netskope

Compliance Series

Payment Card Industry Data Security Standard (PCI DSS) v.4.0

Using the Netskope Platform to Assist with PCI DSS Compliance

TABLE OF CONTENTS

INTRODUCTION

The Payment Card Industry Data Security Standard (PCI DSS) is the gold standard for all organizations that "store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE)." Therefore, though it does not have the force of law, merchants that accept credit and debit card payments will often be contractually bound to implement some or all of its requirements.

The PCI DSS framework consists of six overarching strategic Objectives that are further broken down into twelve Requirements, illustrated in the table below..

Objective	Requirement
Build and Maintain a Secure Network and Systems	**1.** Install and Maintain Network Security Controls. **2.** Apply Secure Configurations to All System Components.
Protect Account Data	**3.** Protect Stored Account Data. **4.** Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program	**5.** Protect All Systems and Networks from Malicious Software. **6.** Develop and Maintain Secure Systems and Software
Implement Strong Access Control Measures	**7.** Restrict Access to System Components and Cardholder Data by Business Need to Know. **8.** Identify Users and Authenticate Access to System Components. **9.** Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks	**10.** Log and Monitor All Access to System Components and Cardholder Data. **11.** Test Security of Systems and Networks Regularly.
Maintain an Information Security Policy	**12.** Support Information Security with Organizational Policies and Programs

PCI DSS TERMINOLOGY

Cardholder data (CHD): the cardholder's name, primary account number (PAN), expiration date, and service code

Sensitive authentication data (SAD): full track data (magnetic stripe data or equivalent on a chip), card verification code, and PINs or PIN blocks

Cardholder data environment (CDE): the system components, people, and processes that store, process, and transmit CHD and/or SAD, as well as system components that do not necessarily store, process, and transmit CHD and/or SAD, but which have unrestricted connectivity to system components that do.

PCI DSS 4.0 introduces significant updates to enhance payment card data security, addressing evolving threats and technologies. The new version offers greater flexibility with the introduction of Customized Approach options, allowing organizations to tailor security controls to their specific environments while maintaining compliance. It emphasises continuous compliance, focusing on ongoing security practices rather than point-in-time assessments. Enhanced authentication measures now mandate Multi-Factor Authentication (MFA) for all access to the Cardholder Data Environment (CDE) and update password and authentication requirements.

New and updated requirements include targeted risk analysis for determining activity frequency, secure management of payment page scripts, and clarifications to existing standards to align with current security practices. Penetration testing methodologies have been updated and expanded to address new threats.

Data discovery and masking enhancements require the identification and documentation of all locations where account data is stored, processed, or transmitted, and improved data masking protects cardholder information. Incident response procedures are strengthened for timely and effective reactions to security incidents. Additionally, security awareness training is enhanced with phishing simulations, and expanded logging and monitoring requirements ensure comprehensive tracking and quick anomaly detection.

HOW TO USE THIS GUIDE

The Netskope platform consists of a suite of tools integrated into a Secure Access Service Edge architecture. In the tables below, each Objective is broken down into its constituent Requirements and Sections. Each Section is mapped to an appropriate tool or tools, with a description of how the Netskope platform assists with the organization's compliance needs. For the sake of brevity and ease of reading, we have not broken each Section out into its constituent subsections, but have attempted to craft responses to each Section that are inclusive of all its subsections' requirements.

Note the following acronyms and/or aliases for the Netskope products:

Industry terminology	Netskope Product Line/Abbreviation
Security Access Service Edge	SASE
Security Service Edge	SSE
Next-Gen Secure Web Gateway	NG-SWG
Cloud Access Security Broker	CASB
Public Cloud Security	Public Cloud Security
Zero Trust Network Access	ZTNA Next
Cloud Security Posture Management	CSPM
SaaS Security Posture Management	SSPM
Data Loss Prevention	DLP (Standard & Advanced)
Firewall as a Service	Cloud Firewall
Reporting and Analytics	Advanced Analytics
Threat Intelligence	Threat Protection (Standard & Advanced)
Remote Browser Isolation	RBI
Artificial Intelligence Security	SkopeAI
Software-Defined Wide Area Network (SD-WAN)	Borderless SD-WAN Secure SD-WAN Endpoint SD-WAN Wireless SD-WAN IoT Intelligent Accessl
Threat/Risk Sharing	Cloud Exchange Cloud Threat Exchange (CTE) Cloud Risk Exchange (CRE)
IT/IoT/OT Security	Device Intelligence
Proactive Digital Experience Management	P-DEM
Third-Party Risk Management/Supply Chain	Cloud Confidence Index (CCI)
User Risk Metrics	User Confidence Index (UCI)

BUILD AND MAINTAIN A SECURE NETWORK AND SYSTEMS

Requirement		Netskope Response	Products
1. Install and maintain Network Security Controls	1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.	Netskope enforces organizational policies through pop-up banners and coaching pages that notify employees of potential infringements. It also supports asset inventory, acquisition strategies, third-party risk management, and business continuity by identifying and assessing managed and unmanaged apps. Zero Trust Network Access (ZTNA) Next facilitates secure remote access to private apps with end-to-end encryption and granular controls Netskope's Cloud Access Security Broker (CASB) monitors SaaS and IaaS activities, applying real-time data loss prevention controls and offering training on organizational policies. It scores SaaS applications in its Cloud Confidence Index (CCI), providing risk assessment details such as security policies, certifications, and privacy concerns. Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention (DLP) engine which ensures data security across web, cloud, and endpoints, using machine learning to classify and protect sensitive data with contextaware policies. Netskope's Cloud Firewall applies security policies to egress traffic, guarding against DNS attacks and integrating with SIEM tools. Device Intelligence catalogs and classifies network devices, detecting anomalies and applying zero trust principles. Advanced Analytics maps data flows and assesses cloud risks, providing a dashboard for tracking security trends. Cloud Security Posture Management prevents misconfigurations in mission-critical IaaS platforms and scans cloud storage for data exfiltration, integrating with Netskope's Cloud Ticket Orchestrator for alerting and remediation. SaaS Security Posture Management (SSPM) prevents misconfigurations in SaaS functions and offers remediation steps, integrating with Cloud Ticket Orchestrator for automated fixes.	• All products • ZTNA Next • CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • Cloud Firewall • DLP • SSPM • Advanced Analytics • Device Intelligence • CTO
	1.2 Network security controls (NSCs) are configured and maintained.	Netskope assists organizations in implementing a network security architecture that's aligned with industry- recognized cybersecurity and data privacy best practices. This includes a "defense-in-depth" strategy that minimizes interactions between security layers, allowing them to function independently. Properly customized and configured, the Netskope platform addresses risk to organizational operations, assets, individuals, and third partiess.	• All products • Public Cloud Security • CSPM • Cloud Firewall • SD-WAN • SSPM • ZTNA Next • CTO

Requirement		Netskope Response	Products
		Netskope's Cloud Security Posture Management (CSPM) monitors critical IaaS platforms to prevent misconfigurations, ensuring compliance with access policies and standards, and scans cloud storage to prevent data exfiltration. CSPM integrates with Cloud Ticket Orchestrator for automated alerts and remediation. Similarly, SaaS Security Posture Management (SSPM) prevents misconfigurations in SaaS functions and integrates with Cloud Ticket Orchestrator for automated issue resolution. Remediated configurations can be converted into new rules, improving security based on findings. Netskope's Borderless SD-WAN extends network perimeters to any device and user, using the New Edge network for highavailability connectivity and policy enforcement based on context-specific criteria. The Cloud Firewall applies security policies to egress traffic, inspecting queries to thwart attacks and integrating with SIEM tools for incident response. ZTNA Next offers secure remote access to private apps, supports third-party authentication, encrypts data, and enforces zero trust principles with detailed access logging and policy controls.	
	1.3 Network access to and from the cardholder data environment is restricted.	Netskope Netskope offers a comprehensive suite of security solutions for monitoring and managing cloud and web activities. The Cloud Access Security Broker (CASB) provides in-depth oversight over SaaS and IaaS services and implements realtime data loss prevention and activity controls, along with role-based access controls (RBAC) built on the principle of least privilege. Netskope's NG-SWG integrates with NIST-compliant third party identity providers, extending SSO/MFA across managed and unmanaged web and cloud-based apps and services. It also decodes user activities, detects anomalies, and applies granular policy controls, with responses ranging from multifactor authentication to policy violation alerts. NG-SWG supports RBAC and can generate detailed reports for incident response. Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations and ensure compliance with organizational policies. It integrates with the Cloud Ticket Orchestrator for automated remediation and scanning of cloud storage to prevent data exfiltration. SaaS Security Posture Management (SSPM) offers similar functionalities for SaaS applications, alerting and automating remediation efforts through the Cloud Ticket Orchestrator. Borderless SD-WAN extends network perimeters globally, enforcing policies with adaptive trust criteria. The Cloud Firewall secures egress traffic and integrates with SIEM tools to disrupt cyber-attacks. The Zero Trust Network Access (ZTNA) Next facilitates secure remote access to private apps with end-to-end encryption and granular controls. Advanced User Entity and Behavior Analytics (UEBA) utilizes machine learning models to detect insider threats, offering dynamic risk scoring and policy adaptations based on user behavior.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Firewall • DLP • SD-WAN • SSPM • ZTNA Next • Advanced UEBA • CTO

Requirement		Netskope Response	Products
	1.4 Network connections between trusted and untrusted networks are controlled.	Netskope's Borderless SD-WAN expands network perimeters globally, providing high availability connectivity and policy enforcement based on adaptive trust criteria. Netskope's Cloud Firewall applies security policies to outbound traffic, disrupts denial of service and other forms of DNS attacks, and integrates with SIEM tools for incident response. ZTNA Next provides secure remote access to private apps, integrates with third-party identity providers for authentication, and enforces zero trust principles with granular access controls. Netskope's CASB monitors and logs activities in SaaS and IaaS services, applying real-time controls and data loss prevention measures. Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms for misconfigurations and deviations from policies, preventing data exfiltration, and integrates with Cloud Ticket Orchestrator for automated remediation. SaaS Security Posture Management (SSPM) monitors SaaS functions for misconfigurations and policy deviations, alerts with remediation instructions, and integrates with Cloud Ticket Orchestrator to automate remediation.	• All products • CASB • Public Cloud Security • CSPM • Cloud Firewall • SD-WAN • SSPM • ZTNA Next • CTO
	1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.	Netskope's Cloud Firewall enforces security policies on egress traffic without backhauling to on-prem stacks, inspecting queries to prevent DDoS and DNS attacks, and integrating event logs with SIEM tools for incident response. Netskope Device Intelligence identifies, catalogs, and classifies all devices on the network, using AI/ML to detect anomalies and enforce zero trust policies. Integration with incident response tools allows it to generate security alerts based on organizational criteria. Netskope's Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations and ensure compliance with organizational policies and standards, including scanning cloud storage buckets to prevent data exfiltration. CSPM integrates with Netskope's Cloud Ticket Orchestrator for alerts and automated remediation. Netskope's SaaS Security Posture Management (SSPM) performs similar monitoring for SaaS functions, providing remediation instructions and integration with the Cloud Ticket Orchestrator for generating service tickets and automating fixes. SSPM can convert detected misconfigurations into new rules to enhance security.	• Public Cloud Security • CSPM • Cloud Firewall • SSPM • Device Intelligence • CTO • ZTNA Next

Requirement		Netskope Response	Products
2. Apply Secure Configurations to All System Components	2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.	Netskope enforces organizational policies and assists in policy communication via pop-up banners and coaching pages to notify employees of policy infringements. Advanced Analytics maps data flows across web and cloud services, categorizing data by sensitivity, and assesses cloud risk by evaluating cloud app usage. The product dashboard offers insights into security trends, including app access, detected threats, triggered policies, and impacted users. Netskope's Cloud Security Posture Management (CSPM) continuously monitors critical IaaS platforms to prevent misconfigurations and ensure compliance with organizational and regulatory standards. CSPM also scans cloud storage for data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for alerting and automating remediation. Similarly, Netskope's SaaS Security Posture Management (SSPM) monitors SaaS functions to prevent misconfigurations, providing alerts with remediation steps, and integrates with the Cloud Ticket Orchestrator to automate responses. Misconfigurations can be converted into new rules to enhance security.	• All products • CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • Advanced Analytics • CTO
	2.2 System components are configured and managed securely.	Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) continuously monitor and protect an organization's critical IaaS and SaaS platforms from misconfigurations that deviate from organizational policies or regulatory standards. CSPM focuses on preventing data exfiltration by scanning cloud storage buckets, while SSPM monitors SaaS functions. Both systems integrate with Netskope's Cloud Ticket Orchestrator to send alerts, generate service tickets, and automate remediation efforts. SSPM also provides step-by-step remediation instructions and converts previously detected misconfigurations into new rules for improved security.	• Public Cloud Security • CSPM • SSPM • CTO
	2.3 Wireless environments are configured and managed securely.	Netskope's Borderless SD-WAN extends network perimeters to any user, device, and location, steering traffic through Netskope's global New Edge network to ensure high availability and enforce uniform policy controls based on userspecific context. Netskope's ZTNA Next offers remote access to private apps hosted on-premises or in the cloud, integrating with thirdparty identity providers, employing end-to-end encryption, and applying zero trust principles to manage access and privileges. ZTNA Next also logs all access attempts and enforces policies on failed logins. Netskope Device Intelligence identifies and classifies all devices on the network, segmenting risky devices and using AI/ML to detect anomalies and enforce access controls. It integrates with incident response tools for generating security alerts based on organizational criteria.	• SD-WAN • ZTNA Next • Device Intelligence

PROTECT ACCOUNT DATA

Requirement		Netskope Response	Products
3. Protect Stored Account Data	3.1 Processes and mechanisms for protecting stored account data are defined and understood.	Netskope can enforce organizational policies through pop-up banners and coaching pages, notifying employees of potential policy infringements, blocking risky actions, suggesting safer alternatives, or referring employees to third-party vendors for further cybersecurity or organizational policy training. Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations and deviations from access policies or regulatory standards, while also scanning cloud storage to prevent data exfiltration. CSPM integrates with Cloud Ticket Orchestrator for alerts and automated remediation. Similarly, Netskope's SaaS Security Posture Management (SSPM) monitors SaaS functions to prevent misconfigurations and policy deviations, offering step-by-step remediation instructions and integration with Cloud Ticket Orchestrator. SSPM also learns from previous misconfigurations to enhance security rules. Netskope's Advanced Analytics maps data flows across web and cloud services and characterizes data by category and sensitivity. It assesses cloud risk by analyzing app usage and allows administrators to track security trends via a product dashboard.	• All products • CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • Advanced Analytics • CTO • DLP
	3.2 Storage of account data is kept to a minimum.	Netskope's Cloud Security Posture Management (CSPM) continuously monitors mission-critical IaaS platforms to detect and prevent misconfigurations, ensuring compliance with organizational policies and industry standards. It also routinely scans cloud storage to prevent data exfiltration. CSPM integrates with Netskope's Cloud Ticket Orchestrator to send alerts and automate remediation efforts. Similarly, Netskope's SaaS Security Posture Management (SSPM) oversees SaaS functions to prevent misconfigurations and ensure proper data usage. SSPM provides step-by-step remediation instructions and can also integrate with Cloud Ticket Orchestrator for automated responses. Detected misconfigurations can be turned into new security rules, enhancing overall protection. Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention (DLP) engine which secures organizational data in use, in transit, and at rest across web, cloud applications, and endpoint devices	• Public Cloud Security • CASB • NG-SWG • CSPM • SSPM • CTO • DLP
	3.3 Sensitive authentication data (SAD) is not stored after authorization.	Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention (DLP) engine which secures organizational data in use, in transit, and at rest across web, cloud applications, and endpoint devices. It employs machine learning to identify and protect sensitive data based on both regulatory and organizational requirements. The engine uses context-aware policies that include user, device, app, network, and action information to provide real-time protection by obfuscating, encrypting, or blocking actions.	• CASB • NG-SWG • DLP

Requirement		Netskope Response	Products
		Netskope's DLP also enforces role-based data access during incident response and recovery, ensures the integrity of backups, and maintains log files in dedicated repositories for continuous monitoring and forensic investigations.	
	3.4 Access to displays of full PAN and ability to copy cardholder data are restricted	Netskope's ZTNA Next offers remote access to private apps, whether on-premises or cloud-hosted, from any device and location. It integrates with NIST-compliant third-party identity providers for secure authentication and ensures data security with end-to-end encryption. Adhering to zero trust principles, ZTNA Next applies granular access controls and logs all access attempts. It also enforces organizational policies on failed login attempts.	• ZTNA Next • DLP
	3.5 Primary account number (PAN) is secured wherever it is stored.	Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention (DLP) engine which offers comprehensive security for organizational data across the web, cloud applications, and endpoint devices. Utilizing machine learning, it identifies, classifies, and protects sensitive data based on regulatory and organizational requirements. Context-aware policies consider users, devices, apps, networks, and actions to safeguard data in real-time, through methods like data obfuscation, encryption, and action blocking. Netskope's DLP enforces role-based data access for incident response, ensures backup integrity, and maintains dedicated log repositories for continuous monitoring and forensic investigations.	• CASB • NG-SWG • DLP
	3.6 Cryptographic keys used to protect stored account data are secured.	Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention (DLP) engine which secures organizational data in use, in transit, and at rest across web, cloud applications, and endpoint devices	• CASB • NG-SWG • DLP
	3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.	Netskope's products do not map to this requirement	
4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.	Netskope's ZTNA Next provides secure remote access to private apps, utilizing third-party identity providers, end-toend encryption, and zero trust principles to control access and log attempts. Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention (DLP) engine which secures organizational data in use, in transit, and at rest across web, cloud applications, and endpoint devices Advanced Analytics maps data flows, evaluates cloud risk by assessing app usage, and provides dashboards for tracking security trends including app access, threat detection, policy triggers, and user impact.	• All products • DLP • CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • ZTNA • Advanced Analytics • CTO

Requirement		Netskope Response	Products
		Netskope enforces organizational policies using pop-up banners and coaching pages to notify employees of potential policy infringements. Its Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations and data exfiltration, integrates with the Cloud Ticket Orchestrator to send alerts and automate remediation, and scans cloud storage for security compliance. Netskope's SaaS Security Posture Management (SSPM) similarly monitors SaaS functions, preventing misconfigurations and generating service tickets for remediation. Findings can form new security rules, enhancing protection.	
	4.2 PAN is protected with strong cryptography during transmission.	Netskope's ZTNA Next offers remote access to on-premises or cloud-based private applications from any device, anywhere. It integrates with NIST-compliant third-party identity providers for secure authentication. Utilizing end-to-end encryption, ZTNA Next secures data both in use and in transit. It also applies granular controls to restrict access and privileges based on zero trust principles. Additionally, ZTNA Next logs all access attempts and enforces organizational policies regarding failed login attempts. Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention (DLP) engine which secures organizational data in use, in transit, and at rest across web, cloud applications, and endpoint devices	• ZTNA Next • CASB • NG-SWG • DLP

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

Requirement		Netskope Response	Products
5. Protect All Systems and Networks from Malicious Software	5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.	Netskope enforces organizational policies and assists in their communication through pop-ups and coaching pages, alerting employees to potential infractions or referring them to third party vendors for additional cybersecurity training. Standard Threat Protection safeguards against known threats, employs machine learning for new malware detection, and includes real-time phishing detection and web filtering. It integrates with threat intelligence from Cloud Threat Exchange and other Netskope tools for a comprehensive security solution. Enhanced Threat Protection adds deobfuscation, recursive file unpacking, and multi-stage sandboxing to detect new malware. Netskope's Advanced Analytics maps data flows across web and cloud services, assessing data sensitivity and cloud app risk. The dashboard tracks security trends, including apps accessed, threats detected, policies triggered, and user impact, providing administrators with detailed security insights.	• All products • CASB • NG-SWG • Advanced Threat Protection • Threat Protection • SkopeAI • Advanced Analytics • CTO

Requirement		Netskope Response	Products
	5.2 Malicious software (malware) is prevented, or detected and addressed.	Netskope's NG-SWG includes Remote Browser Isolation, which secures browsing by isolating risky websites in a cloudbased sandbox, preventing malware from infecting the network. Standard Threat Protection safeguards against known threats, employs machine learning for new malware detection, and includes real-time phishing detection and web filtering. It integrates with threat intelligence from Cloud Threat Exchange and other Netskope tools for a comprehensive security solution. Enhanced Threat Protection adds deobfuscation, recursive file unpacking, and multi-stage sandboxing to detect new malware. Netskope's CASB and NG-SWG can be equipped with Netskope's Advanced DLP extends Standard DLP capabilities with IaaS Storage Scanning, detecting and preventing malware in cloud storage. SkopeAI enhances DLP by using machine learning to analyze and protect unstructured data like images. SkopeAI also delivers superior results and speed in detecting multivarious attacks, polymorphic malware, novel phishing web domains, zero-day threats, and malicious web content.	• NG-SWG • RBI • Advanced DLP • Advanced Threat Protection • Threat Protection • SkopeAI
	5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.	Netskope's NG-SWG includes Remote Browser Isolation, a feature that secures risky and uncharacterized websites by isolating them in a cloud-based sandbox to prevent malware infection and unauthorized software execution. Standard Threat Protection utilizes machine learning, realtime phishing detection, corroborative sandboxing, and web filtering, and integrates with threat intelligence feeds from Netskope's Cloud Threat Exchange and other security tools for comprehensive protection. Advanced Threat Protection builds on Standard Threat Protection by incorporating advanced techniques like deobfuscation, recursive file unpacking, and multi-stage sandboxing to detect new malware. Netskope's Public Cloud Security can be equipped with Advanced DLP which enhances Standard DLP by scanning IaaS Storage for hidden malware to protect the cloud environment. SkopeAI uses machine learning to enhance the DLP engine's ability to analyze and protect unstructured data, including images. SkopeAI also delivers superior results and speed in detecting multivarious attacks, polymorphic malware, novel phishing web domains, zero-day threats, and malicious web content.	• NG-SWG • CASB • Public Cloud Security • RBI • Advanced DLP • Advanced Threat Protection • Threat Protection • SkopeAI
	5.4 Anti-phishing mechanisms protect users against phishing attacks.	Standard Threat Protection safeguards against known and new malware using machine learning, real-time phishing detection, corroborative sandboxing, and web filtering. It also integrates with Netskope's Cloud Threat Exchange and other security tools like Remote Browser Isolation, Cloud Firewall, and User Entity and Behavior Analytics for layered protection. Netskope's Public Cloud Security can be equipped with Advanced DLP which enhances Standard DLP by scanning IaaS Storage for hidden malware to protect the cloud environment.	• NG-SWG • CASB • Public Cloud Security • Advanced DLP • Advanced Threat Protection

Requirement		Netskope Response	Products
		Advanced Threat Protection builds on Standard Threat Protection by adding deobfuscation, recursive file unpacking, and multi-stage sandboxing to counter new malware threats. SkopeAI enhances the DLP engine with machine learning for deep contextual awareness, allowing it to identify and protect unstructured data such as images that traditional DLP engines cannot handle effectively. SkopeAI also delivers superior results and speed in detecting multivarious attacks, polymorphic malware, novel phishing web domains, zero-day threats, and malicious web content.	• Threat Protection • SkopeAI
6. Develop and Maintain Secure Systems and Software	6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.	Netskope enforces organizational policies through pop-up banners and coaching pages that notify employees of potential policy violations. Cloud Security Posture Management (CSPM) monitors mission-critical IaaS platforms to prevent misconfigurations and ensure compliance with organizational and regulatory standards. CSPM scans cloud storage to prevent data exfiltration and integrates with the Cloud Ticket Orchestrator for alerting and automating remediation. Similarly, its SaaS Security Posture Management (SSPM) continuously monitors SaaS functions to prevent misconfigurations. SSPM provides remediation instructions and generates service tickets to automate fixes, with the ability to convert detected issues into new security rules. Netskope's Advanced Analytics maps data flows across web and cloud services, assesses cloud risk, and tracks security trends through an informative dashboard.	• All products • CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • Advanced Analytics • CTO
	6.2 Bespoke and custom software are developed securely.	Netskope's Cloud Confidence Index (CCI) assesses risk for SaaS applications based on criteria like security policies, certifications, audit capabilities, and legal privacy concerns. Cloud Security Posture Management (CSPM) monitors crucial IaaS platforms to prevent misconfigurations and ensure compliance with organizational and regulatory standards. CSPM also scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for alerts and automated remediation. Similarly, Netskope's SaaS Security Posture Management (SSPM) continuously oversees critical SaaS functions to avoid misconfigurations and ensure proper data usage. SSPM provides step-by-step remediation instructions, integrates with the Cloud Ticket Orchestrator for automated ticketing, and can convert detected misconfigurations into new security rules, enhancing overall security posture.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • SSPM • CTO
	6.3 Security vulnerabilities are identified and addressed.	Netskope offers comprehensive cloud security solutions, evaluating SaaS applications through its Cloud Confidence Index (CCI) based on security, audit capabilities, legal and privacy concerns. Netskope's Cloud Risk Exchange consolidates risk scores from third-party vendors to enforce adaptive controls, while the Cloud Threat Exchange facilitates near real-time sharing of threat intelligence.	• CASB • NG-SWG • Public Cloud Security • CSPM

Requirement		Netskope Response	Products
		The Cloud Ticket Orchestrator further enhances incident response by automating service ticket generation and workflows, securing role-based access. Cloud Security Posture Management (CSPM) ensures missioncritical IaaS platforms remain compliant by monitoring for misconfigurations and preventing data exfiltration, integrating seamlessly with Netskope's Cloud Ticket Orchestrator for automating remediation. The SaaS Security Posture Management (SSPM) similarly protects SaaS functions, alerting and providing remediation steps for misconfigurations while also automating responses. Device Intelligence identifies and monitors all network-connected devices, utilizing AI/ML to detect anomalies and enforcing zero trust principles.	• Cloud Confidence Index (CCI) • SSPM • CTO
	6.4 Public-facing web applications are protected against attacks.	Netskope's Cloud Security Posture Management (CSPM) continuously monitors critical IaaS platforms to prevent misconfigurations and ensure compliance with organizational policies and industry standards, including data use alignment and data exfiltration prevention. CSPM also integrates with Netskope's Cloud Ticket Orchestrator to send alerts and automate remediation. Netskope's SaaS Security Posture Management (SSPM) similarly monitors vital SaaS functions to avoid misconfigurations, ensuring data use consistency and adherence to policies and standards. SSPM alerts provide step-by-step remediation instructions and can generate service tickets via integration with Cloud Ticket Orchestrator. Misconfigurations can be converted into new security rules to enhance protection. Netskope's Cloud Ticket Orchestrator automates the creation of service tickets and workflows in response to security alerts, supporting incident response and enforcing role-based access controls. It is a component of Netskope's Cloud Exchange, included in every Netskope deployment, facilitating extensive incident response automation and recovery planning.	• Public Cloud Security • CSPM • SSPM • Cloud Firewall • CTO
	6.5 Changes to all system components are managed securely.	Netskope's Cloud Security Posture Management (CSPM) continuously monitors critical IaaS platforms to prevent misconfigurations and ensure compliance with organizational and regulatory standards. This includes routine scans to prevent data exfiltration and integrates with the Cloud Ticket Orchestrator for alerts and automated remediation. Similarly, Netskope's SaaS Security Posture Management (SSPM) monitors key SaaS functions to prevent misconfigurations and ensure proper use. SSPM provides step-by-step remediation instructions and integrates with the Cloud Ticket Orchestrator to automate responses. Misconfigurations can also be turned into new security rules to enhance protection. Netskope Device Intelligence identifies and classifies all devices on a network, segments them into groups, and isolates risky devices. It uses AI/ML to establish normal behavior, detect anomalies, and enforce zero trust access controls. Device Intelligence can generate security alerts through integration with incident response tools based on organizational criteria.	• Public Cloud Security • CSPM • SSPM • Device Intelligence • CTO

IMPLEMENT STRONG ACCESS CONTROL MEASURES

Requirement		Netskope Response	Products
7. Restrict Access to System Components and Cardholder Data by Business Need to Know	7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.	Netskope empowers organizations to enforce and communicate their policies through pop-up banners and coaching pages, which notify employees of potential policy violations. Netskope's CASB monitors activities in SaaS and IaaS services, applying real-time activity-level and data loss prevention (DLP) controls, and employs Role-Based Access Control (RBAC) to maintain least privilege access. Netskope's NG-SWG extends SSO/MFA across web and cloud apps, detects anomalous user behavior, and applies granular policy controls. It can generate reports and alerts, integrating with SIEM tools for incident response and ensuring nonrepudiation of user actions. ZTNA Next secures remote access with end-to-end encryption and granular controls, logging all access attempts. Netskope's Cloud Security Posture Management continuously monitors IaaS platforms for misconfigurations, integrating with Cloud Ticket Orchestrator for automated remediation. It also scans cloud storage for data exfiltration risks. The DLP engine secures data in transit, at rest, and in use across various environments, utilizing machine learning to protect sensitive information and enforce RBAC during incident response and recovery. SaaS Security Posture Management monitors SaaS functions to prevent misconfigurations, automating remediation via Cloud Ticket Orchestrator. Advanced Analytics uses machine learning to map data flows, assess cloud risk, and detect insider threats. Netskope ensures comprehensive policy enforcement and security across diverse organizational needs.	• All products • CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • ZTNA Next • Advanced Analytics • Advanced UEBA • CTO
	7.2 Access to system components and data is appropriately defined and assigned.	Netskope's CASB monitors and logs activities in SaaS and IaaS services, enabling real-time controls such as requiring a business justification for a risky action, suggesting a safer alternative, or providing training. It supports Role-Based Access Control (RBAC) for least privilege access. NG-SWG and ZTNA Next integrate with third party identity providers to extend SSO/MFA across managed and unmanaged web and cloud-based apps and services, and can detect anomalies by establishing user activity baselines. They apply granular policy controls, support incident response with detailed logging, and integrate with SIEM tools. Advanced UEBA leverages machine learning to detect insider threats via risk scores, while Device Intelligence identifies and segregates devices, detecting anomalies and applying zero trust controls. Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention engine which secures data across web, cloud apps, and endpoints, utilizing machine learning to classify and protect sensitive data. Context-aware policies enforce role-based access, protect backups, and facilitate forensic investigations.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • ZTNA Next • Advanced UEBA • Device Intelligence • CTO

Requirement		Netskope Response	Products
		Cloud Security Posture Management continuously monitors for misconfigurations and ensures compliance with organizational, regulatory, and industry standards. It prevents data exfiltration and integrates with Cloud Ticket Orchestrator for alerting and automated remediation. SaaS Security Posture Management prevents misconfigurations in SaaS functions, provides corrective instructions, and integrates with the Cloud Ticket Orchestrator to automate fixes.	
	7.3 Access to system components and data is managed via an access control system(s).	Netskope's CASB monitors SaaS and IaaS activities, applying real-time controls and requesting business justifications or providing policy training. Both CASB and NG-SWG support Role-Based Access Control for least privilege access. NG-SWG extends SSO/MFA across managed and unmanaged web and cloud-based apps and services, detects anomalies, and applies nuanced policy controls, going beyond simple allow/block actions to include user notifications and training integration. ZTNA Next provides secure, remote access to private apps, enforcing zero trust principles and logging all access attempts. Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention engine which safeguards data across various environments using machine learning and contextaware policies for real-time data protection. It also facilitates incident response and regulatory investigations by managing access during incidents and preserving log integrity. Advanced UEBA utilizes anomaly detection models and a User Confidence Index for continuous behavior monitoring, adaptive security policies, and insider threat mitigation. Netskope's solutions integrate with identity providers and SIEM tools, enhancing incident response and security posture. Netskope's Cloud Security Posture Management ensures IaaS configurations align with organizational policies, preventing data leaks and integrating with automated remediation systems. Their SaaS Security Posture Management offers continuous misconfiguration monitoring and generates actionable alerts.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • ZTNA Next • Advanced UEBA • CTO
8. Identify Users and Authenticate Access to System Components	8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.	Netskope enforces organizational policies and uses pop-up banners/coaching pages to alert employees of policy violations. Netskope's Next-Gen Secure Web Gateway (NG-SWG) integrates with identity providers for SSO/MFA, detects anomalous behavior, and enforces context-aware policies. NG-SWG generates customizable alerts and reports for incident response and non-repudiation. ZTNA Next secures remote access to private apps, employing zero trust principles and detailed logging. Advanced Analytics maps data flows, assesses cloud risks, and offers a dashboard for tracking security trends, threats, and policy triggers.	• All products • CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • ZTNA Next • Advanced Analytics • CTO

Requirement		Netskope Response	Products
		Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention engine which secures data across various platforms using machine learning to identify and protect sensitive information. DLP also supports role-based access and continuous monitoring for compliance and incident response. Cloud Security Posture Management (CSPM) monitors IaaS platforms to prevent misconfigurations and data exfiltration, integrating with the Cloud Ticket Orchestrator for alerts and remediation.. The SaaS Security Posture Management (SSPM) continuously monitors SaaS functions, offering remediation guidance and automated responses via the Cloud Ticket Orchestrator.	
	8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.	Netskope's Next-Gen Secure Web Gateway (NG-SWG) integrates with third-party identity providers for SSO/MFA support, monitors user activity for anomalies, and applies granular policy controls. It can also enforce multi-factor authentication and provide just-in-time cybersecurity training. NG-SWG generates customizable reports and alerts for incident response and ensures user action accountability. ZTNA Next provides secure remote access to apps from any device, applying zero trust principles, end-to-end encryption, and granular access controls. It logs access attempts and enforces policies on failed logins. Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention engine which protects data across the web, cloud apps, and devices using machine learning for sensitive data classification. DLP enforces role-based access, maintains backup integrity, and aids forensic investigations. Netskope's Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations and ensure compliance with organizational and regulatory standards. It also scans cloud storage to prevent data exfiltration and integrates with the Cloud Ticket Orchestrator for automated remediation. The SaaS Security Posture Management (SSPM) continuously monitors SaaS functions for misconfigurations, offers remediation steps, and integrates with the Cloud Ticket Orchestrator for automated fixes. Detected misconfigurations can be used to create new security rules.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • ZTNA Next • CTO
	8.3 Strong authentication for users and administrators is established and managed.	Netskope's ZTNA Next enables remote access to private apps hosted on-premises or in the cloud from any device, anywhere. It integrates with NIST-compliant third-party identity providers to ensure secure authentication, and uses end-to-end encryption to protect data both in use and in transit. The solution applies granular, zero trust-based controls to limit access and privileges. ZTNA Next also logs all access attempts and enforces organizational policies related to failed login attempts.	• ZTNA Next

Requirement		Netskope Response	Products
	8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.	Netskope's Next-Generation Secure Web Gateway (NG-SWG) integrates with NIST-compliant third-party identity providers, extending Single Sign-On (SSO) and Multi-Factor Authentication (MFA) across both managed and unmanaged web and cloud services. NG-SWG also decodes and logs over 100 inline activities, establishing a user activity baseline to detect anomalies and applying granular policy controls based on activity nature, data, or app instances. Beyond basic "allow" or "block" rules, its context-aware controls can require a stepped-up MFA for risky actions.	• NG-SWG
	8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.	etskope offers robust solutions for implementing cybersecurity and data privacy practices across various systems and services. Its Cloud Security Posture Management (CSPM) continuously oversees IaaS platforms to prevent misconfigurations, ensure compliance with access management policies, and prevent data exfiltration from cloud storage. CSPM integrates with Cloud Ticket Orchestrator to automate alerts and remediation. For SaaS, Netskope's Security Posture Management (SSPM) monitors critical SaaS functions to avoid misconfigurations and enforce standards. SSPM integrates with Cloud Ticket Orchestrator to automate issue resolution and can convert detected misconfigurations into new security rules. Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention engine which secures data in use, transit, and at rest across web, cloud applications, and devices. Utilizing machine learning, it identifies and protects sensitive data in real-time according to organizational and regulatory requirements. DLP supports role-based access during incident response, ensures backup integrity, and maintains log files for monitoring and investigations. Netskope's ZTNA Next offers secure remote access to onprem and cloud-hosted private apps, integrating with NISTcompliant identity providers for authentication. It uses endto- end encryption and zero trust principles to control access, while logging all access attempts and enforcing policies on failed logins.	• All products • CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • ZTNA Next • CTO
	8.6 Use of application and system accounts and associated authentication factors is strictly managed.	Netskope's Cloud Security Posture Management (CSPM) safeguards critical IaaS platforms by monitoring for misconfigurations and ensuring compliance with organizational and regulatory standards. It scans cloud storage to prevent data exfiltration and integrates with Cloud Ticket Orchestrator for automated alerts and remediation. SaaS Security Posture Management (SSPM) monitors SaaS functions to avoid misconfigurations, provides detailed remediation instructions, and integrates with Cloud Ticket Orchestrator to automate responses. Detected misconfigurations improve security rules.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • ZTNA Next • Advanced DLP • CTO

Requirement		Netskope Response	Products
		Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention engine which secures data across the web, cloud applications, and endpoint devices using machine learning to classify and protect sensitive information. Contextaware policies protect data in real-time, enforce role-based access, and ensure backup integrity. DLP can also detect and prevent unauthorized sharing of passwords and authenticators. ZTNA Next offers secure remote access to both on-prem and cloud-hosted private apps, using NIST-compliant identity providers and zero trust principles.	
9. Restrict Physical Access to Cardholder Data	9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.	Netskope enforces organizational policies and assists in policy adherence through pop-up banners and coaching pages, notifying employees of potential infringements. Cloud Security Posture Management (CSPM) continuously monitors mission-critical IaaS platforms to prevent misconfigurations and data exfiltration, ensuring compliance with organizational, regulatory, and industry standards. CSPM integrates with Netskope's Cloud Ticket Orchestrator to send alerts and automate remediation. Similarly, SaaS Security Posture Management (SSPM) monitors SaaS functions, preventing misconfigurations and integrating with the Cloud Ticket Orchestrator for automated remediation. SSPM also allows for conversion of detected misconfigurations into new rules. Netskope's Advanced Analytics maps organizational data flows, assesses cloud risk, and tracks security trends, helping administrators monitor app usage, threats, policies, and user impact.	• All products • CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • Advanced Analytics • CTO
	9.2 Physical access controls manage entry into facilities and systems containing cardholder data.	Netskope's products do not map to this requirement	
	9.3 Physical access for personnel and visitors is authorized and managed.	Netskope's products do not map to this requirement	
	9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.	Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention engine which ensures comprehensive data security across web, cloud apps, and devices, leveraging machine learning to identify, classify, and protect sensitive data per organizational or regulatory demands. Contextaware policies integrate user, device, app, network, and action data to protect information in real time, employing methods like data obfuscation, encryption, or action blocking. DLP supports role-based access during incident responses, ensures the integrity of backups, and utilizes dedicated log repositories to support forensic investigations and compliance needs.	• CASB • NG-SWG • DLP

Requirement		Netskope Response	Products
		Netskope's Next-Generation Secure Web Gateway (NG-SWG) integrates with NIST-compliant identity providers, extending Single Sign-On (SSO) and Multi-Factor Authentication (MFA) across various apps and services. It monitors over 100 inline activities, establishing a user activity baseline to detect anomalies and applying granular policy controls. Beyond "allow" or "block" rules, NG-SWG offers context-aware responses to risky behaviors such as requiring a stepped-up MFA, suggesting safer alternatives, or referring users for cybersecurity training. NG-SWG generates alerts and reports based on customizable thresholds for SIEM integration and detailed event logging for user action non-repudiation.	
	9.5 Point of interaction (POI) devices are protected from tampering and unauthorized substitution.	Netskope's Cloud Access Security Broker (CASB) provides comprehensive monitoring and control over SaaS and IaaS activities, tracking user, device, instance, and actions, and applying real-time activity-level and data loss prevention controls. CASB aids in asset inventory, third-party risk management, business continuity, and acquisition strategy by inventorying apps and cloud services and assessing their criticality. Netskope's Next-Generation Secure Web Gateway (NG-SWG) supports integration with third-party identity providers, extending SSO/MFA across web and cloud apps, and detects and logs user activities to base granular policy controls and respond to risky behaviors. Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations, ensuring compliance with access management policies and regulatory standards. It scans cloud storage to prevent data exfiltration and integrates with Cloud Ticket Orchestrator for alerts and automation. SaaS Security Posture Management (SSPM) prevents misconfigurations in SaaS applications and integrates with automated remediation tools. Advanced User Entity and Behavior Analytics (UEBA) use ML models to detect anomalies and insider threats, providing a dynamic User Confidence Index. Netskope's Device Intelligence categorizes and controls access for devices connecting to the network, detecting anomalies, and integrating with incident response tools.	• CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • Advanced UEBA • Device Intelligence • CTO

REGULARLY MONITOR AND TEST NETWORKS

Requirement		Netskope Response	Products
10. Log and Monitor All Access to System Components and Cardholder Data	10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.	Netskope enforces organizational policies by notifying employees of potential policy breaches through pop-up banners and coaching pages. Netskope's CASB monitors and logs SaaS and IaaS activities including user details and applies real-time controls, also offering business justification or training for policy adherence. Netskope's NG-SWG decodes over 100 inline activities, detecting anomalous behavior and applying granular contextaware controls such as stepped-up multi-factor authentication or referring the user for just-in-time cybersecurity training. Cloud Security Posture Management ensures compliance with organizational and regulatory standards by preventing misconfigurations and data exfiltration, integrating with Cloud Ticket Orchestrator for alerts and automation. SaaS Security Posture Management similarly prevents misconfigurations in critical SaaS functions, with automated remediation and rule improvements. Advanced Analytics maps data flows across web and cloud services, tracking cloud app usage and security trends. Proactive Digital Experience Management provides visibility from endpoints to the cloud, enabling automated troubleshooting and performance issue mitigation.	• All products • CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • Advanced Analytics • CTO • P-DEM
	10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.	Netskope's CASB monitors and logs activities in SaaS and IaaS services, and its NG-SWG monitors user activities, detecting anomalies and applying context-aware policy controls. ZTNA Next provides secure remote access to apps, leveraging NIST-aligned identity providers, and enforcing zero trust principles. Device Intelligence identifies and classifies devices, creating behavior baselines and detecting anomalies, and can integrate with incident response tools for security alerts. Cloud Security Posture Management (CSPM) ensures these platforms are secure and compliant by preventing misconfigurations and automating remediation through the Cloud Ticket Orchestrator. SaaS Security Posture Management (SSPM) continuously monitors SaaS configurations for compliance, with automated remediation efforts supported by the Cloud Ticket Orchestrator.	• CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • ZTNA Next • Device Intelligence • CTO

Requirement		Netskope Response	Products
	10.3 Audit logs are protected from destruction and unauthorized modifications.	Netskope's CASB triggers alerts and exports them to the organization's Security Incident and Event Management (SIEM) tools to support automated incident responses. It also aids in performing "lessons learned" exercises and generating progress reports. Netskope's Cloud Security Posture Management continuously monitors mission-critical IaaS platforms to prevent misconfigurations and ensure compliance with organizational policies and industry standards. This service also scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for automating remediation efforts. Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention engine which safeguards data across web, cloud applications, and endpoint devices, employing machine learning to identify and protect sensitive information based on context-aware policies. It can obfuscate, encrypt, or block data actions, and enforce role-based access during incident responses. Additionally, it ensures the integrity of backups and maintains logs for continuous monitoring and forensic investigations.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • CTO
	10.4 Audit logs are reviewed to identify anomalies or suspicious activity.	Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) continuously monitor critical cloud infrastructure and applications to prevent misconfigurations and ensure compliance with organizational and regulatory standards. CSPM scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator to automate remediation. SSPM also provides alerts with remediation instructions and integrates with the Cloud Ticket Orchestrator for automated responses. Netskope's Cloud Firewall enforces security policies on egress traffic, disrupts DNS attacks, and generates event logs for incident response. Device Intelligence identifies and classifies devices connecting to the network, detecting anomalies and applying zero trust principles. Advanced Analytics maps data flows and assesses cloud risks, providing administrators with a dashboard to track security trends. Netskope's DLP detects and prevents the sharing of sensitive data. Netskope's Cloud Ticket Orchestrator automates incident response by generating service tickets and enforcing rolebased access controls.	• All products • CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • ZTNA Next • CTO
	10.5 Audit log history is retained and available for analysis.	Netskope's Cloud Security Posture Management (CSPM) continuously monitors mission-critical IaaS platforms to prevent misconfigurations and ensure compliance with access management policies and regulatory standards. CSPM also scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator to automate alerts and remediation. Netskope's SaaS Security Posture Management (SSPM) monitors SaaS functions to prevent misconfigurations and ensure compliance. SSPM also integrates with Cloud Ticket Orchestrator for automated remediation and can convert detected misconfigurations into new security rules.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO

Requirement		Netskope Response	Products
		Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention engine which safeguards data across web, cloud apps, and endpoints, using machine learning to identify and protect sensitive information based on policies and context. DLP enforces role-based access, ensures the integrity of backups, and maintains log files for continuous monitoring and investigations.	
	10.6 Timesynchronization mechanisms support consistent time settings across all systems.	Netskope's Cloud Security Posture Management (CSPM) continuously monitors an organization's IaaS platforms to prevent misconfigurations and ensure compliance with organizational, regulatory, and industry standards. It scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator to send alerts and automate remediation. Netskope's SaaS Security Posture Management (SSPM) monitors SaaS functions to prevent misconfigurations, offers guidance for remediation, and integrates with the Cloud Ticket Orchestrator to automate responses. Previously detected misconfigurations can be converted into new security rules. Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention engine which protects data in use, in transit, or at rest across web, cloud applications, and endpoint devices using machine learning to identify and classify sensitive data. DLP enforces role-based access and contextaware policies to protect data in real time and supports incident response, backup integrity, and forensic investigations.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO
	10.7 Failures of critical security control systems are detected, reported, and responded to promptly.	The Next-Gen Secure Web Gateway (NG-SWG) logs user activities, detects anomalies, and enforces granular policy controls, integrating with identity providers for extended security measures. Netskope's Cloud Access Security Broker (CASB) monitors activities within SaaS and IaaS, applies real-time controls, and supports asset inventory and third-party risk management. It also integrates with Security Incident and Event Management (SIEM) tools for automated incident responses. The Cloud Confidence Index (CCI) scores vendors based on various security and legal criteria. Netskope's Cloud Security Posture Management (CSPM) secures IaaS and cloud storage against misconfigurations and data exfiltration, with capabilities for automated remediation. SaaS Security Posture Management (SSPM) ensures SaaS configurations align with policies, automating remediation via Cloud Ticket Orchestrator.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • DLP • SSPM • Advanced Analytics • Advanced UEBA • Threat Protection • CLS • CTO • P-DEM

Requirement		Netskope Response	Products
		INetskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention engine which protects data across various environments using machine learning and contextaware policies. Advanced User Entity and Behavior Analytics (UEBA) provide in-depth user behavior insights, aiding in insider threat detection. Advanced Analytics tracks data flows and security trends. Standard Threat Protection defends against malware and phishing, integrating with broader Netskope tools for layered security. The Cloud Log Shipper and Cloud Ticket Orchestrator enhance incident response capabilities, while Proactive Digital Experience Management ensures optimal user experience.	
11. Test Security of Systems and Networks Regularly	11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.	Netskope enforces organizational policies through pop-up banners and coaching pages that notify employees of potential infringements. Cloud Confidence Index (CCI) scores SaaS applications, helping organizations assess vendor risks based on various security and legal criteria. Netskope's Cloud Access Security Broker (CASB) assists with asset inventory, third-party risk management, and business continuity planning by identifying and evaluating managed and unmanaged apps. It generates alerts for the Security Incident and Event Management tool to automate incident response and recovery. Netskope's Cloud Security Posture Management continuously monitors IaaS platforms and prevents misconfigurations, ensuring compliance with organizational and regulatory standards. It also scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for automated remediation. Similarly, its SaaS Security Posture Management alerts organizations to misconfigurations and integrates with the Cloud Ticket Orchestrator for remediation efforts. Netskope Device Intelligence catalogues all devices on the network, classifies them, and isolates risky ones. It uses AI/ML to detect anomalies and enforce zero trust principles, creating security alerts through incident response tools. Netskope's Advanced Analytics maps data flows, assesses cloud risk, and tracks security trends through a detailed dashboard.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO
	11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.	Netskope's Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations, aligning with organizational policies and industry standards, and preventing data exfiltration. It integrates with Cloud Ticket Orchestrator for alerts and automated remediation. Netskope's SaaS Security Posture Management (SSPM) similarly monitors SaaS functions, offering step-by-step misconfiguration fixes and integration with Cloud Ticket Orchestrator for automated responses.	• Public Cloud Security • CSPM • Cloud Firewall • SD-WAN

Requirement		Netskope Response	Products
		Previously detected issues can lead to new security rules. Netskope's Borderless SD-WAN extends network perimeters to any device or user globally, steering traffic through the New Edge network for reliable connectivity and uniform policy enforcement based on user, location, and more. Netskope's Cloud Firewall applies security policies to egress traffic without routing through on-prem security, protecting against DNS attacks and integrating event logs with SIEM tools. Netskope Device Intelligence catalogs all network devices, detecting anomalies through AI/ML and enforcing granular controls per zero trust principles. It isolates risky devices and integrates with incident response tools for alert generation.	• SSPM • Device Intelligence • CTO
	11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.	Netskope's Cloud Confidence Index (CCI) evaluates SaaS applications based on security policies, certifications, audits, and privacy concerns, aiding organizations in assessing risks. Netskope's Cloud Security Posture Management (CSPM) oversees IaaS platforms to prevent misconfigurations and ensure adherence to policies and regulatory standards, as well as scanning cloud storage to avert data breaches. CSPM integrates with Netskope's Cloud Ticket Orchestrator to automate alerts and remediation. Similarly, Netskope's SaaS Security Posture Management (SSPM) monitors SaaS functions, providing remediation instructions and generating service tickets through integration with the Cloud Ticket Orchestrator. Detected misconfigurations can improve security rules. Netskope Device Intelligence identifies and classifies devices, segments networks to isolate risky devices, and uses AI/ML to establish normal behavior baselines, detect anomalies, and apply zero trust principles. It integrates with incident response tools for generating security alerts. Netskope's Cloud Risk Exchange normalizes risk scores from third-party vendors to enforce adaptive controls mitigating risky users, apps, and devices. Netskope's Cloud Threat Exchange allows for near real-time sharing of threat indicators among customers and partners, integrating with organizational SIEM tools.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • SSPM • Device Intelligence • CRE • CTE • CTO
	11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.	The Netskope platform aids organizations in optimizing security tests and exercises by inventorying unmanaged apps and devices and assigning them risk-based scores. Cloud Security Posture Management (CSPM) continuously monitors critical IaaS platforms, preventing misconfigurations and ensuring compliance with organizational and regulatory standards. CSPM also scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for automated alerts and remediation. Similarly,	• All products • Public Cloud Security • CSPM • SSPM • CTO

Requirement		Netskope Response	Products
		Netskope's SaaS Security Posture Management (SSPM) monitors essential SaaS functions to prevent misconfigurations, offering step-by-step remediation instructions. SSPM also integrates with the Cloud Ticket Orchestrator for automated ticket generation and remediation. Misconfigurations detected can be used to create new security rules for ongoing improvement.	
	11.5 Network intrusions and unexpected file changes are detected and responded to.	Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention engine which provides comprehensive security for organizational data in use, in transit, or at rest across the web, public and private cloud applications, and endpoint devices. Netskope provides solutions encompassing cybersecurity policy communication, data privacy training, and awareness through pop-up banners and coaching pages that notify and guide employees on potential policy breaches. Netskope's Borderless SD-WAN extends the network perimeter globally, ensuring secure, high-availability connectivity for web and cloud applications, and enforcing uniform policy controls based on adaptive trust criteria. Netskope's Cloud Firewall secures outbound web and cloud traffic by applying security policies, inspecting DNS queries, and facilitating incident response through integration with SIEM tools. User Entity and Behavior Analytics establishes behavior baselines to detect anomalies and adjust policies accordingly. Standard Threat Protection guards against known and new malware, phishing, and integrates with Netskope's security tools to provide defense-in-depth. Advanced Threat Protection enhances Standard Threat Protection with advanced malware detection techniques like deobfuscation and multi-stage sandboxing. Device Intelligence identifies and classifies network devices, using AI/ML to detect anomalies and enforce zero-trust access controls.	• All products • CASB • NG-SWG • Cloud Firewall • SD-WAN • UEBA • Advanced Threat Protection • Device Intelligence • Threat Protection
	11.6 Unauthorized changes on payment pages are detected and responded to.	Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) systems continuously monitor and protect mission-critical IaaS and SaaS platforms to prevent misconfigurations and ensure compliance with organizational policies and regulatory standards. The CSPM scans cloud storage to prevent data exfiltration, while both CSPM and SSPM provide alerts and automate remediation through integration with Netskope's Cloud Ticket Orchestrator. This tool generates service tickets and automates workflow responses to security alerts, playing a key role in an organization's incident response and recovery plan by enforcing role-based access controls. Netskope's Cloud Ticket Orchestrator also converts detected misconfigurations into new security rules, enhancing future security measures.	• Public Cloud Security • CSPM • SSPM • Device Intelligence • CTO

MAINTAIN AN INFORMATION SECURITY POLICY

Requirement		Netskope Response	Products
12. Support Information Security with Organizational Policies and Programs	12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.	Netskope enforces organizational policies and aids communication through pop-up banners and coaching pages to notify employees of potential policy infringements. Advanced Analytics maps data flows across web and cloud services, assessing data sensitivity and cloud risk. The dashboard tracks security trends, including app usage, threats, policies triggered, and user impact. Cloud Security Posture Management (CSPM) monitors IaaS platforms to prevent misconfigurations and ensure compliance with organizational and regulatory standards. CSPM scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator to automate alerts and remediation. Netskope's SaaS Security Posture Management (SSPM) also prevents misconfigurations in SaaS functions, ensuring compliance and providing step-by-step remediation instructions. SSPM integrates with the Cloud Ticket Orchestrator to automate service tickets and remediation efforts. Detected misconfigurations can be converted into new security rules.	• All products • CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • Advanced Analytics • CTO
	12.2 Acceptable use policies for end-user technologies are defined and implemented.	Netskope's Cloud Access Security Broker (CASB) monitors activities in SaaS and IaaS services, logging user, device, instance, and action data. It allows real-time data loss prevention controls and can request justifications or provide training. Netskope's Next-Gen Secure Web Gateway (NGSWG) works with third-party identity providers, extending SSO/MFA across web and cloud apps. It logs over a hundred activities, establishes user behavior baselines, and detects anomalies, applying context-aware policy controls like multifactor authentication or policy violation notifications. Netskope's Cloud Firewall applies security policies to outgoing traffic without backhauling, inspecting queries to prevent DNS attacks. It integrates with SIEM tools for incident response. Their User Entity and Behavior Analytics (UEBA) tracks behavior across cloud apps to detect anomalies and adjust access dynamically. Advanced UEBA includes additional ML-based models and a User Confidence Index (UCI) to quantify risk and adapt policies, aiding in insider threat detection. Netskope's Zero Trust Network Access (ZTNA) provides secure remote access to private apps, supporting end-to-end encryption and logging all access attempts, enforcing organizational login policies based on zero trust principles.	• CASB • NG-SWG • Cloud Firewall • UEBA • ZTNA Next • Advanced UEBA
	12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.	Netskope's Cloud Access Security Broker (CASB) aids in asset inventory, acquisition strategy, third-party risk management, and business continuity by identifying and monitoring managed and unmanaged applications, and the Cloud Confidence Index (CCI) evaluates SaaS applications, examining factors like security policies, certifications, and legal concerns to help organizations assess risks.	• CASB • NG-SWG • Public CloudSecurity • CSPM

Requirement		Netskope Response	Products
		Netskope's Cloud Security Posture Management (CSPM) prevents misconfigurations in mission-critical IaaS platforms and scans cloud storage to prevent data exfiltration. CSPM integrates with Cloud Ticket Orchestrator for alerts and automated remediation. Similarly, SaaS Security Posture Management (SSPM) continuously monitors SaaS functions, providing remediation instructions and integrating with Cloud Ticket Orchestrator. Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention (DLP) engine which uses machine learning to protect sensitive data across various environments, applying context-aware policies to mitigate risks in real-time. The DLP enforces role-based access and supports incident response and forensic investigations. Remote Browser Isolation protects against risky web sites by containing malware in secure sandboxes. Advanced User Entity and Behavior Analytics (UEBA) provides dynamic risk scores for users to detect insider threats. Netskope's Device Intelligence catalogs devices, detecting anomalies and applying zero trust principles. Advanced Analytics maps data flows and assesses cloud risks, while Standard Threat Protection guards against malware and phishing. Integrating with threat intelligence feeds, it supports a layered security approach. The Cloud Risk Exchange normalizes risk scores from thirdparty vendors, enforcing adaptive controls to mitigate risks.	• Cloud Confidence Index (CCI) • DLP • RBI • SSPM • Advanced Analytics • Advanced UEBA • Device Intelligence • Threat Protection • CRE • CTO
	12.4 PCI DSS compliance is managed.	Netskope's Cloud Security Posture Management (CSPM) safeguards critical IaaS platforms by preventing misconfigurations and ensuring compliance with organizational policies and industry standards. It routinely scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for alerting and automating remediation efforts. Similarly, Netskope's SaaS Security Posture Management (SSPM) monitors critical SaaS functions to prevent misconfigurations and ensure proper use of assets and data. SSPM provides step-by-step remediation instructions and can automate service tickets via Cloud Ticket Orchestrator. Additionally, previously detected misconfigurations can be turned into new security rules to enhance overall protection.	• Public Cloud Security • CSPM • SSPM • CTO
	12.5 PCI DSS scope is documented and validated.	Netskope's Cloud Security Posture Management (CSPM) monitors and secures an organization's critical IaaS platforms by preventing misconfigurations and ensuring compliance with access management policies and industry standards. CSPM also scans cloud storage buckets to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator to automate alerts and remediation. Similarly, Netskope's SaaS Security Posture Management (SSPM) monitors critical SaaS functions to prevent misconfigurations and ensure compliance, providing step-bystep remediation instructions. SSPM also integrates with the Cloud Ticket Orchestrator for automated service tickets and remediation. Additionally, SSPM can convert previously detected misconfigurations into new security rules to enhance future security measures.	• Public Cloud Security • CSPM • SSPM • CTO

Requirement		Netskope Response	Products
		SSPM also integrates with the Cloud Ticket Orchestrator for automated service tickets and remediation. Additionally, SSPM can convert previously detected misconfigurations into new security rules to enhance future security measures.	
	12.6 Security awareness education is an ongoing activity.	Netskope's product suite enhances cybersecurity and data privacy by using pop-up banners and coaching pages to notify employees of policy breaches, request justifications, and direct users to additional training. NG-SWG integrates with NIST-compliant third-party identity providers, enabling SSO/MFA for web and cloud apps. NGSWG logs over 100 activities, establishes user baselines to detect anomalies, and applies context-aware controls, such as requiring additional authentication or suggesting safer alternatives. Furthermore, Netskope's advanced User Entity and Behavior Analytics (UEBA) employs multiple ML-based models and features the User Confidence Index (UCI), a dynamic risk score for users based on behavior. UEBA adapts policies, recommends training to mitigate insider threats, and can share insider threat information through Netskope's Cloud Exchange.	• All products • CASB • NG-SWG • Advanced UEBA
	12.7 Personnel are screened to reduce risks from insider threats.	Netskope offers a suite of security solutions, including CASB, NG-SWG, ZTNA Next, and UEBA. Their CASB monitors and logs activities in SaaS and IaaS services at a detailed level, providing real-time controls such as requesting business justifications or policy training. The NG-SWG integrates with NIST-compliant identity providers, supports SSO/MFA, and decodes over 100 activities to baseline user behavior, applying context-aware controls and generating customizable reports for incident response. Standard UEBA tracks user behavior across various apps, establishes a baseline, and uses adaptive policies based on deviations, while Advanced UEBA employs more ML models and provides a User Confidence Index to assess and mitigate insider threats, sharing insights via the Cloud Risk Exchange. ZTNA Next offers secure remote access to private apps from any device, integrates with identity providers, uses end-to-end encryption, and enforces granular zero trust-based access controls, logging all access attempts and adherence to policies on failed logins.	• CASB • NG-SWG • UEBA • ZTNA Next • Advanced UEBA
	12.8 Risk to information assets associated with thirdparty service provider (TPSP) relationships is managed.	Netskope's Cloud Access Security Broker (CASB) aids in asset inventory, acquisition strategy, third-party risk management, and business continuity by cataloging managed and unmanaged applications and cloud services, and categorizing them by usage and risk level. CASB also integrates with Security Incident and Event Management tools to prompt automated responses, leverage event logs for lessons learned, and generate Progress and Action On Milestones reports. Netskope evaluates SaaS applications through its Cloud Confidence Index (CCI), assessing factors like security policies, certifications, audit capabilities, and legal concerns to help organizations gauge vendor risk.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • SSPM • ZTNA Next • CTO

Requirement		Netskope Response	Products
		The Cloud Security Posture Management (CSPM) system continuously monitors mission-critical IaaS platforms, preventing misconfigurations and ensuring compliance with organizational policies and standards. It also scans cloud storage to prevent data breaches and integrates with Cloud Ticket Orchestrator for alerts and automated remediation. The SaaS Security Posture Management (SSPM) system performs similar functions for SaaS, offering step-by-step remediation for misconfigurations and the ability to create new security rules from findings. ZTNA Next provides secure remote access to private apps, supporting NIST-compliant authentication, end-to-end encryption, and zero trust principles to control access and privileges. It logs all access attempts and enforces policies on failed logins.	
	12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.	Netskope provides comprehensive security and risk management solutions for organizations using cloud services. Their Cloud Confidence Index (CCI) rates SaaS applications based on security policies, certifications, audits, legal/privacy concerns, and more. The Cloud Access Security Broker (CASB) offers detailed monitoring, logging, and real-time data loss prevention across SaaS and IaaS services, aiding in inventory, acquisition strategy, and risk management. Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) continuously monitor IaaS and SaaS platforms to prevent misconfigurations, alerting and automating remediation via Cloud Ticket Orchestrator. Their Data Loss Prevention (DLP) engine protects data across all mediums using machine learning for identifying and classifying sensitive data. The Next-Generation Secure Web Gateway (NG-SWG) isolates risky websites, while User Entity and Behavior Analytics (UEBA) tracks user behavior for anomaly detection. Advanced Threat Protection defends against novel malware with advanced techniques. Device Intelligence monitors and manages devices connecting to the network to maintain security. Netskope's Advanced Analytics assesses data flows and cloud risk, offering a dashboard for tracking security trends and providing an integrated real-time threat protection system with Cloud Threat Exchange and other security tools.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • DLP • RBI • SSPM • UEBA • Advanced Analytics • Advanced Threat Protection • Device Intelligence • Threat Protection • CTO
	12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.	Netskope products provide comprehensive insights and rich metadata for traffic across web, SaaS, IaaS, and custom apps, aiding in estimating the scope of cyber incidents by identifying affected systems, users, data, and services. Netskope's Cloud Access Security Broker (CASB) generates alerts for Security Incident and Event Management (SIEM) tools to enable automated incident response and recovery. The Next-Generation Secure Web Gateway (NG-SWG) integrates with NIST-compliant identity providers, extending SSO/MFA across managed and unmanaged apps, and logs over 100 activities to detect anomalies.	• All products • CASB • NG-SWG • Advanced Analytics • CLS • CTO

Requirement		Netskope Response	Products
		NG-SWG's contextaware controls can require multi-factor authentication or notify users of policy violations, offering safer alternatives or just-in-time training. The Cloud Log Shipper exports logs from various Netskope tools to SIEMs, and the Cloud Ticket Orchestrator automates incident response workflows by creating service tickets and enforcing role-based access controls. These integrations and automations facilitate detailed incident analysis and response, ensuring robust cybersecurity management.	

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.