot be the same as the previous four passwords/passphrases. |  |  | X |
| **8.2.6** Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use. |  |  |  |  |
| **8.2.6** Examine password procedures and observe security personnel to verify that first-time passwords/passphrases for new users, and reset passwords/passphrases for existing users, are set to a unique value for each user and changed after first use. |  |  | X | Skytap maintains password policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing the creation of user accounts. Skytap Cloud IAM features include basic password management options for local accounts, such as password length and complexity requirements.  Additional password management controls can be provided by leveraging tools such as Multi- Factor Authentication (MFA) provided by Skytap Cloud or integrating with a corporate directory service.  Additionally, for password management on VMs instances, customers are responsible for establishing a policy for the servers that align with the applicable PCI requirements.   * <https://help.skytap.com/Password_Policy.html> * <https://help.skytap.com/users-create.html> * <https://help.skytap.com/Resending_a_User_Activation_Link.html> |
| **8.3** Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication  ***Note:*** *Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.* |  |  |  |  |
| **8.3.1** Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.   Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. |  |  |  |  |
| **8.3.1.a** Examine network and/or system configurations, as applicable, to verify multi-factor authentication is required for all non-console administrative access into the CDE. |  |  | X | Skytap requires multi-factor authentication for access to systems used to operate the Skytap Cloud platform.  Skytap Cloud provides an opt-in Multi-Factor Authentication   * <https://help.skytap.com/Sso_Policy.html>   Customers are responsible for maintaining two-factor authentication methods for access to their server instances running on customer managed VMs. In the case of the Skytap Cloud Management Console, two-factor authentication may not be required when on premise at the customer’s corporate offices if access is limited to the VPN access established between the Management Console environment and corporate offices depending on the architecture and segmentation model deployed for the CDE. Remote access to the Management Console from outside the corporate offices will require two- factor authentication. However, VMs will require some method of two-factor authentication for accessing and managing the VMs server instances.   * https://help.skytap.com/Sso\_Policy.html |
| **8.3.1.b** Observe a sample of administrator personnel login to the CDE and verify that at least two of the three authentication methods are used. |  |  | X |
| **8.3.2** Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity’s network. |  |  |  |  |
| **8.3.2.a** Examine system configurations for remote access servers and systems to verify multi-factor authentication is required for:  • All remote access by personnel, both user and administrator, and  • All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes). |  |  | X | Skytap requires multi-factor authentication for access to systems used to operate the Skytap Cloud platform.  Skytap Cloud provides an opt-in Multi-Factor Authentication (MFA) solution to support customers meeting the requirement for Multi-Factor authentication.  Customers are responsible for maintaining two-factor authentication methods for access to their server instances running on customer managed VMs. In the case of the Skytap Cloud Management Console, two-factor authentication may not be required when on premise at the customer’s corporate offices if access is limited to the VPN access established between the Management Console environment and corporate offices depending on the architecture and segmentation model deployed for the CDE. Remote access to the Management Console from outside the corporate offices will require two- factor authentication. However, VMs will require some method of two-factor authentication for accessing and managing the VMs server instances.  https://help.skytap.com/Sso\_Policy.html |
| **8.3.2.b** Observe a sample of personnel (for example, users and administrators) connecting remotely to the network and verify that at least two of the three authentication methods are used. |  |  | X |
| **8.4** Document and communicate authentication policies and procedures to all users including:  • Guidance on selecting strong authentication credentials.  • Guidance for how users should protect their authentication credentials.  • Instructions not to reuse previously used passwords.  • Instructions to change passwords if there is any suspicion the password could be compromised. |  |  |  |  |
| **8.4.a** Examineprocedures and interview personnel to verify that authentication policies and procedures are distributed to all users. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> * <https://help.skytap.com/users-delete-deactivate.html> |
| **8.4.b** Review authentication policies and procedures that are distributed to users and verify they include:  • Guidance on selecting strong authentication credentials.  • Guidance for how users should protect their authentication credentials.  • Instructions for users not to reuse previously used passwords.  • Instructions to change passwords if there is any suspicion the password could be compromised. |  |  | X |
| **8.4.c** Interview a sample of users to verify that they are familiar with authentication policies and procedures. |  |  | X |
| **8.5** Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:  • Generic user IDs are disabled or removed.  • Shared user IDs do not exist for system administration and other critical functions.  • Shared and generic user IDs are not used to administer any system components. |  |  |  |  |
| **8.5.a** For a sample of system components, examine user ID lists to verify the following:  • Generic user IDs are disabled or removed.  • Shared user IDs for system administration activities and other critical functions do not exist.  • Shared and generic user IDs are not used to administer any system components. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> * <https://help.skytap.com/users-delete-deactivate.html> |
| **8.5.b** Examine authentication policies and procedures to verify that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited. |  |  | X |
| **8.5.c** Interview system administrators to verify that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested. |  |  | X |
| **8.5.1** Additional requirement for service providers only:Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. *This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.* |  |  |  |  |
| **8.5.1** Additional procedure for service provider assessments only: Examine authentication policies and procedures and interview personnel to verify that different authentication credentials are used for access to each customer. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> * <https://help.skytap.com/users-delete-deactivate.html> |
| **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. |  |  |  |  |
| **8.6.a** Examine authentication policies and procedures to verify that procedures for using authentication mechanisms such as physical security tokens, smart cards, and certificates are defined and include:  • Authentication mechanisms are assigned to an individual account and not shared among multiple accounts.  • Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Skytap Cloud provides various mechanisms for controlling access to the services including Skytap Cloud IAM for integration with corporate directories and granular access controls to the Skytap Cloud Management Console. Customers are responsible for all access control of operating systems and applications running on customer managed VMs.   * <https://help.skytap.com/Access_Policy.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html> * <https://help.skytap.com/Security_Best_Practices.html> * <https://help.skytap.com/users-delete-deactivate.html>   Customers are responsible for maintaining two-factor authentication methods for access to their server instances. In the case of the Skytap Cloud Management Console, two-factor authentication may not be required when on premise at the customers’ corporate offices if access is limited to the VPN access established between the Management Console environment and corporate offices   * <https://help.skytap.com/Access_Policy.html#Browser_activation> * <https://help.skytap.com/users-create.html> * <https://help.skytap.com/User_Roles_and_Access_Permissions.html#Addition> |
| **8.6.b** Interview security personnel to verify authentication mechanisms are assigned to an account and not shared among multiple accounts. |  |  | X |
| **8.6.c** Examine system configuration settings and/or physical controls, as applicable, to verify that controls are implemented to ensure only the intended account can use that mechanism to gain access. |  |  | X |
| **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). |  |  |  |  |
| **8.7.a** Review database and application configuration settings and verify that all users are authenticated prior to access. |  | X |  | Customers are responsible for managing access to customer managed VMs. This includes access controls to all applications installed by the customer, including databases.  No Skytap databases contain cardholder data. Skytap does not have access to databases on customer managed VMs. |
| **8.7.b** Examine database and application configuration settings to verify thatall user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures). |  | X |  |
| **8.7.c** Examine database access control settings and database application configuration settings to verify that user direct access to or queries of databases are restricted to database administrators. |  | X |  |
| **8.7.d** Examine database access control settings, database application configuration settings, and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes). |  | X |  |
| **8.8** Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties. |  |  |  |  |
| **8.8** Examine documentation and interview personnel to verify that security policies and operational procedures for identification and authentication are:  • Documented,   • In use, and   • Known to all affected parties. |  |  | X | Skytap maintains identity, authentication, and access policies and procedures covering systems used to operate the Skytap Cloud platform. These policies and procedures are document, in use, and known to all affected parties.  Customers are responsible for managing access to customer managed VMs and Skytap VPN. Customers are responsible for ensuring that their policies and procedures for identification and authentication are documented and known to all affected parties. |
| **9.1** Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. |  |  |  |  |
| **9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment.  • Verify that access is controlled with badge readers or other devices including authorized badges and lock and key.   • Observe a system administrator’s attempt to log into consoles for randomly selected systems in the cardholder data environment and verify that they are “locked” to prevent unauthorized use. | X |  |  | Skytap Cloud maintains the physical security and media handling controls for Skytap Cloud data centers supporting the services included in the assessment. |
| **9.1.1** Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. ***Note:*** *“Sensitive areas” refers to any data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.* |  |  |  |  |
| **9.1.1.a** Verify that either video cameras or access control mechanisms (or both) are in place to monitor the entry/exit points to sensitive areas. | X |  |  | Skytap maintains the physical security and media handling controls for Skytap Cloud data centers supporting the services included in the assessment. |
| **9.1.1.b** Verify that either video cameras or access control mechanisms (or both) are protected from tampering or disabling. | X |  |  |
| **9.1.1.c** Verify that data from video cameras and/or access control mechanisms is reviewed, and that data is stored for at least three months. | X |  |  |
| **9.1.2** Implement physical and/or logical controls to restrict access to publicly accessible network jacks. *For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.* |  |  |  |  |
| **9.1.2** Interview responsible personnel and observe locations of publicly accessible network jacks to verify that physical and/or logical controls are in place to restrict access to publicly-accessible network jacks. | X |  |  | Skytap maintains the physical security and media handling controls for Skytap Cloud data centers supporting the services included in the assessment. |
| **9.1.3** Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines. |  |  |  |  |
| **9.1.3** Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted. | X |  |  | Skytap maintains the physical security and media handling controls for Skytap Cloud data centers supporting the services included in the assessment. |
| **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). |  |  |  |  |
| **9.2.a** Review documented processes to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors.  Verify procedures include the following:  • Identifying onsite personnel and visitors (for example, assigning badges),  • Changing access requirements, and  • Revoking terminated onsite personnel and expired visitor identification (such as ID badges). | X |  |  | Skytap maintains the physical security and media handling controls for Skytap Cloud data centers supporting the services included in the assessment. |
| **9.2.b** Examine identification methods (such as ID badges) and observe processes for identifying and distinguishing between onsite personnel and visitors to verify that:  • Visitors are clearly identified, and   • It is easy to distinguish between onsite personnel and visitors. | X |  |  |
| **9.2.c** Verify that access to the identification process (such as a badge system) is limited to authorized personnel. | X |  |  |
| **9.3** Control physical access for onsite personnel to sensitive areas as follows:  • Access must be authorized and based on individual job function.  • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled. |  |  |  |  |
| **9.3.a** For a sample of onsite personnel with physical access to sensitive areas, interview responsible personnel and observe access control lists to verify that:  • Access to the sensitive area is authorized.   • Access is required for the individual’s job function. | X |  |  | Skytap maintains the physical security and media handling controls for Skytap Cloud data centers supporting the services included in the assessment. |
| **9.3.b** Observe personnel accessing sensitive areas to verify that all personnel are authorized before being granted access. | X |  |  |
| **9.3.c** Select a sample of recently terminated employees and review access control lists to verify the personnel do not have physical access to sensitive areas. | X |  |  |
| **9.4** Implement procedures to identify and authorize visitors.  Procedures should include the following: |  |  |  |  |
| **9.4.1** Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained. |  |  |  |  |
| **9.4.1.a** Observe procedures and interview personnel to verify that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained. | X |  |  | Skytap maintains the physical security and media handling controls for Skytap Cloud data centers supporting the services included in the assessment. |
| **9.4.1.b** Observe the use of visitor badges or other identification to verify that a physical token badge does not permit unescorted access to physical areas where cardholder data is processed or maintained. | X |  |  |
| **9.4.2** Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel. |  |  |  |  |
| **9.4.2.a** Observe people within the facility to verify the use of visitor badges or other identification, and that visitors are easily distinguishable from onsite personnel. | X |  |  | Skytap maintains the physical security and media handling controls for Skytap Cloud data centers supporting the services included in the assessment. |
| **9.4.2.b** Verify that visitor badges or other identification expire. | X |  |  |
| **9.4.3** Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration. |  |  |  |  |
| **9.4.3** Observe visitors leaving the facility to verify visitors are asked to surrender their badge or other identification upon departure or expiration. | X |  |  | Skytap maintains the physical security and media handling controls for Skytap Cloud data centers supporting the services included in the assessment. |
| **9.4.4** A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted.  Document the visitor’s name, the firm represented, and the onsite personnel authorizing physical access on the log.  Retain this log for a minimum of three months, unless otherwise restricted by law. |  |  |  |  |
| **9.4.4.a** Verify that a visitor log is in use to record physical access to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. | X |  |  | Skytap maintains the physical security and media handling controls for Skytap Cloud data centers supporting the services included in the assessment. |
| **9.4.4.b** Verify that the log contains:  • The visitor’s name,   • The firm represented, and   • The onsite personnel authorizing physical access. | X |  |  |
| **9.4.4.c** Verify that the log is retained for at least three months. | X |  |  |
| **9.5** Physically secure all media. |  |  |  |  |
| **9.5** Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes). |  |  | X | Skytap maintains the physical security and media handling controls for Skytap Cloud data centers supporting the services included in the assessment.  Customers are responsible for backup, compliance and destruction of media outside of the Skytap Cloud environment.  Skytap does not store customer data on removable media. |
| **9.5.1** Store media backups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location’s security at least annually. |  |  |  |  |
| **9.5.1.** Verify that the storage location security is reviewed at least annually to confirm that backup media storage is secure. |  |  | X | Skytap maintains the physical security and media handling controls for Skytap Cloud data centers supporting the services included in the assessment.  Customers are responsible for backup, compliance and destruction of media outside of the Skytap Cloud environment. |
| **9.6** Maintain strict control over the internal or external distribution of any kind of media, including the following: |  |  |  |  |
| **9.6** Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals. |  |  | X | Skytap maintains policies and procedures covering distribution of media used to operate the Skytap Cloud platform.  Customers are responsible for backup, compliance and destruction of media outside of the Skytap Cloud environment. |
| **9.6.1** Classify media so the sensitivity of the data can be determined. |  |  |  |  |
| **9.6.1** Verify that all media is classified so the sensitivity of the data can be determined. |  |  | X | Skytap maintains policies and procedures covering classification of media used to operate the Skytap Cloud platform.  Customers are responsible for backup, compliance and destruction of media outside of the Skytap Cloud environment. |
| **9.6.2** Send the media by secured courier or other delivery method that can be accurately tracked. |  |  |  |  |
| **9.6.2.a** Interview personnel and examine records to verify that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked. |  |  | X | Skytap maintains policies and procedures covering handling of media used to operate the Skytap Cloud platform.  Customers are responsible for backup, compliance and destruction of media outside of the Skytap Cloud environment. |
| **9.6.2.b** Select a recent sample of several days of offsite tracking logs for all media, and verify tracking details are documented. |  |  | X |
| **9.6.3** Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals). |  |  |  |  |
| **9.6.3** Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals). |  |  | X | Skytap maintains policies and procedures covering handling of media used to operate the Skytap Cloud platform.  Customers are responsible for backup, compliance and destruction of media outside of the Skytap Cloud environment. |
| **9.7** Maintain strict control over the storage and accessibility of media. |  |  |  |  |
| **9.7** Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories. |  |  | X | Skytap maintains policies and procedures covering handling of media used to operate the Skytap Cloud platform.  Customers are responsible for backup, compliance and destruction of media outside of the Skytap Cloud environment. |
| **9.7.1** Properly maintain inventory logs of all media and conduct media inventories at least annually. |  |  |  |  |
| **9.7.1** Review media inventory logs to verify that logs are maintained and media inventories are performed at least annually. |  |  | X | Skytap maintains policies and procedures covering handling of media used to operate the Skytap Cloud platform.  Customers are responsible for backup, compliance and destruction of media outside of the Skytap Cloud environment. |
| **9.8** Destroy media when it is no longer needed for business or legal reasons as follows: |  |  |  |  |
| **9.8** Examine the periodic media destruction policy and verify that it covers all media and defines requirements for the following:  • Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.  • Storage containers used for materials that are to be destroyed must be secured.  • Cardholder data on electronic media must be rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media). |  |  | X | Skytap maintains policies and procedures covering handling of media used to operate the Skytap Cloud platform.  Customers are responsible for backup, compliance and destruction of media outside of the Skytap Cloud environment. |
| **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. |  |  |  |  |
| **9.8.1.a** Interview personnel and examine procedures to verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. |  |  | X | Skytap maintains policies and procedures covering handling of media used to operate the Skytap Cloud platform.  Customers are responsible for backup, compliance and destruction of media outside of the Skytap Cloud environment. |
| **9.8.1.b** Examine storage containers used for materials that contain information to be destroyed to verify that the containers are secured. |  |  | X |
| **9.8.2** Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed. |  |  |  |  |
| **9.8.2** Verify that cardholder data on electronic media is rendered unrecoverable (e.g. via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media). |  |  | X | Skytap maintains policies and procedures covering handling of media used to operate the Skytap Cloud platform.  Customers are responsible for backup, compliance and destruction of media outside of the Skytap Cloud environment.  Skytap does not have direct access to any cardholder data. |
| **9.9** Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. ***Note:*** *These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.* |  |  |  |  |
| **9.9** Examine documented policies and procedures to verify they include:  • Maintaining a list of devices.   • Periodically inspecting devices to look for tampering or substitution.   • Training personnel to be aware of suspicious behavior and to report tampering or substitution of POS devices. |  | X |  | Customer is responsible for any devices that capture payment card data via direct physical interaction with the card. |
| **9.9.1.a** Examine the list of devices to verify it includes:  • Make, model of device.   • Location of device (for example, the address of the site or facility where the device is located).   • Device serial number or other method of unique identification. |  | X |  |
| **9.9.1.b** Select a sample of devices from the list and observe devices and device locations to verify that the list is accurate and up-to-date. |  | X |  |
| **9.9.1.c** Interview personnel to verify the list of devices is updated when devices are added, relocated, decommissioned, etc. |  | X |  |
| **9.9.2** Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).  **Note:** Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings. |  |  |  |  |
| **9.9.2.a** Examine documented procedures to verify processes are defined to include the following:  • Procedures for inspecting devices.  • Frequency of inspections. |  | X |  | Customer is responsible for any devices that capture payment card data via direct physical interaction with the card. |
| **9.9.2.b** Interview responsible personnel and observe inspection processes to verify:  • Personnel are aware of procedures for inspecting devices.   • All devices are periodically inspected for evidence of tampering and substitution. |  | X |  |
| **9.9.3** Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following:  • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.  • Do not install, replace, or return devices without verification.   • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).  • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). |  |  |  |  |
| **9.9.3.a** Review training materials for personnel at point-of-sale locations to verify it includes training in the following:  • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.  • Not to install, replace, or return devices without verification.   • Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).  • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). |  | X |  | Customers are responsible for providing training to ensure appropriate personnel are aware of any tampering or replacement of point-of-sale devices or abnormalities of point-of-sale locations. |
| **9.9.3.b** Interview a sample of personnel at point-of-sale locations to verify they have received training and are aware of the procedures for the following:   • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.  • Not to install, replace, or return devices without verification.   • Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).  • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). |  | X |  |
| **9.10** Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties. |  |  |  |  |
| **9.10** Examine documentation and interview personnel to verify that security policies and operational procedures for restricting physical access to cardholder data are:  • Documented,   • In use, and   • Known to all affected parties. |  |  | X | Skytap maintains policies and procedures for securing physical access to the CDE. These policies and procedures are documented, in use, and known to all affected parties.  Customers are responsible for ensuring that their policies and procedures for restricting physical access to cardholder data are documented and known to all affected parties.  Skytap does not have direct access to any cardholder data. |
| **10.1** Implement audit trails to link all access to system components to each individual user. |  |  |  |  |
| **10.1** Verify, through observation and interviewing the system administrator, that:   • Audit trails are enabled and active for system components.  • Access to system components is linked to individual users. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customers are responsible for reviewing audit logs of customer activity on Skytap Cloud Console and Skytap Cloud API. These logs may be accessed by customers via Skytap Cloud Log Management tools.   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing audit logging for systems and applications running on customer managed VMs. |
| **10.2** Implement automated audit trails for all system components to reconstruct the following events: |  |  |  |  |
| **10.2** Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following: |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customers are responsible for reviewing audit logs of customer activity on Skytap Cloud Console and Skytap Cloud API. These logs may be accessed by customers via Skytap Cloud Log Management tools.   * <https://help.skytap.com/Auditing.html> * Customers are responsible for implementing audit logging for systems and applications running on customer managed VMs. |
| **10.2.1** All individual user accesses to cardholder data. |  |  |  |  |
| **10.2.1** Verify all individual access to cardholder data is logged. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customers are responsible for reviewing audit logs of customer activity on Skytap Cloud Console and Skytap Cloud API. These logs may be accessed by customers via Skytap Cloud Log Management tools.   * <https://help.skytap.com/Auditing.html> * Customers are responsible for implementing audit logging for systems and applications running on customer managed VMs. |
| **10.2.2** All actions taken by any individual with root or administrative privileges. |  |  |  |  |
| **10.2.2** Verify all actions taken by any individual with root or administrative privileges are logged. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customers are responsible for reviewing audit logs of customer activity on Skytap Cloud Console and Skytap Cloud API. These logs may be accessed by customers via Skytap Cloud Log Management tools.   * <https://help.skytap.com/Auditing.html> * Customers are responsible for implementing audit logging for systems and applications running on customer managed VMs. |
| **10.2.3** Access to all audit trails. |  |  |  |  |
| **10.2.3** Verify access to all audit trails is logged. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customers are responsible for reviewing audit logs of customer activity on Skytap Cloud Console and Skytap Cloud API. These logs may be accessed by customers via Skytap Cloud Log Management tools.   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing audit logging for systems and applications running on customer managed VMs. |
| **10.2.4** Invalid logical access attempts. |  |  |  |  |
| **10.2.4** Verify invalid logical access attempts are logged. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customers are responsible for reviewing audit logs of customer activity on Skytap Cloud Console and Skytap Cloud API. These logs may be accessed by customers via Skytap Cloud Log Management tools.   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing audit logging for systems and applications running on customer managed VMs. |
| **10.2.5** Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges. |  |  |  |  |
| **10.2.5.a** Verify use of identification and authentication mechanisms is logged. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customers are responsible for reviewing audit logs of customer activity on Skytap Cloud Console and Skytap Cloud API. These logs may be accessed by customers via Skytap Cloud Log Management tools.   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing audit logging for systems and applications running on customer managed VMs. |
| **10.2.5.b** Verify all elevation of privileges is logged. |  |  |
| **10.2.5.c** Verify all changes, additions, or deletions to any account with root or administrative privileges are logged. |  |  |
| **10.2.6** Initialization, stopping, or pausing of the audit logs. |  |  |  |  |
| **10.2.6** Verify the following are logged:  • Initialization of audit logs.  • Stopping or pausing of audit logs. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customers are responsible for reviewing audit logs of customer activity on Skytap Cloud Console and Skytap Cloud API. These logs may be accessed by customers via Skytap Cloud Log Management tools.   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing audit logging for systems and applications running on customer managed VMs. |
| **10.2.7** Creation and deletion of system-level objects. |  |  |  |  |
| **10.2.7** Verify creation and deletion of system level objects are logged. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customers are responsible for reviewing audit logs of customer activity on Skytap Cloud Console and Skytap Cloud API. These logs may be accessed by customers via Skytap Cloud Log Management tools.   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing audit logging for systems and applications running on customer managed VMs. |
| **10.3** Record at least the following audit trail entries for all system components for each event: |  |  |  |  |
| **10.3** Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following: |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customers are responsible for reviewing audit logs of customer activity on Skytap Cloud Console and Skytap Cloud API. These logs may be accessed by customers via Skytap Cloud Log Management tools.   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing audit logging for systems and applications running on customer managed VMs. |
| **10.3.1** User identification |  |  |  |  |
| **10.3.1** Verify user identification is included in log entries. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customers are responsible for reviewing audit logs of customer activity on Skytap Cloud Console and Skytap Cloud API. These logs may be accessed by customers via Skytap Cloud Log Management tools.   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing audit logging for systems and applications running on customer managed VMs. |
| **10.3.2** Type of event |  |  |  |  |
| **10.3.2** Verify type of event is included in log entries. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customers are responsible for reviewing audit logs of customer activity on Skytap Cloud Console and Skytap Cloud API. These logs may be accessed by customers via Skytap Cloud Log Management tools.   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing audit logging for systems and applications running on customer managed VMs. |
| **10.3.3** Date and time |  |  |  |  |
| **10.3.3** Verify date and time stamp is included in log entries. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customers are responsible for reviewing audit logs of customer activity on Skytap Cloud Console and Skytap Cloud API. These logs may be accessed by customers via Skytap Cloud Log Management tools.   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing audit logging for systems and applications running on customer managed VMs. |
| **10.3.4** Success or failure indication |  |  |  |  |
| **10.3.4** Verify success or failure indication is included in log entries. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customers are responsible for reviewing audit logs of customer activity on Skytap Cloud Console and Skytap Cloud API. These logs may be accessed by customers via Skytap Cloud Log Management tools.   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing audit logging for systems and applications running on customer managed VMs. |
| **10.3.5** Origination of event |  |  |  |  |
| **10.3.5** Verify origination of event is included in log entries. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customers are responsible for reviewing audit logs of customer activity on Skytap Cloud Console and Skytap Cloud API. These logs may be accessed by customers via Skytap Cloud Log Management tools.   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing audit logging for systems and applications running on customer managed VMs. |
| **10.3.6** Identity or name of affected data, system component, or resource |  |  |  |  |
| **10.3.6** Verify identity or name of affected data, system component, or resources is included in log entries. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customers are responsible for reviewing audit logs of customer activity on Skytap Cloud Console and Skytap Cloud API. These logs may be accessed by customers via Skytap Cloud Log Management tools.   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing audit logging for systems and applications running on customer managed VMs. |
| **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.  ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).* |  |  |  |  |
| **10.4** Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2. |  |  | X | Skytap maintains time-synchronization on all systems used to operate the Skytap Cloud platform.  Customers are responsible for implementing time-synchronization on customer managed VMs. See instructions in link below for help with implementing time-synchronization on customer managed VMs.   * <https://help.skytap.com/editing-vm-bios-time-sync.html> |
| **10.4.1** Critical systems have the correct and consistent time. |  |  |  |  |
| **10.4.1.a** Examine the process for acquiring, distributing and storing the correct time within the organization to verify that:   • Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.  • Where there is more than one designated time server, the time servers peer with one another to keep accurate time.  • Systems receive time information only from designated central time server(s). |  |  | X | Skytap maintains time-synchronization on all systems used to operate the Skytap Cloud platform.  Customers are responsible for implementing time-synchronization on customer managed VMs. See instructions in link below for help with implementing time-synchronization on customer managed VMs.   * <https://help.skytap.com/editing-vm-bios-time-sync.html> |
| **10.4.1.b** Observe the time-related system-parameter settings for a sample of system components to verify:  • Only the designated central time server(s) receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.  • Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time.   • Systems receive time only from designated central time server(s). |  |  | X |
| **10.4.2** Time data is protected. |  |  |  |  |
| **10.4.2.a** Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data. |  |  | X | Skytap maintains time-synchronization on all systems used to operate the Skytap Cloud platform.  Customers are responsible for implementing time-synchronization on customer managed VMs. See instructions in link below for help with implementing time-synchronization on customer managed VMs.  <https://help.skytap.com/editing-vm-bios-time-sync.html> |
| **10.4.2.b** Examine system configurations, time synchronization settings and logs, and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed. |  |  |
| **10.4.3** Time settings are received from industry-accepted time sources. |  |  |  |  |
| **10.4.3** Examine systems configurations to verify that the time server(s) accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers). |  |  | X | Skytap maintains time-synchronization on all systems used to operate the Skytap Cloud platform.  Customers are responsible for implementing time-synchronization on customer managed VMs. See instructions in link below for help with implementing time-synchronization on customer managed VMs.  <https://help.skytap.com/editing-vm-bios-time-sync.html> |
| **10.5** Secure audit trails so they cannot be altered. |  |  |  |  |
| **10.5** Interview system administrators and examine system configurations and permissions to verify that audit trails are secured so that they cannot be altered as follows: |  |  |  |  |
| **10.5.1** Limit viewing of audit trails to those with a job-related need. |  |  |  |  |
| **10.5.1** Only individuals who have a job-related need can view audit trail files. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customer may access audit logs of customer activity via Skytap Cloud Log Management tools. Customers are responsible for assigning appropriate access to Log management tool   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing and securing audit logging for systems and applications running on customer managed VMs. |
| **10.5.2** Protect audit trail files from unauthorized modifications. |  |  |  |  |
| **10.5.2** Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customer may access audit logs of customer activity via Skytap Cloud Log Management tools. Customers are responsible for assigning appropriate access to Log management tool   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing and securing audit logging for systems and applications running on customer managed VMs. |
| **10.5.3** Promptly back up audit trail files to a centralized log server or media that is difficult to alter. |  |  |  |  |
| **10.5.3** Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customer may access audit logs of customer activity via Skytap Cloud Log Management tools. Customers are responsible for assigning appropriate access to Log management tool   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing and securing audit logging for systems and applications running on customer managed VMs. |
| **10.5.4** Write logs for external-facing technologies onto a secure, centralized, internal log server or media device. |  |  |  |  |
| **10.5.4** Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customer may access audit logs of customer activity via Skytap Cloud Log Management tools. Customers are responsible for assigning appropriate access to Log management tool   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing and securing audit logging for systems and applications running on customer managed VMs. |
| **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). |  |  |  |  |
| **10.5.5** Examine system settings, monitored files, and results from monitoring activities to verify the use of file-integrity monitoring or change-detection software on logs. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customer may access audit logs of customer activity via Skytap Cloud Log Management tools. Customers are responsible for assigning appropriate access to Log management tool   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing and securing audit logging for systems and applications running on customer managed VMs. |
| **10.6** Review logs and security events for all system components to identify anomalies or suspicious activity. ***Note:*** *Log harvesting, parsing, and alerting tools may be used to meet this Requirement.* |  |  |  |  |
| **10.6** Perform the following: |  |  |  |  |
| **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.). |  |  |  |  |
| **10.6.1.a** Examine security policies and procedures to verify that procedures are defined for, reviewing the following at least daily, either manually or via log tools:  • 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 | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customer may access audit logs of customer activity via Skytap Cloud Log Management tools. Customers are responsible for assigning appropriate access to Log management tool   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing and securing audit logging for systems and applications running on customer managed VMs. |
| **10.6.1.b** Observe processes and interview personnel to verify that the following are reviewed 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 |
| **10.6.2** Review logs of all other system components periodically based on the organization’s policies and risk management strategy, as determined by the organization’s annual risk assessment. |  |  |  |  |
| **10.6.2.a** Examine security policies and procedures to verify that procedures are defined for reviewing logs of all other system components periodically—either manually or via log tools—based on the organization’s policies and risk management strategy. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customer may access audit logs of customer activity via Skytap Cloud Log Management tools. Customers are responsible for assigning appropriate access to Log management tool   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing and securing audit logging for systems and applications running on customer managed VMs. |
| **10.6.2.b** Examine the organization’s risk assessment documentation and interview personnel to verify that reviews are performed in accordance with organization’s policies and risk management strategy. |  |  |
| **10.6.3** Follow up exceptions and anomalies identified during the review process. |  |  |  |  |
| **10.6.3.a** Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customer may access audit logs of customer activity via Skytap Cloud Log Management tools. Customers are responsible for assigning appropriate access to Log management tool   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing and securing audit logging for systems and applications running on customer managed VMs. |
| **10.6.3.b** Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed. |  |  |
| **10.7** Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). |  |  |  |  |
| **10.7.a** Examine security policies and procedures to verify that they define the following:  • Audit log retention policies.  • Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online. |  |  | X | Skytap maintains audit logging for all systems used to operate the Skytap Cloud platform.  Customer may access audit logs of customer activity via Skytap Cloud Log Management tools. Customers are responsible for assigning appropriate access to Log management tool   * <https://help.skytap.com/Auditing.html>   Customers are responsible for implementing and securing audit logging for systems and applications running on customer managed VMs. |
| **10.7.b** Interview personnel and examine audit logs to verify that audit logs are retained for at least one year. |  |  |
| **10.7.c** Interview personnel and observe processes to verify that at least the last three months’ logs are 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)   Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. |  |  |  |  |
| **10.8.a** Examine documented policies and procedures to verify that processes are defined 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 | Skytap maintains procedures for timely detection and reporting of failures for critical security control systems used to operate the Skytap Cloud platform.  Customers are responsible for ensuring procedures are implemented for timely detection and reporting of failures of critical security control systems running on customer managed VMs. |
| **10.8.b** Examine detection and alerting processes and interview personnel to verify that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert. |  |  |
| **10.8.1** Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:   • Restoring security functions   • Identifying and documenting the duration (date and time start to end) of the security failure   • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause   • Identifying and addressing any security issues that arose during the failure   • Performing a risk assessment to determine whether further actions are required as a result of the security failure   • Implementing controls to prevent cause of failure from reoccurring   • Resuming monitoring of security controls   Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. |  |  |  |  |
| **10.8.1.a** Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to respond to a security control failure, and include:   • Restoring security functions   • Identifying and documenting the duration (date and time start to end) of the security failure   • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause   • Identifying and addressing any security issues that arose during the failure   • Performing a risk assessment to determine whether further actions are required as a result of the security failure   • Implementing controls to prevent cause of failure from reoccurring   • Resuming monitoring of security controls |  |  | X | Skytap maintains incident response policies and procedures for critical security controls. These policies and procedures include identifying and documenting impact, restoring critical security functions, conducting root cause analysis, and incorporating system improvements to prevent similar failures in the future.  Customers are responsible for policies and procedures to address failures of critical security control systems running on customer managed VMs and security notices provided to customers by Skytap. |
| **10.8.1.b** Examine records to verify that security control failures are documented to include:   • Identification of cause(s) of the failure, including root cause   • Duration (date and time start and end) of the security failure   • Details of the remediation required to address the root cause |  |  |
| **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. |  |  |  |  |
| **10.9** Examine documentation and interview personnel to verify 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 | Skytap maintains policies and procedures for monitoring access to network resources used to operate the Skytap Cloud platform. These policies and procedures are documented, in use, and known to all affected parties.  Customers are responsible for ensuring that their policies and procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.  Skytap does not have any direct access to cardholder data. |
| **11.1** Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. ***Note:*** *Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.* Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices. |  |  |  |  |
| **11.1.a** Examine policies and procedures to verify processes are defined for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis. | X |  |  | Skytap maintains policies and procedures for ensuring that only authorized wireless access points are present in the Skytap Cloud infrastructure. |
| **11.1.b** Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:  • WLAN cards inserted into system components.  • Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.).  • Wireless devices attached to a network port or network device. | X |  |  |
| **11.1.c** If wireless scanning is utilized, examine output from recent wireless scans to verify that:   • Authorized and unauthorized wireless access points are identified, and  • The scan is performed at least quarterly for all system components and facilities. | X |  |  |
| **11.1.d** If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to notify personnel. | X |  |  |
| **11.1.1** Maintain an inventory of authorized wireless access points including a documented business justification. |  |  |  |  |
| **11.1.1** Examine documented records to verify that an inventory of authorized wireless access points is maintained and a business justification is documented for all authorized wireless access points. | X |  |  | Skytap maintains policies and procedures for ensuring that only authorized wireless access points are present in the Skytap Cloud infrastructure. This includes an inventory and business justification for all authorized wireless access points. |
| **11.1.2** Implement incident response procedures in the event unauthorized wireless access points are detected. |  |  |  |  |
| **11.1.2.a** Examine the organization’s incident response plan (Requirement 12.10) to verify it defines and requires a response in the event that an unauthorized wireless access point is detected. | X |  |  | Skytap maintains policies and procedures for ensuring that only authorized wireless access points are present in the Skytap Cloud infrastructure. This includes incident response procedures carried out upon detection of any unauthorized wireless access points. |
| **11.1.2.b** Interview responsible personnel and/or inspect recent wireless scans and related responses to verify action is taken when unauthorized wireless access points are found. | X |  |  |
| **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). ***Note:*** *Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.  For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.* |  |  |  |  |
| **11.2** Examine scan reports and supporting documentation to verify that internal and external vulnerability scans are performed as follows: |  |  |  |  |
| **11.2.1** Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all “high-risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel. |  |  |  |  |
| **11.2.1.a** Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. |  |  | X | Skytap conducts vulnerability scanning of systems, infrastructure, and applications used to operate the Skytap Cloud platform.  Customers are responsible for vulnerability scanning, of operating systems and applications running on customer managed VMs. Customer vulnerability scans should include only customer managed VMs and IP addresses allocated to customer, not Skytap Cloud services endpoints. Skytap Cloud services endpoints are included in Skytap’s vulnerability scans of the Skytap Cloud platform. |
| **11.2.1.b** Review the scan reports and verify that all “high-risk” vulnerabilities are addressed and the scan process includes rescans to verify that the “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. |  |  | X |
| **11.2.1.c** Interview personnel to verify that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). |  |  | X |
| **11.2.2** Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).  Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.* |  |  |  |  |
| **11.2.2.a** Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly external vulnerability scans occurred in the most recent 12-month period. |  |  | X | Skytap conducts vulnerability scanning of systems, infrastructure, and applications used to operate the Skytap Cloud platform.  Customers are responsible for vulnerability scanning, of operating systems and applications running on customer managed VMs. Customer vulnerability scans should include only customer managed VMs and IP addresses allocated to customer, not Skytap Cloud services endpoints. Skytap Cloud services endpoints are included in Skytap’s vulnerability scans of the Skytap Cloud platform. |
| **11.2.2.b** Review the results of each quarterly scan and rescan to verify that the ASV Program Guide requirements for a passing scan have been met (for example, no vulnerabilities rated 4.0 or higher by the CVSS, no automatic failures). |  |  | X |
| **11.2.2.c** Review the scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV). |  |  | X |
| **11.2.3** Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel. |  |  |  |  |
| **11.2.3.a** Inspect and correlate change control documentation and scan reports to verify that system components subject to any significant change were scanned. |  |  | X | Skytap conducts vulnerability scanning of systems, infrastructure, and applications used to operate the Skytap Cloud platform.  Customers are responsible for vulnerability scanning, of operating systems and applications running on customer managed VMs. Customer vulnerability scans should include only customer managed VMs and IP addresses allocated to customer, not Skytap Cloud services endpoints. Skytap Cloud services endpoints are included in Skytap’s vulnerability scans of the Skytap Cloud platform. |
| **11.2.3.b** Review scan reports and verify that the scan process includes rescans until:   • For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS.   • For internal scans, all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. |  |  | X |
| **11.2.3.c** Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). |  |  | X |
| **11.3** Implement a methodology for penetration testing that includes at least the following:  • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115).  • Includes coverage for the entire CDE perimeter and critical systems.  • Includes testing from both inside and outside of the network.  • Includes testing to validate any segmentation and scope reduction controls.  • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5.  • Defines network-layer penetration tests to include components that support network functions as well as operating systems.  • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months.   • Specifies retention of penetration testing results and remediation activities results. |  |  |  |  |
| **11.3** Examine penetration-testing methodology and interview responsible personnel to verify a methodology is implemented and includes at least the following:  • Is based on industry-accepted penetration testing approaches.  • Includes coverage for the entire CDE perimeter and critical systems.  • Includes testing from both inside and outside the network.  • Includes testing to validate any segmentation and scope reduction controls.  • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5.  • Defines network-layer penetration tests to include components that support network functions as well as operating systems.  • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months.  • Specifies retention of penetration testing results and remediation activities results. |  |  | X | Skytap conducts penetration testing of systems, infrastructure, and applications used to operate the Skytap Cloud platform.  Customers are responsible for penetration testing, of operating systems and applications running on customer managed VMs. Customer penetration testing should include only customer managed VMs and IP addresses allocated to customer, not Skytap Cloud services endpoints. Skytap Cloud services endpoints are included in Skytap’s penetration testing of the Skytap Cloud platform. |
| **11.3.1** Perform ***external*** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). |  |  |  |  |
| **11.3.1.a** Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed as follows:  • Per the defined methodology  • At least annually   • After any significant changes to the environment |  |  | X | Skytap conducts penetration testing of systems, infrastructure, and applications used to operate the Skytap Cloud platform.  Customers are responsible for penetration testing, of operating systems and applications running on customer managed VMs. Customer penetration testing should include only customer managed VMs and IP addresses allocated to customer, not Skytap Cloud services endpoints. Skytap Cloud services endpoints are included in Skytap’s penetration testing of the Skytap Cloud platform. |
| **11.3.1.b** Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). |  |  | X |
| **11.3.2** Perform **internal** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). |  |  |  |  |
| **11.3.2.a** Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed as follows:  • Per the defined methodology  • At least annually   • After any significant changes to the environment |  |  | X | Skytap conducts penetration testing of systems, infrastructure, and applications used to operate the Skytap Cloud platform.  Customers are responsible for penetration testing, of operating systems and applications running on customer managed VMs. Customer penetration testing should include only customer managed VMs and IP addresses allocated to customer, not Skytap Cloud services endpoints. Skytap Cloud services endpoints are included in Skytap’s penetration testing of the Skytap Cloud platform. |
| **11.3.2.b** Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). |  |  | X |
| **11.3.3** Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections. |  |  |  |  |
| **11.3.3** Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected. |  |  | X | Skytap conducts penetration testing of systems, infrastructure, and applications used to operate the Skytap Cloud platform.  Customers are responsible for penetration testing, of operating systems and applications running on customer managed VMs. Customer penetration testing should include only customer managed VMs and IP addresses allocated to customer, not Skytap Cloud services endpoints. Skytap Cloud services endpoints are included in Skytap’s penetration testing of the Skytap Cloud platform. |
| **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. |  |  |  |  |
| **11.3.4.a** Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE. |  |  | X | Skytap conducts testing of network segmentation controls for infrastructure used to operate the Skytap Cloud platform.  Customers are responsible for testing segmentation testing of any infrastructure and applications running on customer managed VMs inside of the customer environment. |
| **11.3.4.b** Examine the results from the most recent penetration test to verify that:  • Penetration testing to verify segmentation controls is performed at least annually and after any changes to segmentation controls/methods.  • The penetration testing covers all segmentation controls/methods in use.  • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. |  |  | X |
| **11.3.4.c** Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). |  |  | X |
| **11.3.4.1** Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* |  |  |  |  |
| **11.3.4.1.a** Examine the results from the most recent penetration test to verify that:   • Penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods.   • The penetration testing covers all segmentation controls/methods in use.   • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. |  |  | X | Skytap conducts testing of network segmentation controls for infrastructure used to operate the Skytap Cloud platform.  Customers are responsible for testing segmentation testing of any infrastructure and applications running on customer managed VMs inside of the customer environment. |
| **11.3.4.1.b** Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). |  |  | X |
| **11.4** Use intrusion-detection systems 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. |  |  |  |  |
| **11.4.a** Examine system configurations and network diagrams to verify that techniques (such as intrusion-detection systems and/or intrusion-prevention systems) are in place to monitor all traffic:   • At the perimeter of the cardholder data environment.  • At critical points in the cardholder data environment. |  |  | X | Skytap maintains intrusion-detection systems covering infrastructure, systems, and applications used to operate the Skytap Cloud platform.  Customers are responsible for implementing intrusion-detection systems for any network segments, systems, and applications running on customer managed. |
| **11.4.b** Examine system configurations and interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises. |  |  | X |
| **11.4.c** Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection, and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection. |  |  | X |
| **11.5** Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.  ***Note:*** *For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).* |  |  |  |  |
| **11.5.a** Verify the use of a change-detection mechanism by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored:  • System executables  • Application executables  • Configuration and parameter files  • Centrally stored, historical or archived, log and audit files  • Additional critical files determined by entity (i.e., through risk assessment or other means) |  |  | X | Skytap maintains file integrity monitoring on systems used to operate the Skytap Cloud platform.  Customers are responsible for file integrity monitoring on customer managed VMs. |
| **11.5.b** Verify the mechanism is configured to alert personnel to unauthorized modification (including changes, additions and deletions) of critical files, and to perform critical file comparisons at least weekly. |  |  | X |
| **11.5.1** Implement a process to respond to any alerts generated by the change-detection solution. |  |  |  |  |
| **11.5.1** Interview personnel to verify that all alerts are investigated and resolved. |  |  | X | Skytap maintains file integrity monitoring on systems used to operate the Skytap Cloud platform.  Customers are responsible for file integrity monitoring on customer managed VMs. |
| **11.6** Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties. |  |  |  |  |
| **11.6** Examine documentation and interview personnel to verify that security policies and operational procedures for security monitoring and testing are:  • Documented,   • In use, and   • Known to all affected parties. |  |  | X | Skytap maintains policies and procedures covering unauthorized modifications on systems used to operate the Skytap Cloud platform. These policies and procedures are documented, in use, and known to all affected parties.  Customers are responsible for ensuring that their policies and procedures for security monitoring and testing are documented and known to all affected parties. |
| **12.1** Establish, publish, maintain, and disseminate a security policy. |  |  |  |  |
| **12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners). |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.1.1** Review the security policy at least annually and update the policy when business objectives or the risk environment change. |  |  |  |  |
| **12.1.1** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.2** Implement a risk assessment process, that:  • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),  • Identifies critical assets, threats, and vulnerabilities, and   • Results in a formal, documented analysis of risk. Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30. |  |  |  |  |
| **12.2.a** Verify that an annual risk-assessment process is documented that:   • Identifies critical assets, threats, and vulnerabilities   • Results in a formal, documented analysis of risk. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.2.b** Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment. |  |  | X |
| **12.3** Develop usage policies for critical technologies and define proper use of these technologies. ***Note:*** *Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.* Ensure these usage policies require the following: |  |  |  |  |
| **12.3** Examine the usage policies for critical technologies and interview responsible personnel to verify the following policies are implemented and followed: |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.3.1** Explicit approval by authorized parties. |  |  |  |  |
| **12.3.1** Verify that the usage policies include processes for explicit approval from authorized parties to use the technologies. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.3.2** Authentication for use of the technology. |  |  |  |  |
| **12.3.2** Verify that the usage policies include processes for all technology use to be authenticated with user ID and password or other authentication item (for example, token). |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.3.3** A list of all such devices and personnel with access. |  |  |  |  |
| **12.3.3** Verify that the usage policies define:  • A list of all critical devices, and  • A list of personnel authorized to use the devices. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.3.4** A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices). |  |  |  |  |
| **12.3.4** Verify that the usage policies define a method to accurately and readily determine owner, contact information, and purpose (for example,labeling, coding, and/or inventorying of devices). |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.3.5** Acceptable uses of the technology. |  |  |  |  |
| **12.3.5** Verify that the usage policies define acceptable uses for the technology. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.3.6** Acceptable network locations for the technologies. |  |  |  |  |
| **12.3.6** Verify that the usage policies define acceptable network locations for the technology. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.3.7** List of company-approved products. |  |  |  |  |
| **12.3.7** Verify that the usage policies include a list of company-approved products. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.3.8** Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. |  |  |  |  |
| **12.3.8.a** Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.3.8.b** Examine configurations for remote access technologies to verify that remote access sessions will be automatically disconnected after a specific period of inactivity. |  |  | X |
| **12.3.9** Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. |  |  |  |  |
| **12.3.9** Verify that the usage policies require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.3.10** For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements. |  |  |  |  |
| **12.3.10.a** Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.3.10.b** For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements. |  |  | X |
| **12.4** Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. |  |  |  |  |
| **12.4.a** Verify that information security policy and procedures clearly define information security responsibilities for all personnel. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.4.b** Interview a sample of responsible personnel to verify they understand the security policies. |  |  | X |
| **12.4.1** Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include:   • Overall accountability for maintaining PCI DSS compliance   • Defining a charter for a PCI DSS compliance program and communication to executive management   Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. |  |  |  |  |
| **12.4.1.a** Examine documentation to verify executive management has assigned overall accountability for maintaining the entity’s PCI DSS compliance |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.4.1.b** Examine the company’s PCI DSS charter to verify it outlines the conditions under which the PCI DSS compliance program is organized and communicated to executive management. |  |  | X |
| **12.5** Assign to an individual or team the following information security management responsibilities: |  |  |  |  |
| **12.5** Examine information security policies and procedures to verify:   • The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management.   • The following information security responsibilities are specifically and formally assigned |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.5.1** Establish, document, and distribute security policies and procedures. |  |  |  |  |
| **12.5.1** Verify that responsibility for establishing, documenting and distributing security policies and procedures is formally assigned. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.5.2** Monitor and analyze security alerts and information and distribute to appropriate personnel. |  |  |  |  |
| **12.5.2** Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.5.3** Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. |  |  |  |  |
| **12.5.3** Verify that responsibility for establishing, documenting, and distributing security incident response and escalation procedures is formally assigned. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.5.4** Administer user accounts, including additions, deletions, and modifications. |  |  |  |  |
| **12.5.4** Verify that responsibility for administering (adding, deleting, and modifying) user account and authentication management is formally assigned. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.5.5** Monitor and control all access to data. |  |  |  |  |
| **12.5.5** Verify that responsibility for monitoring and controlling all access to data is formally assigned. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.6** Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures. |  |  |  |  |
| **12.6.a** Review the security awareness program to verify it provides awareness to all personnel about the cardholder data security policy and procedures. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.6.b** Examine security awareness program procedures and documentation and perform the following: |  |  | X |
| **12.6.1** Educate personnel upon hire and at least annually. ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.* |  |  |  |  |
| **12.6.1.a** Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions). |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.6.1.b** Verify that personnel attend security awareness training upon hire and at least annually. |  |  | X |
| **12.6.1.c** Interview a sample of personnel to verify they have completed awareness training and are aware of the importance of cardholder data security. |  |  | X |
| **12.6.2** Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures. |  |  |  |  |
| **12.6.2** Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.7** Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only. |  |  |  |  |
| **12.7** Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.8** Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows: |  |  |  |  |
| **12.8**Through observation, review of policies and procedures, and review of supporting documentation, verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data as follows: |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.8.1** Maintain a list of service providers including a description of the service provided. |  |  |  |  |
| **12.8.1** Verify that a list of service providers is maintained and includes a list of the services provided. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.8.2** Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s CDE. ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.* |  |  |  |  |
| **12.8.2** Observe written agreements and confirm they include an acknowledgement by service providers that they 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 | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.8.3** Ensure there is an established process for engaging service providers including proper due diligence prior to engagement. |  |  |  |  |
| **12.8.3** Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.8.4** Maintain a program to monitor service providers’ PCI DSS compliance status at least annually. |  |  |  |  |
| **12.8.4** Verify that the entity maintains a program to monitor its service providers’ PCI DSS compliance status at least annually. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.8.5** Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. |  |  |  |  |
| **12.8.5** Verify the entity maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **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.  ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.* |  |  |  |  |
| **12.9** Additional testing procedure for service provider assessments only: Review service provider’s policies and procedures and observe templates used for written agreement to confirm the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment. |  |  | X  X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.10** Implement an incident response plan. Be prepared to respond immediately to a system breach. |  |  |  |  |
| **12.10** Examine the incident response plan and related procedures to verify entity is prepared to respond immediately to a system breach by performing the following: |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **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 back-up 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. |  |  |  |  |
| **12.10.1.a** Verify that the incident response plan includes:  • Roles, responsibilities, and communication 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 back-up processes  • Analysis of legal requirements for reporting compromises (for example, California Bill 1386, which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database).  • Coverage and responses for all critical system components.  • Reference or inclusion of incident response procedures from the payment brands. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.10.1.b** Interview personnel and review documentation from a sample of previously reported incidents or alerts to verify that the documented incident response plan and procedures were followed. |  |  | X |
| **12.10.2** Review and test the plan at least annually, including all elements listed in Requirement 12.10.1. |  |  |  |  |
| **12.10.2** Interview personnel and review documentation from testing to verify that the plan is tested at least annually and that testing includes all elements listed in Requirement 12.10.1. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.10.3** Designate specific personnel to be available on a 24/7 basis to respond to alerts. |  |  |  |  |
| **12.10.3** Verify through observation, review of policies, and interviews of responsible personnel that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.10.4** Provide appropriate training to staff with security breach response responsibilities. |  |  |  |  |
| **12.10.4** Verify through observation, review of policies, and interviews of responsible personnel that staff with responsibilities for security breach response are periodically trained. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.10.5** Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. |  |  |  |  |
| **12.10.5** Verify through observation and review of processes that monitoring and responding to alerts from security monitoring systems are covered in the Incident Response Plan. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.10.6** Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. |  |  |  |  |
| **12.10.6** Verify through observation, review of policies, and interviews of responsible personnel that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **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 A584  Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement. |  |  |  |  |
| **12.11.a Examine** policies and procedures to verify that processes are defined for reviewing and confirming that personnel are following security policies and operational procedures, and that reviews cover:  • Daily log reviews   • Firewall rule-set reviews   • Applying configuration standards to new systems   • Responding to security alerts   • Change management processes |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **12.11.b** Interview responsible personnel and examine records of reviews to verify that reviews are performed at least quarterly |  |  | X |
| **12.11.1** Additional requirement for service providers only: Maintain documentation of quarterly review process to include:   • Documenting results of the reviews   • Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program   Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement |  |  |  |  |
| **12.11.1.a** Examine documentation from the quarterly reviews to verify they include:  • Documenting results of the reviews.   • Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program. |  |  | X | Skytap maintains policies and procedures applicable to operation of the Skytap Cloud platform.  Customers are responsible for maintaining policies and processes applicable to their cardholder data environment. |
| **A1** Protect each entity’s (that is, merchant, service provider, or other entity) hosted environment and data, per A1.1 through A1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. *Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.* |  |  |  |  |
| **A1** Specifically for a PCI DSS assessment of a shared hosting provider, to verify that shared hosting providers protect entities’ (merchants and service providers) hosted environment and data, select a sample of servers (Microsoft Windows and Unix/Linux)across a representative sample of hosted merchants and service providers*,* and perform A1.1 through A1.4 below: |  |  |  |  |
| **A1.1** Ensure that each entity only runs processes that have access to that entity’s cardholder data environment. |  |  |  |  |
| **A1.1** If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example:   • No entity on the system can use a shared web server user ID.  • All CGI scripts used by an entity must be created and run as the entity’s unique user ID. |  |  | X | Skytap Cloud maintains segmentation of customer information through physical and logical network and application layer access controls.  Customers are responsible for access management for their user accounts deployed using Skytap Cloud.  The Secondary Shared-Hosting Provider is responsible to protect entities’ hosted environments, data server instances and applications running on customer managed VMs. |
| **A1.2** Restricteach entity’s access and privileges to its own cardholder data environment only. |  |  |  |  |
| **A1.2.a** Verify the user ID of any application process is not a privileged user (root/admin). |  |  | X | Skytap Cloud maintains segmentation of customer information through physical and logical network and application layer access controls.  The Secondary Shared-Hosting Provider is responsible to protect entities’ hosted environments, data, server instances and applications running on customer managed VMs. |
| **A1.2.b** Verify each entity (merchant, service provider) has read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.) **Important:** An entity’s files may not be shared by group. |  |  | X |
| **A1.2.c** Verify that an entity’s users do not have write access to shared system binaries. |  |  |  |
| **A1.2.d** Verify that viewing of log entries is restricted to the owning entity |  |  | X |
| **A1.3** Ensure logging and audit trails are enabled and unique to each entity’s cardholder data environment and consistent with PCI DSS Requirement 10. |  |  |  |  |
| **A1.3** Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment:   • Logs are enabled for common third-party applications.  • Logs are active by default.  • Logs are available for review by the owning entity.  • Log locations are clearly communicated to the owning entity. |  |  | X | Skytap Cloud maintains segmentation of customer information through physical and logical network and application layer access controls.  The Secondary Shared-Hosting Provider is responsible to protect entities’ hosted environments, data, server instances and applications running on customer managed VMs. |
| **A1.4** Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider. |  |  |  |  |
| **A1.4** Verify the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise. |  |  | X | Skytap Cloud maintains segmentation of customer information through physical and logical network and application layer access controls.  The Secondary Shared-Hosting Provider is responsible to protect entities’ hosted environments, data, server instances and applications running on customer managed VMs. |
| **A2.1** Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either: • Confirm the devices are not susceptible to any known exploits for those protocols. Or: • Have a formal Risk Mitigation and Migration Plan in place. |  |  |  |  |
| **A2.1** For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS:   • Confirm the entity has documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS. Or:  • Complete A2.2 below. |  | X |  | Skytap Cloud maintains TLS 1.1 or greater to support customer's PCI workloads. Skytap Cloud provides a minimum-security policy of TLS 1.0 for customers with non-PCI workloads that still require it.  Customers are responsible for initiating TLS connections that use TLS 1.1 or greater to meet their PCI compliance requirements. |
| **A2.2** Entities with existing implementations (other than as allowed in A.2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. |  |  |  |  |
| **A2.2** Review the documented Risk Mitigation and Migration Plan to verify it includes:   • Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment;   • Risk-assessment results and risk-reduction controls in place;  • Description of processes to monitor for new vulnerabilities associated with SSL/early TLS;   • Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments;   • Overview of migration project plan including target migration completion date no later than June 30, 2018. |  | X |  | Skytap Cloud maintains TLS 1.1 or greater to support customer's PCI workloads. Skytap Cloud provides a minimum-security policy of TLS 1.0 for customers with non-PCI workloads that still require it.  Customers are responsible for initiating TLS connections that use TLS 1.1 or greater to meet their PCI compliance requirements. |
| **A2.3 Additional Requirement for Service Providers Only:** All service providers must provide a secure service offering by June 30, 2016. *Note: Prior to June 30, 2016, the service provider must either have a secure protocol option included in their service offering, or have a documented Risk Mitigation and Migration Plan (per A.2.2) that includes a target date for provision of a secure protocol option no later than June 30, 2016. After this date, all service providers must offer a secure protocol option for their service.* |  |  |  |  |
| **A2.3** Examine system configurations and supporting documentation to verify the service provider offers a secure protocol option for their service. |  | X |  | Skytap Cloud maintains TLS 1.1 or greater to support customer's PCI workloads. Skytap Cloud provides a minimum-security policy of TLS 1.0 for customers with non-PCI workloads that still require it.  Customers are responsible for initiating TLS connections that use TLS 1.1 or greater to meet their PCI compliance requirements. |