netskope

Compliance Series

FedRAMP High

Control Mapping to Netskope Products

TABLE OF CONTENTS

INTRODUCTION

FedRAMP is the Federal Risk and Authorization Management Program, a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

FedRAMP controls are currently derived from the 5th revision of the National Institute of Standards and Technology (NIST) Special Publication 800-53. They encompass 18 of the 20 control families of the NIST 800-53 framework, as well as specific FedRAMP-assigned control enhancements, including additional requirements and guidance.

Depending on the desired or required level of stringency, organizations can seek FedRAMP authorization at the Low, Moderate, or High levels. Netskope is one of only a few dozen private companies to have attained FedRAMP High authorization, and Netskope engineers on the dedicated FedRAMP team have the requisite security clearance to support sensitive environments and data.

HOW TO USE THIS GUIDE

The tables below break down each control family that appears in the FedRAMP High controls. Individual control identifiers begin with the family abbreviation, followed by the specific control number, followed by the enhancement in parentheses. For example, AC-2(4) would be the fourth enhancement in the second control of the Access Control family.

Following the control identifier is the text of the requirement. Where there are any specific FedRAMP-assigned modifications to the requirement, those have already been incorporated into the text.

Following the requirement is Netskope's response and a list of Netskope products that meet or assist with fulfilling the requirements of the control.

While there are some controls to which Netskope does not map, deploying Netskope's unified SASE architecture can propel an organization toward substantial FedRAMP compliance.

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
Threat/Risk Sharing	Cloud Exchange Cloud Threat Exchange (CTE) Cloud Risk Exchange (CRE)
IT/IoT/OT Security	Device Intelligence
Third-Party Risk Management/Supply Chain	Cloud Confidence Index (CCI)
User Risk Metrics	User Confidence Index (UCI)

The following table will break down each Family, Control by Control, mapping specific Netskope products and use cases to individual requirements.

ACCESS CONTROL

Control	Requirements(s)	Netskope Response	Products
AC-1	a. Develop, document, and disseminate to organization-defined personnel or roles: 1. An organization-level; mission/ business process-level; system-level access control policy that: a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the access control policy and procedures; and c. Review and update the current access control: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes.	Netskope enforces organizational policies and uses pop-up banners and coaching pages to notify employees of policy infringements, suggest safer alternatives to risky actions, or refer users for further cybersecurity training. Netskope's CASB and NG-SWG feature a data loss prevention (DLP) engine that utilizes machine learning to protect sensitive data across web, cloud applications, and endpoints, with real-time and context-aware policies. CASB aids in asset inventory, acquisition strategies, third-party risk management, and business continuity by assessing the criticality of cloud apps and services based on usage and risk. Private Access secures remote access to apps with end-to-end encryption and granular access controls based on zero trust principles. It logs access attempts and enforces organizational login policies. Netskope's Advanced Analytics maps data flows and assesses cloud risk, allowing administrators to monitor security trends via a comprehensive dashboard. Netskope's Cloud Log Shipper can send event and alert logs to the organization's SIEM tool, and the Cloud Ticket Orchestrator can generate service tickets and automate incident response workflows.	• CASB • NG-SWG • Public Cloud Security • DLP • Private Access • Advanced Analytics • CLS • CTO
AC-2	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require organization-defined prerequisites and criteria for group and role membership; d. Specify: 1. Authorized users of the system; 2. Group and role membership; and	Netskope's security solutions, including its CASB, NG-SWG, DLP, and Private Access, all support role-based access control (RBAC) to enforce organizational access management policies based on the principle of least privilege. Netskope's CASB provides real-time monitoring, logging, and activity-level controls on SaaS and IaaS services, enabling data loss prevention and requiring business justifications or training on policy adherence. NG-SWG integrates with third-party identity providers to extend SSO/MFA across web and cloud apps, logging over 100 activities and establishing user behavior baselines to detect anomalies and apply context-aware controls such as advanced authentication or policy training. Its detailed logging and reporting capabilities enhance incident response and user action traceability.	• CASB • NG-SWG • DLP • Private Access • Public Cloud Security • Advanced UEBA • Device Intelligence • CTO

Control	Requirements(s)	Netskope Response	Products
	3. Access authorizations (i.e., privileges) and organization-defined attributes (as required) for each account; e. Require approvals by organization-defined personnel or roles for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with organization-defined policy, procedures, prerequisites, and criteria; g. Monitor the use of accounts; h. Notify account managers and organization-defined personnel or roles within: 1. twenty-four (24) hours] when accounts are no longer required; 2. eight (8) hours when users are terminated or transferred; and 3. eight (8) hours when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Organization-defined attributes (as required); j. Review accounts for compliance with account management requirements monthly for privileged accessed, every six (6) months for non-privileged access; k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and l. Align account management processes with personnel termination and transfer processes.	Private Access additionally provides secure remote access to private apps hosted on-premises or in the cloud, integrating with NIST-compliant identity providers for authentication. It employs end-to-end encryption to secure data and enforces granular access controls. Private Access also logs all access attempts and supports RBAC to adhere to organizational policies. Netskope's products do not map to this requirement. Netskope's Advanced User and Entity Behavior Analytics (UEBA) employs advanced machine learning models to detect anomalies. It includes the User Confidence Index (UCI), a risk score based on user behavior, which helps adapt policies, controls, and recommend security training to mitigate insider threats. The UCI can also integrate with Netskope's Cloud Exchange to share insider threat information across platforms. Device Intelligence catalogs all devices connecting to the network, creates behavior baselines, and applies zero trust principles to manage access based on detected anomalies. Cloud Ticket Orchestrator automates incident response by generating service tickets and enforcing role-based controls, integrating seamlessly into organizations' security infrastructures via the Netskope Cloud Exchange.	

Control	Requirements(s)	Netskope Response	Products
	AC-2(1): Support the management of system accounts using automated mechanisms.		
	AC-2(2): Automatically disable temporary and emergency accounts after no more than 24 hours from last use.		
	AC-2(3): Disable accounts 24 hours when the accounts have expired, are no longer associated with a user or individual, are in violation of organizational policy, or have been inactive for 35 days. **Additional FedRAMP Requirements and Guidance:** **Guidance**: For DoD clouds, see DoD cloud website for specific DoD requirements that go above and beyond FedRAMP https://public.cyber.mil/dccs/. **Requirement**: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the JAB/AO. Where user management is a function of the service, reports of activity of consumer users shall be made available. **(d) Requirement**: The service provider defines the time period of inactivity for device identifiers.		
	AC-2(4): Automatically audit account creation, modification, enabling, disabling, and removal actions.		
	AC-2(5): Require that users log out when inactivity is anticipated to exceed fifteen (15) minutes. **Guidance**: Use a shorter timeframe than AC-12.		
	AC-2(7): Establish and administer privileged user accounts in accordance with a role-based access scheme or an attribute-based access scheme. Monitor privileged role or attribute assignments. Monitor changes to roles or attributes. Revoke access when privileged role or attribute assignments are no longer appropriate.		

Control	Requirements(s)	Netskope Response	Products
	AC-2(9): Only permit the use of shared and group accounts that meet agency-defined conditions for establishing shared and group accounts. Consider the increased risk due to lack of accountability before permitting the use of shared or group accounts.		
	AC-2(11): Enforce organization-defined circumstances and/or usage conditions for organization-defined accounts.		
	AC-2(12): Monitor system accounts for agency-defined atypical usage, and report atypical usage of system accounts to agency-defined personnel or roles.		
	AC-2(13): Disable accounts of users posing a significant risk within one day of discovery of the risk.		
AC-3	Enforce approved authorizations for logical access to information and systems resources in accordance with applicable access control policies.	Netskope's Private Access provides remote access to private applications hosted on-premises or in the cloud from any device, anywhere. It integrates with NIST-compliant identity providers for secure authentication and uses end-to-end encryption. Granular controls based on zero trust principles manage access and privileges, while all access attempts are logged to enforce organizational policies on login failures. Concurrently, Netskope Device Intelligence identifies and categorizes all devices on the network, segmenting them to isolate risky ones. Its AI/ML engine establishes a normal behavior baseline, detects anomalies, and enforces access controls per zero trust principles. Device Intelligence can integrate with incident response tools to generate security alerts based on organizational criteria.	• Private Access • Device Intelligence
AC-4	Enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based on organization-defined information flow control policies..	Netskope's Cloud Firewall enforces organizational security policies on outbound traffic to web and cloud applications across all ports and protocols, eliminating the need for on-premises security backhauling. It protects against DDoS, man-in-the-middle, and DNS attacks by inspecting queries for harmful, newly registered, or algorithmically generated domains. Additionally, event logs from Netskope's Cloud Firewall can be integrated with an organization's SIEM tool to aid in incident response and recovery.	• Cloud Firewall • Advanced Analytics • DLP

Control	Requirements(s)	Netskope Response	Products
		Netskope's Cloud Firewall enforces organizational security Netskope's Advanced Analytics maps an organization's data flows across web and cloud services, characterizing data by category and sensitivity. Advanced Analytics also assesses cloud risk by cataloguing and characterizing cloud app usage, and the product dashboard allows administrators to track security trends by number of apps accessed, threats detected, policies triggered, and users impacted. Netskope's DLP uses machine learning to identify, classify, and protect sensitive data based on organizational or regulatory requirements, and context-aware policies incorporate information on users, devices, apps, networks, and actions to protect data in real time, such as by obfuscating personal data, encrypting a sensitive file, or blocking certain actions.	
	AC-4(4): Prevent encrypted information from bypassing intrusion detection mechanisms by: decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information. **Additional FedRAMP Requirements and Guidance:** **Requirement**: The service provider must support Agency requirements to comply with M-21-31 (https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf) and M-22-09 (https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf).	By default, all traffic steered through Netskope will be decrypted and analyzed via real-time protection policies.	• All products
	AC-4(21): Separate information flows logically or physically using organization-defined mechanisms and/or techniques to accomplish organization- defined required separations by types of information.	Netskope's Advanced Analytics maps data flows across the organization, and its Private Access and Cloud Firewall capabilities support network segmentation.	• Advanced Analytics • Private Access • Cloud Firewall

Control	Requirements(s)	Netskope Response	Products
AC-5	Identify and document separate duties of individuals to prevent harmful activity without collusion, and define system access authorizations to support separation of duties. Guidance: CSPs have the option to provide a separation of duties matrix as an attachment to the SSP..	Netskope's Next-Gen Secure Web Gateway (NG-SWG) supports NIST-compliant identity providers for extended SSO/MFA and logs over a hundred inline activities to detect anomalies and enforce granular policy controls based on context-aware assessments. NG-SWG can require multi-factor authentication for risky behaviors or provide user training for policy violations, feeding logs into the organization's SIEM for incident response. Netskope's CASB monitors and logs user activities across cloud services, enabling real-time data loss prevention and activity-level controls. Private Access offers secure remote access to private applications, using zero trust principles, and logs all access attempts. Device Intelligence identifies and classifies network devices, forming a baseline of normal behavior to detect anomalies and enforce access controls.	• Public Cloud Security • Private Access
AC-6	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	Netskope's Next Gen Secure Web Gateway (NG-SWG) supports NIST-compliant identity providers for extended SSO/MFA and logs over a hundred inline activities to detect anomalies and enforce granular policy controls based on context-aware assessments. NG-SWG can require multi-factor authentication for risky behaviors or provide user training for policy violations, feeding logs into the organization's SIEM for incident response. Netskope's CASB monitors and logs user activities across cloud services, enabling real-time data loss prevention and activity-level controls. Private Access offers secure remote access to private applications, using zero trust principles, and logs all access attempts. Device Intelligence identifies and classifies network devices, forming a baseline of normal behavior to detect anomalies and enforce access controls.	• CASB • NG-SWG • Public Cloud Security • Private Access • Device Intelligence
	AC-6(1): Authorize access for organization-defined individuals or roles to: (a) all functions not publicly accessible; and (b) all security-relevant information not publicly available. AC-6(2): Require that users of system accounts or roles with access to all security functions use non-privileged accounts or roles when accessing nonsecurity functionst. AC-6(3): Authorize network access to all privileged commands only for organization-defined compelling operational needs and document the rationale for such access in the security plan for the system.	Netskope's CASB, NG-SWG, and ZTNA Next all support role-based access control (RBAC) to aid organizations in implementing access management policies based on the principle of least privilege. This ensures users have only the permissions necessary for their roles, enhancing security across various platforms. Netskope's Cloud Access Security Broker (CASB) and Next Gen Secure Web Gateway (NG-SWG) provide comprehensive monitoring, logging, and security controls for both SaaS/IaaS services and web/cloud-based apps. CASB tracks user activities, device, instance, and actions, offering real-time data loss prevention and activity-level controls. NG-SWG integrates with third-party identity providers compliant with NIST standards, extends SSO/MFA, and logs over 100 inline activities. It establishes user activity baselines to detect anomalies and applies granular controls based on activity nature, data, or app instance.	• CASB • NG-SWG • Private Access • DLP • Public Cloud Security • CTO

Control	Requirements(s)	Netskope Response	Products
	AC-6(5): Restrict privileged accounts on the system to organization-defined personnel or roles. AC-6(7): Review at a minimum annually the privileges assigned to all users with privileges, and reassign or remove privileges if necessary to correctly reflect organizational mission and business needs. AC-6(8): Prevent any software except software explicitly documented from executing at higher privilege levels than users executing the software. AC-6(9): Log the execution of privileged functions. AC-6(10): Prevent non-privileged users from executing privileged functions..	Beyond basic allow/block rules, NG-SWG's context-aware controls can demand multi-factor authentication for risky behavior, notify users of policy violations, request a business justification for a risky action, suggest safer alternatives, or refer to cybersecurity training. It also generates customizable reports and alerts for SIEM integration, aiding in incident response and non-repudiation of user actions. Netskope's Private Access offers secure remote access to private apps from any device, integrating with third-party identity providers for secure authentication. It uses end-to-end encryption and granular controls based on zero trust principles to protect data and manage access. Private Access also logs access attempts and enforces policies on failed logins.	
AC-7	Enforce a limit of [organization-defined number] invalid logon attempts by a user during an organization-defined time period, and automatically lock the account or node for an organization-defined time period or until released by an administrator; delay next logon prompt per [organization-defined delay algorithm]; notify system administrator; take other organization-defined action when the maximum number of unsuccessful attempts is exceeded.	Private Access logs all access attempts and ensures compliance with organizational policies on failed login attempts. Netskope's Cloud Log Shipper can send event and alert logs to the organization's SIEM tool, and the Cloud Ticket Orchestrator can generate service tickets and automate incident response workflows .	• Private Access • CLS • CTO
AC-8	a. Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that: 1. users are accessing a U.S. Government System, 2. system usage may be monitored, recorded, and subject to audit, 3. unauthorized use of the system is prohibited and subject to criminal and civil penalties, and 4. use of system indicates consent to monitoring and recording.	Netskope's product suite enhances cybersecurity and data privacy by communicating policies, tracking acknowledgements, and facilitating training through pop-up banners and coaching pages. These features notify employees of potential infringements, request justifications for risky actions, provide notification banners, and refer users to third-party training as necessary. Netskope's Private Access offers secure remote access to private apps from any device, integrating with third-party identity providers for secure authentication. It uses end-to-end encryption and granular controls based on zero trust principles to protect data and manage access. Private Access also logs access attempts and enforces policies on failed logins.	• All products • Private Access

Control	Requirements(s)	Netskope Response	Products
	b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system. c. For publicly accessible systems, 1. display organization-defined system use notification message before granting further access to the publicly accessible system, 2. display any references to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities, and 3. include a description of the authorized uses of the system. **Additional FedRAMP Requirements and Guidance:** **Requirement**: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/AO. **Requirement**: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO. **Requirement**: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results is approved and accepted by the JAB/AO.		

Control	Requirements(s)	Netskope Response	Products
	Guidance: If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.		
AC-10	Limit the number of concurrent sessions to three sessions for privileged access and two sessions for non-privileged access.	Netskope's Private Access offers secure remote access to private applications, whether on-premises or cloud-hosted, from any device, anywhere. It integrates with NIST-compliant third-party identity providers for secure authentication and employs end-to-end encryption to safeguard data in use and transit. Utilizing zero trust principles, Private Access enforces granular controls to restrict access and privileges. It also logs all access attempts and can enforce organizational policies on failed login attempts.	• Private Access
AC-11	Prevent further access to the system by initiating a device lock after 15 minutes of inactivity, requiring the user to initiate a device lock before leaving the system unattended, and retain the device lock until the user reestablishes access using established identification and authentication procedures. AC-11(1): Conceal, via the device lock, information previously visible on the display with a publicly viewable image.	Netskope's products do not map to this requirement..	
AC-12	Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.	Private Access logs all access attempts and enforces organizational policies related to failed login attempts.	• Private Access
AC-14	a. Identify organization-defined user actions that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.	Netskope's CASB allows monitoring and logging of activities performed in SaaS and IaaS services–including information on user, device, instance, and action–and can apply activity-level and data loss prevention controls in real time, not just blocking an action but also requesting a business justification for risky actions or providing training on organization policy. The NG-SWG integrates with NIST-compliant identity providers, enhancing SSO/MFA for web and cloud apps. It monitors user activities, applying granular policy controls to detect anomalous behavior and enforce context-aware responses, such as stepped-up MFA or cybersecurity training. The NG-SWG also generates customizable reports and alerts to facilitate incident response and non-repudiation. Lastly, Private Access secures remote access to private apps, leveraging NIST-compliant identity providers and end-to-end encryption. It uses granular controls to limit access based on zero trust principles and logs all access attempts.	• CASB • NG-SWG • Private Access

Control	Requirements(s)	Netskope Response	Products
AC-17	Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access, and authorize each type of wireless access to the system prior to allowing such connections.	Netskope's Private Access offers secure remote access to private applications, whether on-premises or cloud-hosted, from any device and location. It integrates with NIST-compliant third-party identity providers for robust authentication, employs end-to-end encryption to secure data both in use and in transit, and enforces granular access and privilege controls based on zero trust principles. Private Access also logs all access attempts and can enforce organizational policies concerning failed login attempts.	• Private Access
	AC-17(1): Employ automated mechanisms to monitor and control remote access methods.		
	AC-17(2): Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions		
	AC-17(3) Route remote accesses through authorized and managed network access control points.		
	AC-17(4): Authorize the execution of privileged commands and accesses to security-relevant information via remote access only in a format that provides assessable evidence, and for organization-defined needs. Document the rationale for remote access in the security plan for the system.		
AC-18	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access, and b. Authorize each type of wireless access to the system prior to allowing such connections..	Netskope does not map to this requirement.	
	AC-18(1): Protect wireless access to the system using authentication of both users and devices and encryption.		
	AC-18(3): Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.		
	AC-18(4): Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.		

Control	Requirements(s)	Netskope Response	Products
	AC-18(5): Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.		
AC-19	a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices to include when such devices are outside of controlled areas, and b. Authorize the connection of mobile devices to organizational systems.	Netskope's Private Access offers remote access to private apps from any device, integrating with third-party identity providers for secure authentication. It employs end-to-end encryption, applies granular access controls based on zero trust principles, logs all access attempts, and enforces policies on failed login attempts. Netskope Device Intelligence catalogs all managed and unmanaged devices on the network, isolates risky devices, and uses AI/ML to establish normal device behavior and detect anomalies. It applies granular controls to enforce zero trust principles, and integrates with incident response tools to trigger security alerts based on organizational criteria.	• Private Access • Device Intelligence
	AC-19(5): Employ container-based encryption to protect the confidentiality and integrity of information on organization-defined mobile devices.	Netskope's products do not map to this requirement.	
AC-20	a. Establish organization-defined terms and conditions; Identify organization-defined controls asserted to be implemented on external systems, consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to: 1. Access the system from external systems; and 2. Process, store, or transmit organization-controlled information using external systems; or b. Prohibit the use of organizationally defined types of external systems. **AC-20 Additional FedRAMP Requirements and Guidance:** **Guidance**: The interrelated controls of AC-20, CA-3, and SA-9 should be differentiated as follows: AC-20 describes system access to and from external systems. CA-3 describes documentation of an agreement between the respective system owners when data is exchanged between the CSO and an external system.	Netskope products can be used to apply controls and baseline assessments required for and by suppliers in line with security requirements. Netskope CASB and Public Cloud Security can audit web and cloud applications and provide metadata to understand if suppliers are using underlying cloud infrastructure to support supply chain discovery. Netskope also offers reverse proxy capabilities to protect cloud applications along with Netskope's Zero Trust Network Access (Private Access) to manage suppliers' access to organizational assets. Netskope's CASB and Next Gen Secure Web Gateway (NG-SWG) use machine learning for comprehensive DLP across the web, cloud apps, and devices. Policies protect data in real time by obfuscating, encrypting, or blocking actions based on context. The DLP engine ensures role-based access, maintains backup integrity, and stores logs for continuous monitoring and forensic investigations.	• CASB • Public Cloud Security • NG-SWG • Cloud Confidence Index (CCI) • DLP • NG-SWG

Control	Requirements(s)	Netskope Response	Products
	SA-9 describes the responsibilities of external system owners. These responsibilities would typically be captured in the agreement required by CA-3.		
	AC-20(1): Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after: a. Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or b. Retention of approved system connection or processing agreements with the organizational entity hosting the external system.	Netskope Zero Trust Network Access (ZTNA) ensures that remote users only have access to the private applications that are provisioned via policy through an outbound connection, without the need for full network access.	• Private Access
	AC-20(2): Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using organization-defined policy.	Netskope's CASB and NG-SWG solutions integrate a data loss prevention (DLP) engine designed to safeguard organizational data across the web, cloud applications, and endpoint devices. Netskope's endpoint DLP provides monitoring and protection for endpoint data in use, including control for USB storage devices.	• CASB • NG-SWG • DLP
AC-21	a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for organization-defined information-sharing circumstances where user discretion is required; and b. Employ organization-defined automated mechanisms or manual processes to assist users in making information-sharing and collaboration decisions.	Netskope's Cloud Access Security Broker (CASB) and Next Gen Secure Web Gateway (NG-SWG) provide comprehensive monitoring and security for SaaS and IaaS services, logging user activities and applying real-time data loss prevention (DLP) controls. Netskope's DLP engine uses machine learning to protect sensitive data across various environments by classifying, encrypting, or obfuscating data based on regulatory and organizational policies. These tools enforce role-based access and maintain backup integrity, while supporting continuous monitoring and forensic investigations. NG-SWG integrates with third-party identity providers to extend SSO/MFA across web and cloud apps, decoding numerous activities to build a baseline of user behavior. It detects anomalies and applies nuanced policy controls, such as requesting business justifications for risky actions, requiring a stepped-up authentication, or referring the user for further training. Advanced User and Entity Behavior Analytics (UEBA) uses machine learning for enhanced anomaly detection, incorporating a User Confidence Index to quantify risk and adapt policies. This can be integrated with Netskope's Cloud Exchange to share insider threat information.	• CASB • NG-SWG • DLP • Advanced UEBA

Control	Requirements(s)	Netskope Response	Products
AC-22	Designate individuals authorized to make information publicly accessible; b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and d. Review the content on the publicly accessible system for nonpublic information at least quarterly and remove such information, if discovered.	Netskope's Cloud Access Security Broker (CASB) and Next Generation Secure Web Gateway (NG-SWG) leverage an advanced data loss prevention (DLP) engine to secure data in use, in transit, or at rest. DLP uses machine learning to detect and protect sensitive information according to organizational or regulatory guidelines. With context-aware policies, the system considers various factors such as users, devices, apps, networks, and actions to protect data in real time by obfuscating personal data, encrypting files, or blocking actions. It can also request a stepped-up authentication or business justification for risky actions or refer users for further training.	• CASB • NG-SWG • DLP

AWARENESS AND TRAINING

Control	Requirements(s)	Netskope Response	Products
AT-1	a. Develop, document, and disseminate to organization-defined personnel or roles: 1. An organization-level; mission/business process-level; system-level awareness and training policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and	Netskope enforces organizational policies and assists in policy communication through pop-up banners and coaching pages that alert employees to potential infringements. Netskope's CASB identifies and inventories apps and cloud services, assessing their risk levels for asset management, acquisition strategy, and business continuity planning. Netskope's NG-SWG integrates with third-party identity providers for SSO/MFA and logs activities to detect anomalies, applying context-aware policy controls. These controls can trigger multi-factor authentication, notify about policy violations, suggest safer alternatives, or direct users to cybersecurity training. NG-SWG also supports incident response through customizable reports and alerts. Advanced User and Entity Behavior Analytics includes more ML-based models and a User Confidence Index to detect insider threats and adapt users' access privileges based on risk. Advanced Analytics maps data flows, assesses cloud risk, and provides a dashboard to track security trends.	• CASB • NG-SWG • Public Cloud Security • Advanced Analytics • Advanced UEBA • CTO

Control	Requirements(s)	Netskope Response	Products
	c. Review and update the current awareness and training: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes.		
AT-2	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors): 1. As part of initial training for new users and [FedRAMP Assignment: at least annually] thereafter; and 2. When required by system changes or following [Assignment: organization-defined events]; b. Employ organization-defined awareness techniques to increase the security and privacy awareness of system users; c. Update literacy training and awareness content at least annually and following organization-defined events; and d. Incorporate lessons learned from internal or external security or privacy incidents into literacy training and awareness techniques.	Netskope's NG-SWG and CASB's context-aware controls address risky behavior by requiring extra authentication, notifying users of potential violations, suggesting safer alternatives, or directing users to cybersecurity training. Customizable reports and alerts can be integrated with an organization's SIEM tools to aid incident response, while detailed event logging supports non-repudiation of user actions. The Advanced User and Entity Behavior Analytics (UEBA) includes numerous ML-based anomaly-detection models and a User Confidence Index (UCI), which is a dynamic risk score for each user based on their behavior. UCI helps adapt policies, control measures, and recommend security training to mitigate insider threats. It can also integrate with Netskope's Cloud Exchange to share insider threat information via the Cloud Risk Exchange.	• CASB • NG-SWG • Advanced UEBA • Cloud Exchange
	AT-2(2): Provide literacy training on recognizing and reporting potential indicators of insider threat.	Netskope's product suite enhances cybersecurity and data privacy awareness by using pop-up banners and coaching pages. These tools notify employees of potential policy infringements, request justifications for risky actions, and refer users to third-party training tools like KnowBe4. Netskope also enforces organizational policies and tracks policy acknowledgements, helping ensure compliance through timely notifications and training facilitation.	• All products
	AT-2(3): Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.	Netskope's product suite enhances cybersecurity and data privacy awareness by using pop-up banners and coaching pages. These tools notify employees of potential policy infringements, request justifications for risky actions, and refer users to third-party training as needed. Netskope also enforces organizational policies and tracks policy acknowledgements, helping ensure compliance through timely notifications and training facilitation.	• All products

Control	Requirements(s)	Netskope Response	Products
AT-3	a. Provide role-based security and privacy training to personnel with organization-defined roles and responsibilities: 1. Before authorizing access to the system, information, or performing assigned duties, and at least annually thereafter; and 2. When required by system changes; b. Update role-based training content at least annually and following organization-defined events; and c. Incorporate lessons learned from internal or external security or privacy incidents into role-based training.	Netskope's Cloud Access Security Broker (CASB) and Next Gen Secure Web Gateway (NG-SWG) provide comprehensive monitoring, logging, and control for SaaS and IaaS activities. Policy controls are applied based on activity, data nature, or app instance, and can prompt additional MFA, notify users of violations, suggest safer alternatives, or refer them for cybersecurity training. NG-SWG generates customizable reports and alerts for incident response and supports non-repudiation through detailed event logging.	• CASB • NG-SWG
AT-4	a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and b. Retain individual training records for five (5) years or 5 years after completion of a specific training program.	Netskope's product suite enhances cybersecurity and data privacy by using pop-up banners and coaching pages to communicate policies and provide awareness training. These tools notify employees of possible policy violations, request justifications for risky actions, and direct users to third-party vendors for additional training as per organizational needs.	• All products

AUDIT AND ACCOUNTABILITY

Control	Requirements(s)	Netskope Response	Products
AU-1	a. Develop, document, and disseminate to organization-defined personnel or roles: 1. Organization-level; mission/ business process-level; system-level audit and accountability policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and c. Review and update the current audit and accountability: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes.	Netskope's CASB assists with asset inventory, acquisition strategy, third-party risk management, and business continuity by identifying managed and unmanaged apps and assessing their criticality. Meanwhile, Advanced Analytics maps data flows, characterizes cloud app usage, and tracks security trends. Netskope's Cloud Log Shipper can send event and alert logs to the organization's SIEM tool, and the Cloud Ticket Orchestrator can generate service tickets and automate incident response workflows.	• CASB • NG-SWG • Public Cloud Security • Advanced Analytics • CLS • CTO
AU-2	a. Identify the types of events that the system is capable of logging in support of the audit function: successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;	Netskope NG-SWG, CASB, and Private Access provide detailed logging of all web, cloud, and on-premises access activity by users, with the ability to detect more than 100 inline actions within cloud services and SaaS applications, such as login, logout, view, browse, post, upload, delete, or download. Netskope's Cloud Firewall enforces security policies for egress traffic to the web or cloud apps across all ports and protocols, mitigating threats like DDoS and DNS attacks by inspecting malicious domains. It generates logs for SIEM tools to aid incident response. Activity logs and alerts can be exported to other platforms (such as SIEM and SOAR platforms) with the Cloud Log Shipper tool, or used to automatically create service tickets with Netskope's Cloud Ticket Orchestrator (CTO) tool. Proxy transaction events can be streamed to cloud storage or SIEMs in near real-time automatically create service tickets with Netskope's Cloud Ticket Orchestrator (CTO) tool. Proxy transaction events can be streamed to cloud storage or SIEMs in near real time.	• CASB • NG-SWG • Private Access • Public Cloud Security • Cloud Firewall • CTO • CLS

Control	Requirements(s)	Netskope Response	Products
	c. Specify the organization-defined subset of the auditable events defined in AU-2a to be audited continually for each identified event; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging annually and whenever there is a change in the threat environment. **AU-2 Additional FedRAMP Requirements and Guidance:** **(e) Guidance**: Annually or whenever changes in the threat environment are communicated to the service provider by the JAB/AO. **Requirement**: Coordination between service provider and consumer shall be documented and accepted by the JAB/AO.		
AU-3	Ensure that audit records contain information that establishes the following: a. What type of event occurred; b. When the event occurred; c. Where the event occurred; d. Source of the event; e. Outcome of the event; and f. Identity of any individuals, subjects, or objects/entities associated with the event.	Netskope's CASB, NG-SWG, and Private Access monitor and log activities in SaaS and IaaS services, providing details on user, device, instance, and actions performed. They can detect more than 100 inline actions within cloud services and SaaS applications, such as login, logout, view, browse, post, upload, delete, or download. Netskope's Private Access logs all access attempts and applies organizational policies for failed login attempts. Activity logs and alerts can be exported to other platforms (such as SIEM and SOAR platforms) with the Cloud Log Shipper tool, or used to automatically create service tickets with Netskope's Cloud Ticket Orchestrator (CTO) tool. Proxy transaction events can be streamed to cloud storage or SIEMs in near real time.	• CASB • Private Access • NG-SWG • DLP • CLS • CTO
	AU-3(1)1: Generate audit records containing the following additional information: session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon; individual identities of group account users; full-text of privileged commands.		

Control	Requirements(s)	Netskope Response	Products
	AU-3 (1) Additional FedRAMP Requirements and Guidance: **Guidance**: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.		
AU-4	Allocate audit log storage capacity to accommodate organization-defined audit log retention requirements.	Netskope's products do not map to this requirement.	
AU-5	a. Alert organization-defined personnel or roles within organization-defined time period in the event of an audit logging process failure; and b. Overwrite the oldest record..	Netskope's products do not map to this requirement.	
	AU-5(1): Provide a warning to organization-defined personnel, roles, and/or locations within organization-defined time period when allocated audit log storage volume reaches 75%, or one month before expected negative impact of repository maximum audit log storage capacity.		
	AU-5(2): Provide an alert within real-time to service provider personnel with authority to address failed audit events when the following audit failure events occur: organization-defined audit logging failure events requiring real time alerts.		
AU-6	a. Review and analyze system audit records at least weekly for indications of organization-defined inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity; b. Report findings to organization-defined personnel or roles; and c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information. **AU-6 Additional FedRAMP Requirements and Guidance:**	Netskope's Advanced Analytics maps an organization's data flows across web and cloud services, characterizing data by category and sensitivity. Advanced Analytics also assesses cloud risk by cataloguing and characterizing cloud app usage, and the product dashboard allows administrators to track security trends by number of apps accessed, threats detected, policies triggered, and users impacted. Netskope's Cloud Firewall enforces organizational security policies on egress traffic across all ports and protocols without routing through on-premises security. It protects against DDoS, man-in-the-middle, and DNS attacks by inspecting queries for malicious domains. Logs from the Cloud Firewall can be integrated with SIEM tools for improved incident response and recovery. Netskope's Cloud Ticket Orchestrator automates incident response workflows and enforces role-based access controls, significantly streamlining the organization's security operations. It is a key component of Netskope's Cloud Exchange, included in every Netskope deployment.	• Public Cloud Security • Cloud Firewall • CTO • Advanced Analytics

Control	Requirements(s)	Netskope Response	Products
	Requirement: Coordination between service provider and consumer shall be documented and accepted by the JAB/AO. In multi-tenant environments, capability and means for providing review, analysis, and reporting to consumer for data pertaining to consumer shall be documented.		
	AU-6(1): Integrate audit record review, analysis, and reporting processes using organization-defined automated mechanisms.	Netskope's CASB and NG-SWG can be configured to generate reports and alerts based on customizable thresholds, which can be fed into the organization's SIEM tool to facilitate incident response, and its detailed event logging can assist organizations in asserting non-repudiation of user actions. Netskope's Cloud Log Shipper exports event and alert logs from various Netskope security tools to a customer's security information and event management (SIEM) or incident response systems.	• CASB • NG-SWG • CLS
	AU-6(3): Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.	Netskope's Cloud Log Shipper exports event and alert logs from Netskope's CASB, NG-SWG, Private Access, and Public Cloud Security to a customer's security information and event management (SIEM) or incident response systems. The Cloud Risk Exchange integrates with third-party vendors like Crowdstrike and ServiceNow to ingest and normalize risk scores for users, devices, and applications. It then applies adaptive controls to mitigate risks associated with the highest risk entities. Cloud Threat Exchange enables near real-time sharing of threat indicators, such as malicious URLs and file hashes, with Netskope customers and partners, and can automatically integrate with an organization's SIEM.	• CASB • NG-SWG • Private Access • Public Cloud Security • CLS • CRE • CTE
	AU-6(4): Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.	Netskope products provide detailed reports and interactive dashboards that inventory, categorize, assign risk scores to, and show the usage of more than 85,000 cloud applications in use within the enterprise including SaaS and Public Cloud services. With Netskope, IT and Security teams are able to map communication and data flows to an exceptional degree of accuracy. Netskope will not only map where data is flowing, including for company and personal app instances, but also provide the necessary controls to contain data flows when unmanaged devices are being used and unmanaged services are being adopted by end-users.	• NG-SWG • CASB • Public Cloud Security • CCI • Advanced Analytics • Device Intelligence
	AU-6(5): Integrate analysis of audit records with analysis of vulnerability scanning information; performance data; information system monitoring information; penetration test data; organization-defined data/ information collected from other sources to further enhance the ability to identify inappropriate or unusual activity.	The Netskope platform provides a significant amount of visibility to administrators while supporting privacy by design. Netskope products can be configured to secure activity to web, SaaS, IaaS, and egress traffic from on-network and remote users, but also secures app and cloud service activity to the extent that specific user actions (such as share, edit, delete, upload, download, etc.) within cloud apps are recorded. Netskope has the unique ability to decode inline unpublished API calls and JSON streams to secure user activity in real time across apps and cloud services, including by instance (i.e., company vs. personal).	• All products

Control	Requirements(s)	Netskope Response	Products
		Threat protection and data protection (DLP) components are also used to identify activities that may be malicious such as intentionally downloading malicious code or attempting to exfiltrate data. In addition, configuration of public cloud and SaaS services can also be monitored to assist in identifying accidental or intentional misconfigurations. Cloud Exchange can be leveraged to extend and share activity data across an ecosystem of network and security tools.	
	AU-6(6): Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity. **AU-6 (6) Additional FedRAMP Requirements and Guidance:** **Requirement**: Coordination between service provider and consumer shall be documented and accepted by the JAB/AO.	Netskope does not map to this requirement.	
	AU-6(7): Specify the permitted actions for each information system process; role; user associated with the review, analysis, and reporting of audit record information	Both CASB and NG-SWG, along with ZTNA Next, enforce role-based access control to uphold organizational access management policies following the principle of least privilege. Netskope's DLP supports role-based access during incident response and recovery, ensures backup integrity, and maintains logs for continuous monitoring and forensic investigations.	• CASB • NG-SWG • DLP • Private Access
AU-7	Provide and implement an audit record reduction and report generation capability that: a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and b. Does not alter the original content or time ordering of audit records.	Netskope's NG-SWG decodes and logs over 100 activities inline, establishing user activity baselines to detect anomalies and implement granular policy controls. It generates custom reports and alerts for SIEM integration to enhance incident response and non-repudiation. Netskope's User and Entity Behavior Analytics (UEBA) tracks user behavior across various apps, establishes baselines, and detects anomalies to adjust access and privileges. Device Intelligence classifies all devices on the network, creating baselines at the device level to detect and control risky behavior, adhering to zero trust principles. It integrates with incident response tools for generating security alerts. Cloud Log Shipper exports logs from multiple Netskope tools to the organization's SIEM for streamlined incident management. Cloud Ticket Orchestrator automates incident response workflows, creating service tickets in response to security alerts.	• CASB • NG-SWG • UEBA • Device Intelligence • CLS • CTO

Control	Requirements(s)	Netskope Response	Products
	AU-7(1): Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: organization-defined fields within audit records.	Netskope's NG-SWG generates customizable alerts and reports for SIEM integration to facilitate incident responses. Netskope's Advanced Analytics maps an organization's data flows across web and cloud services, characterizing data by category and sensitivity. Advanced Analytics also assesses cloud risk by cataloguing and characterizing cloud app usage, and the product dashboard allows administrators to track security trends by number of apps accessed, threats detected, policies triggered, and users impacted. Netskope's User and Entity Behavior Analytics (UEBA) tracks user behavior across web and cloud apps, detecting anomalies against a baseline of normal behavior and adjusting access controls accordingly. Device Intelligence identifies and classifies devices on the network, using AI/ML to establish normal behavior baselines and detect anomalies, ensuring zero trust principles are applied. The Cloud Log Shipper exports logs from various Netskope tools to an organization's SIEM, aiding incident response. Cloud Ticket Orchestrator automates service tickets and workflows in response to security alerts, enforcing role-based access controls during incident response.	• CASB • NG-SWG • Advanced Analytics • UEBA • Device Intelligence • CLS • CTO
AU-8	a. Use internal system clocks to generate time stamps for audit records; and b. Record time stamps for audit records that meet one-second granularity of time measurement and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.	Netskope's products do not map to this requirement.	
AU-9	a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and b. Alert organization-defined personnel or roles upon detection of unauthorized access, modification, or deletion of audit information.	Netskope's CASB and NG-SWG utilize a data loss prevention (DLP) engine to secure organizational data across the web, cloud applications, and endpoint devices. DLP leverages machine learning to identify and protect sensitive data, complying with organizational and regulatory requirements. Context-aware policies protect data in real time by employing techniques such as data obfuscation, encryption, or action blocking. DLP also supports role-based access during incident response, ensures backup integrity, and facilitates continuous monitoring and forensic investigations through dedicated log repositories.	• CASB • NG-SWG • Public Cloud Security • DLP • CTO
	AU-9(2): Store audit records at least weekly in a repository that is part of a physically different system or system component than the system or component being audited.	Netskope's DLP engine can store event and alert logs in dedicated repositories for later review.	• NG-SWG • DLP • CASB

Control	Requirements(s)	Netskope Response	Products
	AU-9(3): Implement cryptographic mechanisms to protect the integrity of audit information and audit tools. **AU-9 (3) Additional FedRAMP Requirements and Guidance:** **Guidance:** Note that this enhancement requires the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13.).	The Netskope platform can store forensic data in forensic tools or repositories defined by customers to support enterprise risk management processes.	• All products
	AU-9(4): Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles]..	Netskope's CASB and NG-SWG enforce role-based access control across web and cloud-based apps and services. They incorporate a data loss prevention Engine that uses machine learning to identify, categorize, and protect sensitive data..	• CASB • NG-SWG • DLP
AU-10	Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed minimum actions including the addition, modification, deletion, approval, sending, or receiving of data.	Netskope NG-SWG, CASB, and Private Access provides detailed logging of all web, cloud, and on-premises access activity by users, including inline app and cloud service API-level. This detailed activity level of logging and proxy transaction events will assist organizations in asserting non-repudiation for actions in their web, cloud, and on-premises applications.	• NG-SWG • CASB • Private Access • Public Cloud Security
AU-11	Retain audit records for a time period in compliance with M-21-31 to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements. **AU-11 Additional FedRAMP Requirements and Guidance:** **Guidance**: The service provider is encouraged to align with M-21-31 where possible. **Requirement**: The service provider retains audit records online for at least ninety (90) days and further preserves audit records off-line for a period that is in accordance with NARA requirements. **Requirement**: The service provider must support Agency requirements to comply with M-21-31.	Netskope's products do not map to this requirement.	

Control	Requirements(s)	Netskope Response	Products
AU-12	a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on all information system and network components where audit capability is deployed/ available; b. Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.	Netskope's NG-SWG and CASB can generate customizable reports and alerts to aid incident response, with detailed logs to assert non-repudiation of user actions. They also integrate a robust data loss prevention (DLP) engine to secure organizational data across the web, cloud applications, and endpoint devices. DLP also maintains log files in dedicated repositories for continuous monitoring and forensic investigations. Netskope's User and Entity Behavior Analytics tracks user behavior across various apps, establishing normal baselines and detecting anomalies to adjust access based on risk. Device Intelligence classifies network devices, isolates risky ones, and uses AI/ML to detect and control anomalous device behavior, integrating with incident response tools. Cloud Log Shipper ingests event logs and alerts from CASB, NG-SWG, Private Access, and Cloud Firewall, and exports them to the organization's SIEM or other incident response tool. Advanced Analytics maps data flows across the organization's network, and allows administrators to visualize security trends by tracking vulnerabilities detected, policies triggered, and users affected.	• CASB • NG-SWG • UEBA • Device Intelligence • CLS • CTO • DLP • Advanced Analytics • Private Access
	AU-12(1): Compile audit records from all network, data storage, and computing devices into a system-wide (logical or physical) audit trail that is time-correlated to within organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail		
	AU-12(3): Provide and implement the capability for service provider-defined individuals or roles with audit configuration responsibilities to change the logging to be performed on all network, data storage, and computing devices based on organization-defined selectable event criteria within organization-defined time thresholds.		

ASSESSMENT, AUTHORIZATION, AND MONITORING

Control	Requirements(s)	Netskope Response	Products
CA-1	a. Develop, document, and disseminate to organization-defined personnel or roles: 1. Organization-level; mission/ business process-level; system-level assessment, authorization, and monitoring policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and c. Review and update the current assessment, authorization, and monitoring: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes.	Netskope enforces organizational policies and assists with policy communication using pop-up banners and coaching pages to notify employees of potential infringements. The Cloud Access Security Broker (CASB) aids in asset inventory, acquisition strategy, risk management, and business continuity by inventorying apps and cloud services, assessing their criticality, and ensuring compliance. Advanced Analytics maps data flows, assesses cloud risk, and characterizes data by sensitivity, enabling administrators to track security trends via a dashboard.	• CASB • NG-SWG • Advanced Analytics

Control	Requirements(s)	Netskope Response	Products
CA-2	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment; d. Assess the controls in the system and its environment of operation at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy e. Produce a control assessment report that documents the results of the assessment; and f. Provide the results of the control assessment to individuals or roles to include FedRAMP PMO. **CA-2 Additional FedRAMP Requirements and Guidance:** **Guidance**: Reference FedRAMP Annual Assessment Guidance.	The Netskope platform helps define the scope of organizational security tests and exercises by inventorying unmanaged apps and devices and assigning them risk-based scores. It assesses SaaS application risks via the Cloud Confidence Index (CCI), considering security policies, certifications, and other criteria. Netskope's CASB aids in asset inventory, acquisition strategy, third-party risk management, and business continuity by identifying critical managed and unmanaged apps and services. It also generates alerts for automated incident response and logs for reports. Netskope's Advanced Analytics maps data flows, categorizes data, and assesses cloud app risks, allowing administrators to track security trends through a detailed dashboard.	• CASB • NG-SWG • Cloud Confidence Index (CCI) • Advanced Analytics
	CA-2(1): Employ independent assessors or assessment teams to conduct control assessments. **CA-2 (1) Additional FedRAMP Requirements and Guidance:** **Requirement**: For JAB Authorization, must use an accredited 3PAO.	Netskope's products do not map to this requirement.	

Control	Requirements(s)	Netskope Response	Products
	CA-2(2): Include as part of control assessments at least annually, announced; unannounced: in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; data leakage or data loss assessment; other forms of assessment. **CA-2 (2) Additional FedRAMP Requirements and Guidance:** **Requirement**: To include 'announced', 'vulnerability scanning'..	The Netskope platform can help organizations prepare for and get the most out of security tests and exercises. For example, Netskope can help organizations define the scope of tests and exercises by inventorying all unmanaged apps and devices in an ICT environment, and assigning risk-based scores. Netskope's Cloud Exchange can assist before and during security tests or exercises. The Cloud Threat Exchange and Cloud Risk Exchange can help identify risky users and assets, and provide up-to-the-minute intel on various threats and vulnerabilities. Meanwhile, Netskope's Cloud Log Shipper (CLS) and Cloud Ticket Orchestrator (CTO) enable a comprehensive, bird's-eye view of any attack–real or simulated–and help streamline an organization's response.	• NG-SWG • CASB • Private Access • Public Cloud Security • Cloud Exchange • Cloud Firewall • DLP • RBI
	CA-2(3): Leverage the results of control assessments performed by any FedRAMP Accredited 3PAO on organization-defined system when the assessment meets organization-defined requirements.		
CA-3	a. Approve and manage the exchange of information between the system and other systems using: interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements, organization-defined type of agreement; b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and c. Review and update the agreements at least annually and on input from JAB/AO.	Netskope's CASB aids in asset inventory, acquisition strategy, third-party risk management, and business continuity planning by identifying and assessing managed and unmanaged apps and cloud services in an organization's IT ecosystem. It evaluates their criticality based on usage and risk level.	• CASB • Public Cloud Security • CTO
	CA-3(6): Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.	Netskope's products do not map to this requirement.	

Control	Requirements(s)	Netskope Response	Products
CA-5	a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and b. Update existing plan of action and milestones at least monthly based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.	Netskope's CASB and NG-SWG aid in asset inventory, acquisition strategy, third-party risk management, and business continuity planning by identifying and inventorying both managed and unmanaged apps and cloud services within an organization's IT ecosystem.	• CASB • NG-SWG
	CA-5 Additional FedRAMP Requirements and Guidance: **Guidance**: Reference FedRAMP-POAM-Template **Requirement**: POA&Ms must be provided at least monthly.		
CA-6	a. Assign a senior official as the authorizing official for the system; b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems; c. Ensure that the authorizing official for the system, before commencing operations: 1. Accepts the use of common controls inherited by the system; and 2. Authorizes the system to operate; d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems; and e. Update the authorizations in accordance with OMB A-130 requirements or when a significant change occurs. **CA-6 Additional FedRAMP Requirements and Guidance:**	Netskope's products do not map to this requirement.	

Control	Requirements(s)	Netskope Response	Products
	(e) **Guidance**: Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F and according to FedRAMP Significant Change Policies and Procedures. The service provider describes the types of changes to the information system or the environment of operations that would impact the risk posture. The types of changes are approved and accepted by the JAB/AO.		
CA-7	Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes: a. Establishing the following system-level metrics to be monitored: organization-defined system-level metrics; b. Establishing organization-defined freqfuencies for monitoring and organization-defined frequencies for assessment of control effectiveness; c. Ongoing control assessments in accordance with the continuous monitoring strategy; d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy; e. Correlation and analysis of information generated by control assessments and monitoring; f. Response actions to address results of the analysis of control assessment and monitoring information; and g. Reporting the security and privacy status of the system to include JAB/AO, organization-defined frequencies. **CA-7 Additional FedRAMP Requirements and Guidance:**	Netskope enforces organizational policies and notifies employees of potential infringements through pop-up banners and coaching pages. Netskope's CASB and NG-SWG are equipped with a data loss prevention (DLP) engine, which uses machine learning to protect sensitive data in real time, including blocking or requesting business justifications for risky actions, or referring users for further cybersecurity training. Netskope also scores SaaS applications on its Cloud Confidence Index (CCI) and helps organizations assess the risk of using various vendors' applications. Netskope's Public Cloud Security can scan IaaS Storage for malware. Remote Browser Isolation secures against risky websites, and Private Access provides secure remote access to private apps. Standard Threat Protection guards against known and new malware, integrating with Netskope's security tools. Advanced Threat Protection uses deobfuscation and sandboxing to detect new malware. Device Intelligence identifies and categorizes devices, detecting anomalies and applying zero trust principles. And Advanced Analytics maps data flows and assesses cloud risks, with a dashboard that gives administrators insights into vulnerabilities discovered, policies triggered, and users impacted. Netskope's Cloud Log Shipper can send event and alert logs to the organization's SIEM tool, and the Cloud Ticket Orchestrator can generate service tickets and automate incident response workflows.	• CASB • NG-SWG • Public Cloud Security • Cloud Confidence Index (CCI) • DLP • RBI • Private Access • Advanced Analytics • Advanced DLP • Advanced Threat Protection • Device Intelligence • Threat Protection • CTO

Control	Requirements(s)	Netskope Response	Products
	Guidance: FedRAMP does not provide a template for the Continuous Monitoring Plan. CSPs should reference the FedRAMP Continuous Monitoring Strategy Guide when developing the Continuous Monitoring Plan. **Requirement**: Operating System, Database, Web Application, Container, and Service Configuration Scans, at least monthly. All scans performed by Independent Assessor, at least annually. **Requirement**: CSOs with more than one agency ATO must implement a collaborative Continuous Monitoring (ConMon) approach described in the FedRAMP Guide for Multi-Agency Continuous Monitoring. This requirement applies to CSOs authorized via the Agency path as each agency customer is responsible for performing ConMon oversight. It does not apply to CSOs authorized via the JAB path because the JAB performs ConMon oversight.		
	CA-7(1): Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.	Netskope's products do not map to this requirement.	
	CA-7(4): Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following: (a) Effectiveness monitoring; (b) Compliance monitoring; and (c) Change monitoring	Netskope's Advanced Analytics monitors and maps an organization's data flows across web and cloud services, categorizing data by sensitivity. It evaluates cloud risk by cataloguing cloud app usage. The product dashboard enables administrators to track security trends, including apps accessed, threats detected, policies triggered, and users impacted.	• CASB • NG-SWG • Advanced Analytics
CA-8	Conduct penetration testing at least annually on organization-defined systems or system components. **CA-8 Additional FedRAMP Requirements and Guidance:** **Guidance**: Reference the FedRAMP Penetration Test Guidance..	The Netskope platform aids organizations in optimizing security tests and exercises by defining their scope effectively. It inventories all managed and unmanaged apps and devices within the ICT environment and assigns them risk-based scores, thereby enhancing preparation and outcomes.	• All products
	CA-8(1): Employ an independent penetration testing agent or team to perform penetration testing on the system or system components	Netskope does not map to this requirement.	

Control	Requirements(s)	Netskope Response	Products
	CA-8(2): Employ organization-defined red team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement. **CA-8(2) Additional FedRAMP Requirements and Guidance:** **Guidance**: See the FedRAMP Documents page > Penetration Test Guidance. https://www.FedRAMP.gov/documents/	The Netskope platform can help organizations prepare for and get the most out of security tests and exercises. For example, Netskope can help organizations define the scope of tests and exercises by inventorying all unmanaged apps and devices in an ICT environment, and assigning risk-based scores. Netskope's Cloud Exchange can assist before and during security tests or exercises. The Cloud Threat Exchange and Cloud Risk Exchange can help identify risky users and assets and provide up-to-the-minute intel on various threats and vulnerabilities. Meanwhile, Netskope's Cloud Log Shipper (CLS) and Cloud Ticket Orchestrator (CTO) enable a comprehensive, bird's-eye view of any attack–real or simulated–and help streamline an organization's response.	• NG-SWG • CASB • Public Cloud Security • DLP • Cloud Exchange • RBI • Cloud Firewall • Private Access
CA-9	a. Authorize internal connections of organization-defined system components or classes of components to the system; b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated; c. Terminate internal system connections after organization-defined conditions; and d. Review at least annually the continued need for each internal connection	Netskope offers inline controls that manage employee access to web, cloud, or private application information, with capabilities to block, notify, or allow access. It can identify various instances of cloud applications (development, testing, production) and enforce data protection rules accordingly. Netskope's Cloud Access Security Broker (CASB) supports asset inventory, acquisition strategy, third-party risk management, and business continuity planning by identifying and evaluating managed and unmanaged apps and cloud services based on their usage and risk level. Netskope Device Intelligence identifies, catalogs, and classifies all devices, both managed and unmanaged, that connect to an organization's network. It groups these devices into network segments to isolate any that are considered risky. Utilizing AI and machine learning, it establishes a baseline for normal device behavior and detects anomalies. Device Intelligence applies granular access and activity controls based on zero trust principles and can integrate with an organization's incident response tools to generate tailored security alerts.	• CASB • Public Cloud Security • CTO • Device Intelligence

CONFIGURATION MANAGEMENT

Control	Requirements(s)	Netskope Response	Products
CM-1	a. Develop, document, and disseminate to organization-defined personnel or roles: 1. Organization-level; mission/ business process-level; system-level configuration management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the configuration management policy and procedures; and c. Review and update the current configuration management: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes.	Netskope enforces organizational policies and assists communication by using pop-up banners and coaching pages to notify employees of potential policy violations. Its Cloud Access Security Broker (CASB) helps with asset inventory, acquisition strategy, third-party risk management, and business continuity by identifying and assessing managed and unmanaged apps and cloud services based on usage and risk. Netskope's Advanced Analytics maps data flows across web and cloud services, assessing cloud app usage and risk while providing dashboards for tracking security trends, including apps accessed, threats detected, policies triggered, and impacted users. Netskope's Cloud Log Shipper can send event and alert logs to the organization's SIEM tool, and the Cloud Ticket Orchestrator can generate service tickets and automate incident response workflows.	• CASB • NG-SWG • Public Cloud Security • Advanced Analytics • CLS • CTO
CM-2	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and b. Review and update the baseline configuration of the system: 1. At least annually and when a significant change occurs; 2. When directed by the JAB; and 3. When system components are installed or upgraded. **CM-2 Additional FedRAMP Requirements and Guidance.**	The Netskope platform can be integrated with change management solutions. Specific controls and baseline assessments can be completed for cloud infrastructure and cloud services tied to change management and business processes including the ability to add exceptions.	• All products

Control	Requirements(s)	Netskope Response	Products
	(b)(1) Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F. CM-2(2): Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms]. CM-2(3): Retain organization-defined number of previous versions of baseline configurations of the previously approved baseline configuration of IS components of previous versions of baseline configurations of the system to support rollback. CM-2(7): (a) Issue organization-defined systems or system components with organization-defined configurations to individuals traveling to locations that the organization deems to be of significant risk; and (b) Apply organization-defined controls to the systems or components when the individuals return from travel.		
CM-3	Develop and document an inventory of a. Determine and document the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c. Document configuration change decisions associated with the system; d. Implement approved configuration-controlled changes to the system; e. Retain records of configuration-controlled changes to the system for organization-defined time period; f. Monitor and review activities associated with configuration-controlled changes to the system; and	Netskope evaluates SaaS applications through its Cloud Confidence Index (CCI), assessing risks using criteria like security policies, certifications, audit capabilities, and legal/privacy concerns.	• NG-SWG • CASB • Public Cloud Security • CTO

Control	Requirements(s)	Netskope Response	Products
	g. Coordinate and provide oversight for configuration change control activities through organization-defined configuration change control elements that convene at an organization-defined frequency; upon organization-defined configuration change conditions.		
	CM-3 Additional FedRAMP Requirements and Guidance: (e) **Guidance**: In accordance with record retention policies and procedures. **Requirement**: The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the JAB/AO		
	CM-3(1): Use organization-defined automated mechanisms to: (a) Document proposed changes to the system; (b) Notify organization-defined approval authorities of proposed changes to the system and request change approval; (c) Highlight proposed changes to the system that have not been approved or disapproved within organization agreed-upon time period; (d) Prohibit changes to the system until designated approvals are received; (e) Document all changes to the system; and (f) Notify organization-defined configuration management approval authorities when approved changes to the system are completed.	The Netskope platform can be integrated with change management solutions. Specific controls and baseline assessments can be completed for cloud infrastructure and cloud services tied to change management and business processes including the ability to add exceptions.	• All products

Control	Requirements(s)	Netskope Response	Products
	CM-3(2): Test, validate, and document changes to the system before finalizing the implementation of the changes.	Netskope Device Intelligence identifies and classifies all devices connecting to an organization's network, segmenting them to isolate risky ones. Its AI/ML engine establishes normal behavior baselines, detects anomalies, and enforces access controls based on zero trust principles. It integrates with incident response tools to trigger alerts as per organizational criteria. Netskope's Advanced Analytics monitors data flows across web and cloud services, categorizing data by sensitivity and assessing cloud app usage risk. Its dashboard tracks security trends, including apps accessed, threats detected, policies triggered, and users affected.	• CASB • NG-SWG • Advanced Analytics • Device Intelligence
	CM-3(4): Require organization-defined security and privacy representatives to be members of the Configuration Control Board (CCB) or similar (as defined in CM-3).	Netskope's products do not map to this requirement.	
	CM-3(6): Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: All security safeguards that rely on cryptography.	Netskope's products do not map to this requirement.	
CM-4	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.	Netskope evaluates SaaS applications through its Cloud Confidence Index (CCI), offering crucial insights for organizations to assess the risk associated with each vendor's application or cloud service. The evaluation criteria encompass the vendor's security policies, certifications, audit capabilities, legal issues, privacy concerns, and additional factors. Netskope's Private Access and Cloud Firewall capabilities support network segmentation to separate development, testing, and operational environments.	• CASB • NG-SWG • Cloud Confidence Index (CCI) • Private Access • Cloud Firewall
	CM-4(1): Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.		
	CM-4(2): After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.		
CM-5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	Netskope's Cloud Access Security Broker (CASB) monitors activities in cloud apps and services, providing information on users, devices, actions, and applying real-time controls to prevent data loss. Netskope's NG-SWG integrates with third-party identity providers to extend Single Sign-On and Multi-Factor Authentication across apps. It logs activities, establishes baselines for detecting anomalies, and applies context-aware controls. Both CASB and NG-SWG can demand additional authentication or a business justification for risky behaviors, suggest safer alternatives, or direct the user to further cybersecurity training. They also both generate reports and alerts, assisting incident responses and supporting non-repudiation of user actions.	• CASB • NG-SWG • Public Cloud Security

Control	Requirements(s)	Netskope Response	Products
	CM-5(1): (a) Enforce access restrictions using organization-defined automated mechanisms; and (b) Automatically generate audit records of the enforcement actions.	With the Netskope platform, policy violations and other alerts are logged and workflows are implemented into the console to ensure records can be reviewed efficiently. Activity logs and alerts can be exported to other platforms (such as SIEM and SOAR platforms) with the Cloud Log Shipper tool, or used to automatically create service tickets with Netskope's Cloud Ticket Orchestrator (CTO) tool. Proxy transaction events can be streamed to cloud storage or SIEMs in near real time.	• All products
	CM-5(5): (a) Limit privileges to change system components and system-related information within a production or operational environment; and (b) Review and reevaluate privileges at least quarterly.	Netskope's suite of security products, including CASB, NG-SWG, and Private Access, supports organizational access management with role-based access control (RBAC) based on the principle of least privilege. CASB and NG-SWG utilize RBAC to ensure users have only the access necessary for their roles. Private Access provides secure remote access to private applications from any device, integrating with third-party identity providers for secure authentication. The solution employs end-to-end encryption and granular control measures to limit access based on zero trust principles. Private Access also logs all access attempts and enforces policies on failed login attempts, further enhancing security by strictly adhering to the principle of least privilege.	• CASB • NG-SWG • Private Access
CM-6	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using organization-defined common secure configurations; b. Implement the configuration settings; c. Identify, document, and approve any deviations from established configuration settings for organization-defined system components based on organization-defined operational requirements; and d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.	Netskope Device Intelligence identifies, catalogs, and classifies all managed and unmanaged devices connecting to the organization's network, and groups devices into network segments to isolate risky devices. The Netskope platform generates transaction log data across web, cloud, on-premises, and device summarizing activity and reporting on this activity continuously. Furthermore, policy violations and other alerts are logged and workflows are implemented into the console to ensure records can be reviewed efficiently. Activity logs and alerts can be exported to other platforms (such as SIEM and SOAR platforms) with the Cloud Log Shipper tool, or used to automatically create service tickets with Netskope's Cloud Ticket Orchestrator (CTO) tool. Proxy transaction events can be streamed to cloud storage or SIEMs in near real time.	• All products

Control	Requirements(s)	Netskope Response	Products
	CM-6 Additional FedRAMP Requirements and Guidance: **Guidance:** Compliance checks are used to evaluate configuration settings and provide general insight into the overall effectiveness of configuration management activities. CSPs and 3PAOs typically combine compliance check findings into a single CM-6 finding, which is acceptable. However, for initial assessments, annual assessments, and significant change requests, FedRAMP requires a clear understanding, on a per-control basis, where risks exist. Therefore, 3PAOs must also analyze compliance check findings as part of the controls assessment. Where a direct mapping exists, the 3PAO must document additional findings per control in the corresponding SAR Risk Exposure Table (RET), which are then documented in the CSP's Plan of Action and Milestones (POA&M). This will likely result in the details of individual control findings overlapping with those in the combined CM-6 finding, which is acceptable. During monthly continuous monitoring, new findings from CSP compliance checks may be combined into a single CM-6 POA&M item. CSPs are not required to map the findings to specific controls because controls are only assessed during initial assessments, annual assessments, and significant change requests. **(a) Requirement 1**: The service provider shall use the DoD STIGs to establish configuration settings; Center for Internet Security up to Level 2 (CIS Level 2) guidelines shall be used if STIGs are not available; Custom baselines shall be used if CIS is not available. **(a) Requirement 2**: The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available).		

Control	Requirements(s)	Netskope Response	Products
	CM-6(1): Manage, apply, and verify configuration settings for organization-defined system components using organization-defined automated mechanisms.		
	CM-6(2): Take the following actions in response to unauthorized changes to organization-defined configuration settings: organization-defined actions.		
CM-7	a. Configure the system to provide only organization-defined mission-essential capabilities; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services. **CM-7 Additional FedRAMP Requirements and Guidance**: (b) **Requirement**: The service provider shall use Security guidelines (see CM-6) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if STIGs or CIS is not available.	Netskope's NG-SWG and CASB monitors and logs activities within SaaS and IaaS services, capturing detailed information related to users, devices, instances, and actions. It enforces real-time controls for activities and data loss prevention, enabling actions like blocking, requesting business justifications, and providing training on organizational policies. Netskope Device Intelligence identifies, catalogs, and classifies all managed and unmanaged devices connecting to the organization's network, and groups devices into network segments to isolate risky devices. Netskope's Device Intelligence's AI/ML engine creates a baseline of normal behavior at the device level, detects anomalous behavior, and can apply granular access and activity controls in accordance with zero trust principles. Device Intelligence can be integrated with the organization's incident response tools to generate security alerts based on criteria set by the organization.	• CASB • NG-SWG • Public Cloud Security • CTO • Device Intelligence
	CM-7(1): (a) Review the system at least annually to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and (b) Disable or remove organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure..		
	CM-7(2): Prevent program execution in accordance with: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.		

Control	Requirements(s)	Netskope Response	Products
	CM-7 (2) Additional FedRAMP Requirements and Guidance: **Guidance:** This control refers to software deployment by CSP personnel into the production environment. The control requires a policy that states conditions for deploying software. This control shall be implemented in a technical manner on the information system to only allow programs to run that adhere to the policy (i.e., allow-listing). This control is not to be based off of strictly written policy on what is allowed or not allowed to run.		
	CM-7(5): (a) Identify organization-defined software programs authorized to execute on the system; (b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and (c) Review and update the list of authorized software programs at least quarterly or when there is a change.		
CM-8	a. Develop and document an inventory of system components that: 1. Accurately reflects the system; 2. Includes all components within the system; 3. Does not include duplicate accounting of components or components assigned to any other system; 4. Is at the level of granularity deemed necessary for tracking and reporting; and 5. Includes the following information to achieve system component accountability: organization-defined information deemed necessary to achieve effective system component accountability; and b. Review and update the system component inventory at least monthly.	Netskope's CASB and NG-SWG help organizations with asset inventory, acquisition strategy, third-party risk management, and business continuity planning by identifying and assessing the criticality of managed and unmanaged apps and cloud services. Netskope Device Intelligence identifies, catalogs, and classifies all managed and unmanaged devices connecting to the organization's network, and groups devices into network segments to isolate risky devices. Netskope's Device Intelligence's AI/ML engine creates a baseline of normal behavior at the device level, detects anomalous behavior, and can apply granular access and activity controls in accordance with zero trust principles. Device Intelligence can be integrated with the organization's incident response tools to generate security alerts based on criteria set by the organization.	• CASB • NG-SWG • Device Intelligence

Control	Requirements(s)	Netskope Response	Products
	CM-8 Additional FedRAMP Requirements and Guidance: **Requirement**: Must be provided at least monthly or when there is a change..		
	CM-8(1): Update the inventory of system components as part of component installations, removals, and system updates.		
	CM-8(2): Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms].		
	CM-8(3): (a) Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms with a maximum five-minute delay in detection; and continuously (b) Take the following actions when unauthorized components are detected: disable network access by such components; isolate the components; notify organization-defined personnel or roles.	Netskope's NG-SWG integrates with NIST-compliant third-party identity providers, extending SSO/MFA across web and cloud apps, managing over 100 inline activities to develop a baseline for detecting anomalous behavior. It applies granular policy controls and context-aware responses like requiring multi-factor authentication for risky behavior. The system generates customizable reports and alerts, integrating with SIEM tools for incident response and enabling non-repudiation of user actions. Netskope's Standard Threat Protection safeguards against known and new malware, phishing, and web threats, using machine learning and corroborative sandboxing. It integrates with threat intelligence feeds and other Netskope tools like Remote Browser Isolation and Cloud Firewall to offer a comprehensive, layered security solution. Beyond Standard Threat Protection, Advanced Threat Protection includes deobfuscation, file unpacking, and multi-stage sandboxing to counter new malware. Netskope Device Intelligence identifies, catalogs, and classifies all devices on the network, using AI/ML to establish normal behavior, detect anomalies, and apply zero trust principles for access control, including segregating risky devices onto separate network segments. It also integrates with incident response tools for generating security alerts.	• NG-SWG • Advanced Threat Protection • Device Intelligence • Threat Protection
	CM-8(4): Include in the system component inventory information, a means for identifying by position and role, individuals responsible and accountable for administering those components.	Netskope's products do not map to this requirement.	

Control	Requirements(s)	Netskope Response	Products
CM-9	Develop, document, and implement a configuration management plan for the system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the system and places the configuration items under configuration management; d. Is reviewed and approved by organization-defined personnel or roles; and e. Protects the configuration management plan from unauthorized disclosure and modification. **CM-9 Additional FedRAMP Requirements and Guidance**: **Guidance**: FedRAMP does not provide a template for the Configuration Management Plan. However, NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, provides guidelines for the implementation of CM controls as well as a sample CMP outline in Appendix D of the Guide	Netskope's CASB monitors and logs activities in SaaS and IaaS services, applying real-time data loss prevention controls and requiring business justifications for risky actions or training on policy adherence. NG-SWG integrates with identity providers to extend SSO/MFA across apps, detects anomalous behavior, and applies granular policy controls, offering context-aware responses like requesting additional multi-factor authentication or referring the user for further training.	• CASB • NG-SWG • Public Cloud Security • CTO
CM-10	a. Use software and associated documentation in accordance with contract agreements and copyright laws; b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	Netskope's CASB and NG-SWG utilize a data loss prevention (DLP) engine to secure organizational data across the web, cloud applications, and endpoint devices. DLP leverages machine learning to identify and protect sensitive data, complying with organizational and regulatory requirements. Context-aware policies protect data in real time by employing techniques such as data obfuscation, encryption, or action blocking. DLP also supports role-based access during incident response, ensures backup integrity, and facilitates continuous monitoring and forensic investigations through dedicated log repositories	• CASB • NG-SWG • DLP

Control	Requirements(s)	Netskope Response	Products
CM-11	a. Establish organization-defined policies governing the installation of software by users; b. Enforce software installation policies through the following methods: organization-defined methods; and c. Monitor policy compliance continuously (via CM-7(5)).	Netskope's CASB and NG-SWG enable monitoring and logging of activities in SaaS and IaaS services, capturing details on users, devices, instances, and actions. They build a user activity baseline to detect anomalies, and apply context-aware controls that, among other things, can prevent the unauthorized installation of software by users. Advanced Threat Protection in Netskope offers deobfuscation, recursive file unpacking, and multi-stage sandboxing to detect emerging malware. Device Intelligence identifies and classifies all network-connected devices, utilizing AI/ML to establish behavior baselines and detect anomalies. It enforces granular access controls per zero trust principles and integrates with incident response tools to generate alerts based on the organization's criteria.	• CASB • NG-SWG • Advanced Threat Protection • Device Intelligence
CM-12	a. Identify and document the location of organization-defined information and the specific system components on which the information is processed and stored; b. Identify and document the users who have access to the system and system components where the information is processed and stored; and c. Document changes to the location (i.e., system or system components) where the information is processed and stored. **CM-12 Additional FedRAMP Requirements and Guidance:** **Requirement**: According to FedRAMP Authorization Boundary Guidance.	Netskope's Advanced Analytics maps an organization's data flows across web and cloud services, categorizing data by type and sensitivity. It assesses cloud risk by cataloguing and analyzing app usage. The product dashboard enables administrators to monitor security trends, including the number of apps accessed, threats detected, policies triggered, and the impact on users. Netskope's CASB and NG-SWG leverage a robust data loss prevention (DLP) engine to secure organizational data across various environments, including the web, cloud applications, and endpoint devices. Using machine learning, Netskope's DLP identifies, classifies, and safeguards sensitive data following organizational or regulatory guidelines, applying context-aware policies based on user behavior, device, app usage, network conditions, and actions. It can obfuscate personal information, encrypt sensitive files, or block actions in real time. Additionally, it enforces role-based data access during incident responses, ensures backup integrity, and maintains log files for continuous monitoring and forensic investigations, supporting both internal and regulatory needs.	• CASB • NG-SWG • Advanced Analytics • DLP
	CM-12(1): Use automated tools to identify Federal data and system data that must be protected at the High or Moderate impact levels on organization-defined system components to ensure controls are in place to protect organizational information and individual privacy.		
	CM-12 (1) Additional FedRAMP Requirements and Guidance: **Requirement**: According to FedRAMP Authorization Boundary Guidance.		

Control	Requirements(s)	Netskope Response	Products
CM-14	Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. **CM-14 Additional FedRAMP Requirements and Guidance:** **Guidance**: If digital signatures/ certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) can be utilized.	Netskope's products do not map to this requirement.	

CONTINGENCY PLANNING

Control	Requirements(s)	Netskope Response	Products
CP-1	a. Develop, document, and disseminate to organization-defined personnel or roles: 1. Organization-level; mission/ business process-level; system-level contingency planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and c. Review and update the current contingency planning: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes.	Several Netskope products can assist with determining the scope of a contingency plan, testing the plan, and resuming mission-critical and essential business functions. For example, Netskope's CASB and NG-SWG can identify and inventory both managed and unmanaged apps and cloud services, and Netskope's Device Intelligence can identify and inventory devices connecting to the organization's network.	• All products

Control	Requirements(s)	Netskope Response	Products
CP-2	a. Develop a contingency plan for the system that: 1. Identifies essential mission and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure; 5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented; 6. Addresses the sharing of contingency information; and 7. Is reviewed and approved by organization-defined personnel or roles; b. Distribute copies of the contingency plan to organization-defined key contingency personnel (identified by name and/or by role) and organizational elements; c. Coordinate contingency planning activities with incident handling activities; d. Review the contingency plan for the system at least annually; e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicate contingency plan changes to organization-defined key contingency personnel (identified by name and/or by role) and organizational elements;	The Netskope platform helps organizations identify and prioritize essential services based on usage intensity, including devices, web, cloud services, and remote access. It supports the restoration of remote access and critical services and provides continuous assessments to prevent further targeting. Netskope's Cloud Access Security Broker (CASB) and Next Generation Secure Web Gateway (NG-SWG) can identify and inventory both managed and unmanaged apps and cloud services. This capability helps in evaluating the full extent necessary for contingency plan testing and ensuring the resumption of essential mission and business functions. Netskope evaluates SaaS applications using its Cloud Confidence Index (CCI), which helps organizations understand the risks involved with each vendor's application or cloud service. Assessment criteria include security policies, certifications, audit capabilities, legal and privacy issues, and more. Netskope Data loss prevention tool uses machine learning to ensure that only approved public updates about incident recovery are released, effectively identifying, classifying, and protecting sensitive and critical data within the organization.	• CASB • NG-SWG • Cloud Confidence Index (CCI) • DLP

Control	Requirements(s)	Netskope Response	Products
	g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and h. Protect the contingency plan from unauthorized disclosure and modification. **CP-2 Additional FedRAMP Requirements and Guidance:** **Requirement**: For JAB authorizations the contingency lists include designated FedRAMP personnel. **Requirement**: CSPs must use the FedRAMP Information System Contingency Plan (ISCP) Template (available on the fedramp.gov: https://www.fedramp.gov/assets/resources/templates/SSP-Appendix-G-Information-System-Contingency-Plan-(ISCP)-Template.docx)..		
	CP-2(1): Coordinate contingency plan development with organizational elements responsible for related plans.		
	CP-2(2): Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.		
	CP-2(3): Plan for the resumption of all mission and business functions within time period defined in service provider and organization SLA of contingency plan activation.		
	CP-2(5): Plan for the continuance of essential mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.		
	CP-2(8): Identify critical system assets supporting all; essential mission and business functions.		

Control	Requirements(s)	Netskope Response	Products
CP-3	a. Provide contingency training to system users consistent with assigned roles and responsibilities: 1. Within 10 days of assuming a contingency role or responsibility; 2. When required by system changes; and 3. At least annually thereafter; and b. Review and update contingency training content at least annually and following organization-defined events. **CP-3 Additional FedRAMP Requirements and Guidance:** **(a) Requirement:** Privileged admins and engineers must take the basic contingency training within 10 days. Consideration must be given for those privileged admins and engineers with critical contingency-related roles, to gain enough system context and situational awareness to understand the full impact of contingency training as it applies to their respective level. Newly hired critical contingency personnel must take this more in-depth training within 60 days of hire date when the training will have more impact..	Netskope's products do not map to this requirement.	
	CP-3(1): Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.		
CP-4	a. Test the contingency plan for the system at least annually using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: functional exercises. b. Review the contingency plan test results; and c. Initiate corrective actions, if needed. **CP-4 Additional FedRAMP Requirements and Guidance:** **(a) Requirement**: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended); plans are approved by the JAB/AO prior to initiating testing.	Netskope's CASB and NG-SWG can aid in contingency planning, testing, and business continuity by identifying and inventorying managed and unmanaged apps and cloud services, and categorizing them by usage and risk, Advanced Analytics maps data flows across web and cloud services, assesses cloud risks, and categorizes data by its sensitivity. It also provides a dashboard for administrators to track security trends, including app usage, threats detected, policies triggered, and the number of affected users	• CASB • NG-SWG • Public Cloud Security • Advanced Analytics • CTO

Control	Requirements(s)	Netskope Response	Products
	(a) Requirement: The service provider must include the Contingency Plan test results with the security package within the Contingency Plan-designated appendix (Appendix G, Contingency Plan Test Report).		
	CP-4(1): Coordinate contingency plan testing with organizational elements responsible for related plans.		
	CP-4(2): Test the contingency plan at the alternate processing site: (a) To familiarize contingency personnel with the facility and available resources; and (b) To evaluate the capabilities of the alternate processing site to support contingency operations.		
CP-6	a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.	Netskope's products do not map to this requirement.	
	CP-6(1): Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.		
	CP-6(2): Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.		
	CP-6(3): Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.		

Control	Requirements(s)	Netskope Response	Products
CP-7	a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of organization-defined system operations for essential mission and business functions within organization-defined time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable; b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and c. Provide controls at the alternate processing site that are equivalent to those at the primary site. **CP-7 Additional FedRAMP Requirements and Guidance:** **(a) Requirement**: The service provider defines a time period consistent with the recovery time objectives and business impact analysis	Netskope's products do not map to this requirement	
	CP-7(1): Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats. **CP-7 (1) Additional FedRAMP Requirements and Guidance:** **Guidance:** The service provider may determine what is considered a sufficient degree of separation between the primary and alternate processing sites, based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites will be less relevant.		
	CP-7(2): Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outline explicit mitigation actions.		

Control	Requirements(s)	Netskope Response	Products
	CP-7(3): Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).		
	CP-7(4): Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions		
CP-8	Establish alternate telecommunications services, including necessary agreements to permit the resumption of organization-defined system operations for essential mission and business functions within organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. **CP-8 Additional FedRAMP Requirements and Guidance:** **Requirement**: The service provider defines a time period consistent with the recovery time objectives and business impact analysis..	Netskope's products do not map to this requirement.	
	CP-8(1): (a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and (b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/ or alternate telecommunications services are provided by a common carrier.		
	CP-8(2): Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.		
	CP-8(3): Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.		

Control	Requirements(s)	Netskope Response	Products
	CP-8(4): (a) Require primary and alternate telecommunications service providers to have contingency plans; (b) Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and (c) Obtain evidence of contingency testing and training by providers annually.		
CP-9	a. Conduct backups of user-level information contained in organization-defined system components; daily incremental; weekly full; b. Conduct backups of system-level information contained in the system daily incremental; weekly full; c. Conduct backups of system documentation, including security- and privacy-related documentation daily incremental; weekly full; and d. Protect the confidentiality, integrity, and availability of backup information. **CP-9 Additional FedRAMP Requirements and Guidance:** **Requirement:** The service provider shall determine what elements of the cloud environment require the Information System Backup control. The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check. **(a) Requirement:** The service provider maintains at least three (3) backup copies of user-level information (at least one (1) of which is available online) or provides an equivalent alternative. **(b) Requirement**: The service provider maintains at least three (3) backup copies of system-level information (at least one (1) of which is available online) or provides an equivalent alternative.	Netskope's CASB and NG-SWG feature a robust data loss prevention (DLP) engine that secures organizational data across web platforms, cloud applications, and endpoint devices. DLP uses machine learning to detect, classify, and safeguard sensitive information according to organizational and regulatory standards. Context-aware policies enhance protection by considering user, device, application, network, and action contexts, enabling real-time measures like obfuscating personal data, encrypting sensitive files, or blocking actions. Additionally, Netskope's DLP supports role-based data access for incident response, ensures backup integrity, and maintains dedicated log repositories for continuous monitoring and forensic investigations. Netskope's Data loss prevention (DLP) tool helps check the integrity of data, using machine learning to accurately and reliably identify, classify, and/or protect sensitive and critical data across an organization's IT ecosystem. Furthermore, Netskope's Zero Trust Network Access (Private Access) and Cloud Firewall capabilities support network segmentation to ensure backups are stored in a secure environment.	• CASB • NG-SWG • DLP • Private Access • Cloud Firewall

Control	Requirements(s)	Netskope Response	Products
	(c) Requirement: The service provider maintains at least three (3) backup copies of information system documentation including security information (at least one (1) of which is available online) or provides an equivalent alternative.		
	CP-9(1): Test backup information at least monthly to verify media reliability and information integrity.		
	CP-9(2): Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.		
	CP-9(3): Store backup copies of organization- defined critical system software and other security-related information in a separate facility or in a fire rated container that is not collocated with the operational system.		
	CP-9(5): Transfer system backup information to the alternate storage site time period and transfer rate consistent with the recovery time and recovery point objectives defined in the service provider and organization SLA.		
	CP-9(8): Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of all backup files. **CP-9 (8) Additional FedRAMP Requirements and Guidance:** **Guidance**: Note that this enhancement requires the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13.)		
CP-10	Provide for the recovery and reconstitution of the system to a known state within organization-defined time period consistent with recovery time and recovery point objectives after a disruption, compromise, or failure	Netskope's CASB and NG-SWG leverage a comprehensive data loss prevention (DLP) engine to protect organizational data across web, cloud, and endpoints, using machine learning and context-aware policies. Netskope's DLP enforces role-based access during incident response, ensures backup integrity, and facilitates continuous monitoring and forensic investigations.	• CASB • NG-SWG • Public Cloud Security • Cloud Confidence Index (CCI) • DLP

Control	Requirements(s)	Netskope Response	Products
	CP-10(2): Implement transaction recovery for systems that are transaction-based.	Netskope's products do not map to this requirement.	
	CP-10(4): Provide the capability to restore system components within a time period consistent with the restoration time periods defined in the service provider and organization SLA from configuration-controlled and integrity-protected information representing a known, operational state for the components.	Netskope products support resilience requirements in both normal and adverse conditions including the ability to both scale up and scale down on demand. Netskope supports a 99.999% SLA on availability.	• All products

IDENTIFICATION AND AUTHENTICATION

Control	Requirements(s)	Netskope Response	Products
IA-1	a. Develop, document, and disseminate to organization-defined personnel or roles: 1. Organization-level; mission/ business process-level; system-level identification and authentication policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and c. Review and update the current identification and authentication: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes.	Netskope enforces organizational policies and aids communication through pop-up banners to alert employees about potential policy breaches. Netskope's CASB and NG-SWG leverage a machine-learning-based data loss prevention (DLP) engine to safeguard data across web, cloud applications, and endpoint devices by identifying, classifying, and protecting sensitive data. DLP enforces real-time policies and role-based access, ensuring data integrity and enabling forensic investigations. Netskope's NG-SWG and Private Access integrate with third-party identity providers to extend SSO/MFA across web and cloud apps and services. Private Access provides secure remote access to private apps via end-to-end encryption and granular access controls based on zero trust principles, logging all access attempts. Netskope's Advanced Analytics maps data flows and assesses cloud risk, allowing administrators to track security trends via a comprehensive dashboard.	• CASB • NG-SWG • Public Cloud Security • DLP • Private Access • Advanced Analytics
IA-2	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users. **IA-2 Additional FedRAMP Requirements and Guidance:** **Guidance**: "Phishing-resistant" authentication refers to authentication processes designed to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system.	Netskope's NG-SWG and Private Access integrate with NIST-compliant identity providers, extending SSO/MFA to web and cloud apps. NG-SWG decodes and logs over 100 inline activities to detect anomalies, applying granular policy controls based on the activity or data. Controls go beyond "allow" or "block," responding to risky behavior by requesting an additional MFA or business justification for risky actions, notifying users of potential policy violations, or providing cybersecurity training. Customizable thresholds for generating reports and alerts can be integrated with the organization's SIEM tool to aid in incident response, and detailed logging assists in non-repudiation.	• NG-SWG • Public Cloud Security • Private Access • CTO

Control	Requirements(s)	Netskope Response	Products
	Requirement: For all control enhancements that specify multi-factor authentication, the implementation must adhere to the Digital Identity Guidelines specified in NIST Special Publication 800-63B. **Requirement**: Multi-factor authentication must be phishing-resistant. **Requirement**: All uses of encrypted virtual private networks must meet all applicable Federal requirements and architecture, data flow, and security and privacy controls must be documented, assessed, and authorized to operate..	Netskope's Private Access allows remote access to private apps from any device, anywhere, integrating with NIST-compliant identity providers for secure authentication. It ensures data security with end-to-end encryption and limits access based on zero trust principles. Private Access logs all access attempts and enforces policies on failed login attempts.	
	IA-2(1): Implement multi-factor authentication for access to privileged accounts. **IA-2 (1) Additional FedRAMP Requirements and Guidance:** **Guidance**: Multi-factor authentication to subsequent components in the same user domain is not required. **Requirement**: According to SP 800-63-3, SP 800-63A (IAL), SP 800-63B (AAL), and SP 800-63C (FAL). **Requirement**: Multi-factor authentication must be phishing-resistant.		
	IA-2(2): Implement multi-factor authentication for access to non-privileged accounts. **IA-2 (2) Additional FedRAMP Requirements and Guidance:** **Guidance**: Multi-factor authentication to subsequent components in the same user domain is not required. **Requirement**: According to SP 800-63-3, SP 800-63A (IAL), SP 800-63B (AAL), and SP 800-63C (FAL). **Requirement**: Multi-factor authentication must be phishing-resistant.		

Control	Requirements(s)	Netskope Response	Products
	IA-2(5): When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.		
	IA-2(6): Implement multi-factor authentication for local, network, and remote access to privileged accounts; non-privileged accounts such that: (a) One of the factors is provided by a device separate from the system gaining access; and (b) The device meets FIPS-validated or NSA-approved cryptography. **IA-2 (6) Additional FedRAMP Requirements and Guidance:** **Guidance**: PIV=separate device. Please refer to NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials. **Guidance**: See SC-13 Guidance for more information on FIPS-validated or NSA-approved cryptography.		
	IA-2(8): Implement replay-resistant authentication mechanisms for access to [FedRAMP Assignment: privileged accounts; non-privileged accounts].		
	IA-2(12): Accept and electronically verify Personal Identity Verification-compliant credentials. **IA-2 (12) Additional FedRAMP Requirements and Guidance:** **Guidance**: Include Common Access Card (CAC), i.e., the DoD technical implementation of PIV/FIPS 201/HSPD-12		
IA-3	Uniquely identify and authenticate organization-defined devices and/or types of devices before establishing a local; remote; network connection.	Netskope's Private Access offers remote access to private apps hosted on-premises or in the cloud from any device, anywhere. It ensures secure authentication through integration with NIST-compliant third-party identity providers, uses end-to-end encryption for data security, and implements granular access controls based on zero trust principles. Additionally, Private Access logs all access attempts and enforces policies on failed login attempts.	• Private Access • Device Intelligence

Control	Requirements(s)	Netskope Response	Products
		Netskope Device Intelligence categorizes all devices connecting to the network, whether managed or unmanaged, and segments them to isolate risky devices. Its AI/ML engine establishes a baseline of normal device behavior, detects anomalies, and applies detailed access and activity controls according to zero trust principles. It also integrates with incident response tools to generate security alerts based on predefined criteria.	
IA-4	Manage system identifiers by: a. Receiving authorization from at a minimum, the ISSO (or similar role within the organization) to assign an individual, group, role, service, or device identifier; b. Selecting an identifier that identifies an individual, group, role, service, or device; c. Assigning the identifier to the intended individual, group, role, service, or device; and d. Preventing reuse of identifiers for at least two (2) years. IA-4(4): Manage individual identifiers by uniquely identifying each individual as contractors; foreign nationals.	Netskope's NG-SWG and CASB integrate with third-party identity providers like Okta and Ping to extend SSO/ MFA across web and managed and unmanaged cloud applications. Netskope's Private Access offers remote access to private applications hosted on-premises or in the cloud from any device. It integrates with third-party identity providers for secure authentication, utilizes end-to-end encryption for data security, and applies zero trust principles to limit access. Private Access logs all access attempts and enforces policies on failed login attempts.	• CASB • NG-SWG • Public Cloud Security • Private Access • CTO
IA-5	Manage system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; b. Establishing initial authenticator content for any authenticators issued by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators; e. Changing default authenticators prior to first use; f. Changing or refreshing authenticators organization-defined time period by authenticator type or when organization-defined events occur;	Netskope's NG-SWG and CASB integrate with third-party identity providers like Okta and Ping to extend SSO/ MFA across web and managed and unmanaged cloud applications. Netskope's ZTNA (Zero Trust Network Access) Next provides secure, remote access to private apps hosted on-premises or in the cloud from any device. It integrates with third-party identity providers compliant with NIST standards, uses end-to-end encryption, and enforces granular controls based on zero trust principles. Private Access logs all access attempts and enforces policies on failed login attempts	• CASB • NG-SWG • Public Cloud Security • Private Access • CTO

Control	Requirements(s)	Netskope Response	Products
	g. Protecting authenticator content from unauthorized disclosure and modification; h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and i. Changing authenticators for group or role accounts when membership to those accounts changes.		
	I**A-5 Additional FedRAMP Requirements and Guidance:** **Guidance**: SP 800-63C Section 6.2.3 Encrypted Assertion requires that authentication assertions be encrypted when passed through third parties, such as a browser. For example, a SAML assertion can be encrypted using XML-Encryption, or an OpenID Connect ID Token can be encrypted using JSON Web Encryption (JWE). **Requirement**: Authenticators must be compliant with NIST SP 800-63-3 Digital Identity Guidelines IAL, AAL, FAL level 3. Link https://pages.nist.gov/800-63-3.		
	IA-5(1): For password-based authentication: (a) Maintain a list of commonly used, expected, or compromised passwords and update the list organization-defined frequency and when organizational passwords are suspected to have been compromised directly or indirectly; (b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly used, expected, or compromised passwords in IA-5(1)(a); (c) Transmit passwords only over cryptographically protected channels; (d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;		

Control	Requirements(s)	Netskope Response	Products
	(e) Require immediate selection of a new password upon account recovery; (f) Allow user selection of long passwords and passphrases, including spaces and all printable characters; (g) Employ automated tools to assist the user in selecting strong password authenticators; and (h) Enforce the following composition and complexity rules: organization-defined composition and complexity rules. **IA-5 (1) Additional FedRAMP Requirements and Guidance:** **Guidance**: Note that (c) and (d) require the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13). **Requirement**: Password policies must be compliant with NIST SP 800-63B for all memorized, lookup, out-of-band, or one-time-passwords (OTP). Password policies shall not enforce special character or minimum password rotation requirements for memorized secrets of users. **(h) Requirement**: For cases where technology doesn't allow multi-factor authentication, these rules should be enforced: must have a minimum length of 14 characters and must support all printable ASCII characters. For emergency use accounts, these rules should be enforced: must have a minimum length of 14 characters, must support all printable ASCII characters, and passwords must be changed if used.		
	IA-5(2): For public key-based authentication: (a) Enforce authorized access to the corresponding private key; and (1) Map the authenticated identity to the account of the individual or group; and	Netskope's products do not map to this requirement.	

Control	Requirements(s)	Netskope Response	Products
	(b) When public key infrastructure (PKI) is used: (1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and (2) Implement a local cache of revocation data to support path discovery and validation.		
	IA-5(6): Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	Netskope's CASB and NG-SWG leverage a powerful data loss prevention (DLP) engine to secure organizational data across web, cloud applications, and endpoints. This DLP uses machine learning for identifying and classifying sensitive data, enforcing context-aware policies based on user, device, app, and network information. It ensures real-time data protection through measures like obfuscation, encryption, and action blocking.	• CASB • NG-SWG • DLP
	IA-5(7): Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage. **IA-5 (7) Additional FedRAMP Requirements and Guidance:** **Guidance:** In this context, prohibited static storage refers to any storage where unencrypted authenticators, such as passwords, persist beyond the time required to complete the access process.	Netskope's Data loss prevention (DLP) detects and prevents the sharing of passwords and other authenticators with unauthorized parties.	• CASB • NG-SWG • Public Cloud Security • Advanced DLP • CTO
	IA-5(8): Implement different authenticators in different user authentication domains to manage the risk of compromise due to individuals having accounts on multiple systems. **IA-5 (8) Additional FedRAMP Requirements and Guidance:** **Guidance**: If a single user authentication domain is used to access multiple systems, such as in single sign-on, then only a single, authenticator is required.	Netskope products integrate with third-party identity providers like Okta to extend SSO/MFA across web, managed and unmanaged apps and cloud services.	• NG-SWG • CASB • Private Access

Control	Requirements(s)	Netskope Response	Products
	IA-5(8): Implement different authenticators in different user authentication domains to manage the risk of compromise due to individuals having accounts on multiple systems. **IA-5 (8) Additional FedRAMP Requirements and Guidance:** **Guidance**: If a single user authentication domain is used to access multiple systems, such as in single-sign-on, then only a single authenticator is required.	Netskope products integrate with third party identity providers like Okta to extend SSO/MFA across web, managed and unmanaged apps and cloud services.	• NG-SWG • CASB • Private Access
	A-5(13): Prohibit the use of cached authenticators after organization-defined time period. **IA-5 (13) Additional FedRAMP Requirements and Guidance:** **Guidance**: For components subject to configuration baseline(s) (such as STIG or CIS,) the time period should conform to the baseline standard.	Netskope's products do not map to this requirement.	
IA-6	Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.	Netskope's products do not map to this requirement.	
IA-7	Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.	Netskope's products do not map to this requirement.	
IA-8	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.	Netskope's CASB aids in asset inventory, acquisition strategy, third-party risk management, and business continuity planning by identifying and assessing managed and unmanaged apps and cloud services within an organization's IT ecosystem, based on usage and risk level. Private Access provides secure remote access to on-premises or cloud-hosted private apps from any device. It integrates with third-party identity providers for secure authentication, uses end-to-end encryption, applies zero trust principles to control access, logs access attempts, and enforces policies on failed login attempts.	• CASB • Public Cloud Security • Private Access • CTO

Control	Requirements(s)	Netskope Response	Products
	IA-8(1): Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.	Netskope products can provide external stakeholders secure access to organizations' systems including both cloud and on-premises applications and services.	• Private Access
	IA-8(2): (a) Accept only external authenticators that are NIST-compliant; and (b) Document and maintain a list of accepted external authenticators.	Netskope's NG-SWG and Private Access integrate with NIST-compliant third-party identity providers, extending SSO/MFA across web and cloud apps as well as cloud-hosted and on-premises services.	• NG-SWG • Private Access
	IA-8(4): Conform to the following profiles for identity management: organization-defined identity management profiles.	Netskope's products do not map to this requirement.	
IA-11	Require users to re-authenticate when organization-defined circumstances or situations requiring re-authentication. **IA-11 Additional FedRAMP Requirements and Guidance:** **Guidance:** The fixed time period cannot exceed the limits set in SP 800-63. At this time they are: • AAL3 (high baseline) • Twelve (12) hours or • Fifteen (15) minutes of inactivity.	The NG-SWG monitors user activities, applying granular policy controls to detect anomalous behavior and enforce context-aware responses, such as requiring re-authentication or cybersecurity training. The NG-SWG also generates customizable reports and alerts to facilitate incident response and non-repudiation. Netskope's Private Access offers secure remote access to private on-premises or cloud-hosted applications from any device, anywhere. Integrating with NIST-compliant third-party identity providers, it ensures secure authentication. The solution also features end-to-end encryption to secure data in use and in transit and applies zero trust principles for granular access and privilege controls. Additionally, Private Access logs all access attempts and enforces organizational policies on failed login attempts, providing enhanced security and compliance.	• NG-SWG • Private Access
IA-12	a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines; b. Resolve user identities to a unique individual; and c. Collect, validate, and verify identity evidence. **IA-12 Additional FedRAMP Requirements and Guidance:** **Guidance:** In accordance with NIST SP 800-63A Enrollment and Identity Proofing.	Netskope's Private Access offers secure remote access to on-premises or cloud-hosted private applications from any device, regardless of location. It integrates with NIST-compliant third-party identity providers for secure authentication and employs end-to-end encryption to protect data both in use and during transmission. Adhering to zero trust principles, Private Access applies granular controls to restrict access and privileges. Additionally, it logs all access attempts and can enforce organizational policies concerning failed login attempts.	• Private Access
	IA-12(2): Require evidence of individual identification be presented to the registration authority.	Netskope's products do not map to this requirement.	

Control	Requirements(s)	Netskope Response	Products
	IA-12(3): Require that the presented identity evidence be validated and verified through organizational-defined methods of validation and verification. IA-12(4): Require that the validation and verification of identity evidence be conducted in person before a designated registration authority. IA-12(5): Require that a registration code; notice of proofing be delivered through an out-of-band channel to verify the user's address (physical or digital) of record. **IA-12 (5) Additional FedRAMP Requirements and Guidance:** **Guidance**: In accordance with NIST SP 800-63A Enrollment and Identity Proofing.		

INCIDENT RESPONSE

Control	Requirements(s)	Netskope Response	Products
IR-1	a. Develop, document, and disseminate to organization-defined personnel or roles: 1. Organization-level; mission/ business process-level; system-level incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the incident response policy and procedures; and	Netskope helps enforce organizational policies through pop-up banners and coaching pages that notify employees of potential policy infringements. Netskope's Cloud Access Security Broker (CASB) manages asset inventory, acquisition strategy, third-party risk, and business continuity by identifying and assessing cloud services and apps. The Next Generation Secure Web Gateway (NG-SWG) works with third-party identity providers to extend SSO/ MFA, detect anomalous behavior, and apply context-aware controls, generating reports and alerts for incident response. Advanced Analytics maps data flows and assesses cloud risk, while Cloud Log Shipper exports logs to incident response tools. Cloud Ticket Orchestrator automates workflows and incident response.	• CASB • NG-SWG • Public Cloud Security • Advanced Analytics • CLS • CTO

Control	Requirements(s)	Netskope Response	Products
	c. Review and update the current incident response: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes.		
IR-2	a. Provide incident response training to system users consistent with assigned roles and responsibilities: 1. Within ten (10) days for privileged users, thirty (30) days for Incident Response roles of assuming an incident response role or responsibility or acquiring system access; 2. When required by system changes; and 3. At least annually thereafter; and b. Review and update incident response training content at least annually and following organization-defined events.	Netskope's products do not map to this requirement.	
	IR-2(1): Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.		
	IR-2(2): Provide an incident response training environment using organization-defined automated mechanisms.		
IR-3	Test the effectiveness of the incident response capability for the system at least every six (6) months, including functional at least annually using the following tests: organization-defined tests. **IR-3-2 Additional FedRAMP Requirements and Guidance:** **Requirement**: The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended). Functional testing must occur prior to testing for initial authorization. Annual functional testing may be concurrent with required penetration tests (see CA-8). The service provider provides test plans to the JAB/AO annually. Test plans are approved and accepted by the JAB/AO prior to test commencing.	Netskope's CASB and Next Generation Secure Web Gateway (NG-SWG) solutions can identify and inventory both managed and unmanaged apps and cloud services. This aids in determining the scope and preparation of incident response plans and testing their effectiveness. Both solutions provide accurate, consistent, and reproducible response measures and metrics.	• CASB • NG-SWG

Control	Requirements(s)	Netskope Response	Products
	IR-3(2): Coordinate incident response testing with organizational elements responsible for related plans.		
IR-4	a. Implement an incident-handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinate incident handling activities with contingency planning activities; c. Incorporate lessons learned from ongoing incident-handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and d. Ensure the rigor, intensity, scope, and results of incident-handling activities are comparable and predictable across the organization. **IR-4 Additional FedRAMP Requirements and Guidance:** **Requirement**: The FISMA definition of "incident" shall be used: "An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." **Requirement**: The service provider ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.	Netskope's solutions enhance an organization's cybersecurity and incident response capabilities by integrating with security information and event management (SIEM) tools and automating incident response. Netskope's CASB can issue alerts and export logs to the SIEM for automated incident response and review. NG-SWG integrates with third-party identity providers, enabling SSO/MFA across various apps and services. It logs user activities to detect anomalies and applies granular policy controls, including context-aware responses like requiring extra authentication or notifying users of policy violations. NG-SWG also generates customizable reports and alerts for SIEM integration and supports non-repudiation of user actions. The Cloud Log Shipper exports event and alert logs from multiple Netskope tools (NG-SWG, CASB, Private Access, Cloud Firewall, Cloud and SaaS Security Posture Management) to the SIEM or other incident response tools. Additionally, the Cloud Ticket Orchestrator automates incident response workflows by generating service tickets and enforcing role-based access controls. Netskope's Standard User and Entity Behavior Analytics (UEBA) monitors user behavior across various web and cloud services, establishes a normal behavior baseline, and detects anomalies through sequential rules. Adaptive policy controls adjust user access and privileges based on the riskiness and deviation from this baseline behavior. The Advanced UEBA enhances these capabilities with additional machine learning-based anomaly-detection models and introduces the User Confidence Index (UCI), a dynamic risk score reflecting user behavior over time. This risk score helps adapt policies, controls, and recommend security training to mitigate insider threats. The UCI can also be integrated with Netskope's Cloud Exchange to share insider threat information via the Cloud Risk Exchange. Netskope's Cloud Risk Exchange collects and normalizes risk scores for users, devices, and applications from third-party vendors such as Crowdstrike, KnowBe4, and ServiceNow, based on organizational policies and risk tolerance. It enforces adaptive controls to mitigate risks associated with high-risk users, apps, and devices. Cloud Risk Exchange is part of Netskope's Cloud Exchange, included with every Netskope deployment. Netskope's Cloud Threat Exchange enables near real-time ingestion, curation, and bidirectional sharing of threat indicators like malicious URLs and file hashes among Netskope customers and technology partners. It can be configured to automatically share these indicators with an organization's SIEM tool. Cloud Threat Exchange is also a component of Netskope's Cloud Exchange and is standard with every Netskope deployment.	• CASB • NG-SWG • CLS • CTO • UEBA • Advanced UEBA • CRE • CTE
	IR-4(1): Support the incident handling process using [Assignment: organization-defined automated mechanisms].		
	IR-4(2): Include the following types of dynamic reconfiguration for all network, data storage, and computing devices as part of the incident response capability: organization-defined types of dynamic reconfiguration.		

Control	Requirements(s)	Netskope Response	Products
	IR-4(4): Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. IR-4(6): Implement an incident-handling capability for incidents involving insider threats. IR-4(11): Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in organization-defined time period.		
IR-5	Track and document incidents. IR-5(1): Track incidents and collect and analyze incident information using organization-defined automated mechanisms.	Netskope's CASB and NG-SWG can alert and feed data into an organization's security information and event management (SIEM) tool for automated incident response and recovery. It can also generate logs for lessons learned and Progress and Action On Milestones reports. Netskope's Cloud Log Shipper exports event and alert logs from Netskope's NG-SWG, CASB, Private Access, Cloud Firewall, and Cloud and SaaS Security Posture Management tools to the organization's SIEM or other incident response tool.	• CASB • CTO • CLS
IR-6	a. Require personnel to report suspected incidents to the organizational incident response capability within US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended)]; and b. Report incident information to: [Assignment: organization-defined authorities. IR-6 Additional FedRAMP Requirements and Guidance: Requirement: Reports security incident information according to FedRAMP Incident Communications Procedure. IR-6(1): Report incidents using organization-defined automated mechanisms. IR-6(3): Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.	Netskope's NG-SWG and CASB have customizable reporting and alert capabilities and can be integrated with an organization's security information and event management (SIEM) tools to enhance incident response and ensure non-repudiation of user actions. Netskope's Cloud Log Shipper exports event and alert logs from various Netskope tools to an organization's SIEM or incident response tools. Additionally, the Cloud Ticket Orchestrator automates security alert workflows and service ticket generation, helping to enforce role-based access controls during incident response. Netskope evaluates SaaS applications in its Cloud Confidence Index (CCI), offering organizations detailed insights to assess the risk of using each vendor's application or cloud service. The evaluation criteria include the vendor's security policies, certifications, audit capabilities, and legal and privacy concerns.	• NG-SWG • CASB • CLS • CTO • Public Cloud Security • Cloud Confidence Index (CCI)

Control	Requirements(s)	Netskope Response	Products
IR-7	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.	Netskope's CASB can create alerts and export them to an organization's security information and event management (SIEM) tool to enable automated incident response and recovery. Event logs are valuable for learning lessons and generating Progress and Action On Milestones reports. Netskope's NG-SWG integrates with NIST-compliant third-party identity providers and extends single sign-on (SSO) and Multi-Factor Authentication (MFA) across various web and cloud-based apps and services. It decodes and logs over one hundred activities to establish a baseline of user activity, detects anomalies, and enforces granular policy controls based on the activity, data, or app instance. NG-SWG's context-aware controls go beyond simple rules by responding to risky behavior with stepped-up MFA, policy violation notifications, business justification requests, safer alternatives, or referrals to third-party training. It can generate customizable reports and alerts for the SIEM tool, aiding incident response, and its detailed event logging supports non-repudiation of user actions.	• CASB • NG-SWG
	IR-7(1): Increase the availability of incident response information and support using organization-defined automated mechanism.	Netskope's products do not map to this requirement.	
IR-8	a. Develop an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; 8. Addresses the sharing of incident information; 9. Is reviewed and approved by organization-defined personnel or roles at least annually; and	Netskope's Cloud Access Security Broker (CASB) can identify and catalog both managed and unmanaged apps and cloud services, aiding in the development and assessment of an incident response plan. Additionally, CASB offers reliable and reproducible response measures and metrics, enhancing the accuracy and consistency of incident management efforts. Netskope's Next Generation Secure Web Gateway (NG-SWG) aids in identifying both managed and unmanaged apps and cloud services, facilitating an effective incident response plan and its testing. NG-SWG ensures accurate, consistent, and reproducible response measures and metrics. Netskope's Cloud Log Shipper exports logs from various Netskope tools to an organization's SIEM or incident response tool, enhancing event and alert management. The Cloud Ticket Orchestrator automates the creation of service tickets and workflows in response to security alerts, supporting role-based access controls and automating much of an organization's incident response.	• CASB • NG-SWG • CLS • CTO

Control	Requirements(s)	Netskope Response	Products
	10. Explicitly designates responsibility for incident response to organization-defined entities, personnel, or roles. b. Distribute copies of the incident response plan to: see additional FedRAMP Requirements and Guidance; c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing; d. Communicate incident response plan changes to: see additional FedRAMP Requirements and Guidance; and e. Protect the incident response plan from unauthorized disclosure and modification. **IR-8 Additional FedRAMP Requirements and Guidance:** **(b) Requirement**: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel. **(d) Requirement:** The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.		
IR-9	Respond to information spills by: a. Assigning organization-defined personnel or roles with responsibility for responding to information spills; b. Identifying the specific information involved in the system contamination; c. Alerting organization-defined personnel or roles of the information spill using a method of communication not associated with the spill;	Netskope's CASB and NG-SWG, powered by the company's data loss prevention (DLP) engine, offer robust security for data in use, in transit, or at rest, whether across web, cloud applications, or endpoints. Utilizing machine learning, the DLP engine identifies, classifies, and protects sensitive data based on organizational and regulatory needs. Real-time, context-aware policies can obfuscate personal data, encrypt files, or block actions to enhance security. Additionally, the DLP supports role-based data access, incident response, backup integrity, and log file management for continuous monitoring and forensic investigations.	• CASB • NG-SWG • DLP • CLS • SkopeAI

Control	Requirements(s)	Netskope Response	Products
	d. Isolating the contaminated system or system component; e. Eradicating the information from the contaminated system or component; f. Identifying other systems or system components that may have been subsequently contaminated; and g. Performing the following additional actions: organization-defined actions.	Netskope's Cloud Log Shipper facilitates the export of event and alert logs from various Netskope tools to an organization's SIEM or incident response systems for centralized monitoring and analysis. SkopeAI, another integral part of Netskope's DLP, enhances the engine's contextual awareness and efficiency, enabling it to protect unstructured data, detect sophisticated attacks, polymorphic malware, novel phishing domains, zero-day threats, and malicious web content with high accuracy and speed.	
	IR-9(2): Provide information spillage response training at least annually.	Netskope products can provide real-time user coaching when performing actions in web or cloud services. Netskope can coach users on data loss risks, including providing users the option to proceed with the action, cancel the action, or provide a business justification. These controls can be applied to managed and unmanaged apps and websites, so business processes can continue. Netskope can also redirect users to third-party solutions for just-in-time training, reflecting the combination of the attempted activity and the users' perceived danger level to the company.	• CASB • NG-SWG • Private Access
	IR-9(3): Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective: organization-defined procedures.	Netskope's Private Access and Cloud Firewall support network segmentation. Concurrently, Netskope Device Intelligence identifies and categorizes all devices on the network, segmenting them to isolate risky ones.	• Private Access • Cloud Firewall • Device Intelligence
	IR-9(4): Employ the following controls for personnel exposed to information not within assigned access authorizations: organization-defined controls.		

MAINTENANCE

Control	Requirements(s)	Netskope Response	Products
MA-1	a. Develop, document, and disseminate to organization-defined personnel or roles: 1. Organization-level; mission/ business process-level; system-level maintenance policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the maintenance policy and procedures; and c. Review and update the current maintenance: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes. b. Designate an organization-defined official to manage the development, documentation, and dissemination of the maintenance policy and procedures; and c. Review and update the current maintenance: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes.	Netskope enforces organizational policies and aids communication via pop-up banners/coaching pages for policy notifications. Netskope's CASB helps with asset inventory, acquisition strategy, third-party risk management, and business continuity planning by identifying and assessing managed and unmanaged apps in the IT ecosystem. Private Access offers secure remote access to on-premises or cloud-hosted private apps with end-to-end encryption and integration with third-party identity providers. Advanced Analytics maps data flows, assesses cloud risk, and tracks security trends. Netskope's Cloud Log Shipper exports logs from various tools to the organization's SIEM or incident response system, and Cloud Ticket Orchestrator can create service tickets and automate workflows.	• CASB • NG-SWG • Public Cloud Security • Private Access • Advanced Analytics • CLS • CTO

Control	Requirements(s)	Netskope Response	Products
MA-2	a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location; c. Require that organization-defined personnel or roles explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement; d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information]; e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and f. Include the following information in organizational maintenance records: organization-defined information.	Netskope's Private Access provides remote access to on-premises or cloud-hosted private apps from any device, anywhere. Private Access integrates with NIST-compliant third-party identity providers to support secure authentication, uses end-to-end encryption to secure data in use and in motion, and applies granular controls to limit access and privileges based on zero trust principles.	• CASB • NG-SWG • Public Cloud Security • CTO • Private Acces
	MA-2(2): (a) Schedule, conduct, and document maintenance, repair, and replacement actions for the system using organization-defined automated mechanisms; and (b) Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.		
MA-3	a. Approve, control, and monitor the use of system maintenance tools; and b. Review previously approved system maintenance tools at least annually.	Netskope's products do not map to this requirement.	

Control	Requirements(s)	Netskope Response	Products
	MA-3(1): Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.		
	MA-3(2): Check media containing diagnostic and test programs for malicious code before the media are used in the system.		
	MA-3(3): Prevent the removal of maintenance equipment containing organizational information by: (a) Verifying that there is no organizational information contained on the equipment; (b) Sanitizing or destroying the equipment; (c) Retaining the equipment within the facility; or (d) Obtaining an exemption from the information owner explicitly authorizing removal of the equipment from the facility.		
MA-4	a. Approve and monitor nonlocal maintenance and diagnostic activities; b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system; c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions; d. Maintain records for nonlocal maintenance and diagnostic activities; and e. Terminate session and network connections when nonlocal maintenance is completed.	Netskope's Private Access offers secure remote access to private apps across devices, integrating with third-party identity providers for secure authentication, end-to-end encryption for data security, and granular controls following zero trust principles. Private Access also logs all access attempts and enforces policies on login failures, supporting role-based access control to adhere to least privilege access principles. Netskope's Cloud Log Shipper exports event and alert logs from various Netskope security tools to the organization's SIEM or incident response tools.	• Private Access • CLS
	MA-4(3): (a) Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or		

Control	Requirements(s)	Netskope Response	Products
	(b) Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.		
MA-5	a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel; b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	Netskope's products do not map to this requirement.	
	MA-5(1): (a) Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: (1) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and (2) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances, or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and		

Control	Requirements(s)	Netskope Response	Products
	(b) Develop and implement organization-defined alternate controls in the event a system component cannot be sanitized, removed, or disconnected from the system.		
MA-6	Obtain maintenance support and/or spare parts for organization-defined system components within a timeframe to support advertised uptime and availability of failure.	Netskope's products do not map to this requirement.	

MEDIA PROTECTION

Control	Requirements(s)	Netskope Response	Products
MP-1	a. Develop, document, and disseminate to organization-defined personnel or roles: 1. Organization-level; mission/business process-level; system-level media protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the media protection policy and procedures; and c. Review and update the current media protection: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes.	Netskope enforces organizational policies and communicates them using pop-up banners and coaching pages that notify employees of potential infringements. Netskope's CASB and NG-SWG utilize a data loss prevention (DLP) engine with machine learning to secure data across web, cloud apps, and endpoints. DLP supports real-time data protection through context-aware policies and role-based access during incident response. CASB assists with asset inventory, third-party risk management, and business continuity by identifying and assessing the criticality of apps and cloud services, while NG-SWG integrates with third-party identity providers for SSO/MFA, detects anomalous behavior, and applies granular policy controls. It can also generate customizable reports and alerts for SIEM tools. Advanced Analytics maps data flows and cloud app usage, helping administrators track security trends in a comprehensive dashboard. This suite enhances overall data security and policy compliance within an organization.	• CASB • NG-SWG • Public Cloud Security • DLP • Advanced Analytics

Control	Requirements(s)	Netskope Response	Products
MP-2	Restrict access to all types of digital and/or non-digital media containing sensitive information to organization-defined personnel or roles.	Netskope Device Intelligence identifies and classifies all devices, managed and unmanaged, connecting to an organization's network. It groups these devices into network segments to isolate risks. Using AI/ML, it establishes a baseline of normal behavior for each device, detects anomalies, and enforces granular access and activity controls based on zero trust principles. Additionally, it integrates with incident response tools to generate security alerts based on customized criteria. Netskope's Cloud Access Security Broker (CASB) and Next Gen Secure Web Gateway (NG-SWG) utilize a robust data loss prevention (DLP) engine to safeguard organizational data across web, cloud applications, and endpoint devices. Employing machine learning, Netskope's DLP identifies, classifies, and protects sensitive data in alignment with organizational or regulatory standards. Real-time, context-aware policies enhance security by incorporating user, device, app, network, and action contexts to obfuscate, encrypt, or block data as needed. The DLP also enforces role-based access during incident response, ensures backup integrity, and maintains dedicated log repositories to support continuous monitoring and forensic investigations.	• Device Intelligence • CASB • NG-SWG • DLP
MP-3	a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempt no removable media types from marking if the media remain within organization-defined security safeguards not applicable. **MP-3 Additional FedRAMP Requirements and Guidance:** **(b) Guidance:** Second parameter not applicable.	Netskope's Cloud Access Security Broker (CASB) and Next Gen Secure Web Gateway (NG-SWG) utilize a robust data loss prevention (DLP) engine to safeguard organizational data across web, cloud applications, and endpoint devices. Employing machine learning, Netskope's DLP identifies, classifies, and protects sensitive data in alignment with organizational or regulatory standards. Real-time, context-aware policies enhance security by incorporating user, device, app, network, and action contexts to obfuscate, encrypt, or block data as needed. The DLP also enforces role-based access during incident response, ensures backup integrity, and maintains dedicated log repositories to support continuous monitoring and forensic investigations.	• CASB • NG-SWG • DLP
MP-4	a. Physically control and securely store all types of digital and non-digital media with sensitive information within [see additional FedRAMP requirements and guidance]; and b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures. **MP-4 Additional FedRAMP Requirements and Guidance:** **(a) Requirement**: The service provider defines controlled areas within facilities where the information and information system reside.	Netskope's products do not map to this requirement.	

Control	Requirements(s)	Netskope Response	Products
MP-5	a. Protect and control all media with sensitive information during transport outside of controlled areas using prior to leaving secure/ controlled environment: for digital media, encryption in compliance with Federal requirements and utilizes FIPS-validated or NSA-approved cryptography (see SC-13.); for non-digital media, secured in locked container; b. Maintain accountability for system media during transport outside of controlled areas; c. Document activities associated with the transport of system media; and d. Restrict the activities associated with the transport of system media to authorized personnel. **MP-5 Additional FedRAMP Requirements and Guidance:** **(a) Requirement**: The service provider defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the JAB/AO.	Netskope's products do not map to this requirement.	
MP-6	a. Sanitize techniques and procedures IAW NIST SP 800-88 Section 4: Reuse and Disposal of Storage Media and Hardware prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques and procedures; and b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	Netskope's Cloud Access Security Broker (CASB) and Next Gen Secure Web Gateway (NG-SWG) utilize a data loss prevention (DLP) engine to secure data across webs, cloud applications, and endpoints. The DLP engine employs machine learning to identify, classify, and safeguard sensitive information according to organizational or regulatory standards. It uses context-aware policies that consider various factors like users, devices, and network actions to provide real-time data protection. Examples include obfuscating personal data, encrypting files, or blocking specific activities. Netskope's DLP supports role-based data access during incident response, ensures backup integrity, and maintains logs for ongoing monitoring and forensic investigations.	• CASB • NG-SWG • DLP
	MP-6(1): Review, approve, track, document, and verify media sanitization and disposal actions. **MP-6 (1) Additional FedRAMP Requirements and Guidance:** **Requirement**: Must comply with NIST SP 800-88.	Netskope's products do not map to this requirement.	

Control	Requirements(s)	Netskope Response	Products
	MP-6(2): Test sanitization equipment and procedures at least every six (6) months to ensure that the intended sanitization is being achieved. **MP-6 (2) Additional FedRAMP Requirements and Guidance:** **Guidance**: Equipment and procedures may be tested or validated for effectiveness.		
	MP-6(3): Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: organization-defined circumstances requiring sanitization of portable storage devices. **MP-6 (3) Additional FedRAMP Requirements and Guidance:** **Requirement**: Must comply with NIST SP 800-88.		
MP-7	a. Restrict; Prohibit the use of organization-defined types of system media on organization-defined systems or system components using organization-defined controls; and b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.	Netskope's CASB and NG-SWG integrate a robust data loss prevention (DLP) engine, offering comprehensive security for data across web, cloud applications, and endpoint devices. This DLP leverages machine learning to identify, classify, and protect sensitive data following organizational or regulatory standards. Context-aware policies provide real-time data protection, such as obfuscating personal information, encrypting files, or blocking actions. In addition, Netskope's endpoint DLP provides monitoring and protection for endpoint data in use, including device control for USB storage devices. Netskope Device Intelligence identifies and classifies all devices, managed and unmanaged, connecting to an organization's network. It groups these devices into network segments to isolate risks. Using AI/ML, it establishes a baseline of normal behavior for each device, detects anomalies, and enforces granular access and activity controls based on zero trust principles. Additionally, it integrates with incident response tools to generate security alerts based on customized criteria.	• CASB • NG-SWG • Public Cloud Security • DLP • CTO • Device Intelligence

PHYSICAL AND ENVIRONMENTAL PROTECTION

While Netskope's products do not provide physical and environmental security tools, the Netskope platform provides logging and reporting, access management controls, and user and entity behavior analytics that complement the organization's physical security controls.

PLANNING

Control	Requirements(s)	Netskope Response	Products
PL-1	a. Develop, document, and disseminate to organization-defined personnel or roles: 1. Organization-level; mission/ business process-level; system-level planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the planning policy and the associated planning controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the planning policy and procedures; and c. Review and update the current planning: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes.	Netskope enforces organizational policies and aids communication through pop-up banners that alert employees to potential policy breaches. It evaluates SaaS applications via its Cloud Confidence Index (CCI), examining security policies, certifications, and more to assess vendor risks. Netskope's Cloud Access Security Broker (CASB) helps manage asset inventory, third-party risks, and business continuity by identifying and evaluating cloud services' usage and risk. Netskope's Advanced Analytics tracks data flows across cloud services, categorizing data by sensitivity and assessing cloud risks. Its dashboard helps administrators monitor security trends, app usage, threats detected, policies triggered, and users affected.	• CASB • NG-SWG • Public Cloud Security • Cloud Confidence Index (CCI) • Advanced Analytics
PL-2	a. Develop security and privacy plans for the system that: 1. Are consistent with the organization's enterprise architecture; 2. Explicitly define the constituent system components;	Netskope's CASB and NG-SWG leverage a powerful data loss prevention (DLP) engine to secure organizational data across web, cloud applications, and endpoints. This DLP uses machine learning for identifying and classifying sensitive data, enforcing context-aware policies based on user, device, app, and network information. It ensures real-time data protection through measures like obfuscation, encryption, and action blocking.	• CASB • NG-SWG • DLP • Device Intelligence

Control	Requirements(s)	Netskope Response	Products
	3. Describe the operational context of the system in terms of mission and business processes; 4. Identify the individuals that fulfill system roles and responsibilities; 5. Identify the information types processed, stored, and transmitted by the system; 6. Provide the security categorization of the system, including supporting rationale; 7. Describe any specific threats to the system that are of concern to the organization; 8. Provide the results of a privacy risk assessment for systems processing personally identifiable information; 9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components; 10. Provide an overview of the security and privacy requirements for the system; 11. Identify any relevant control baselines or overlays, if applicable; 12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions; 13. Include risk determinations for security and privacy architecture and design decisions; 14. Include security- and privacy-related activities affecting the system that require planning and coordination to include chief privacy and ISSO and/or similar role or designees; and 15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.	The DLP also supports role-based data access during incidents, backup integrity, and detailed log management for continuous monitoring and forensic investigations. Netskope Device Intelligence catalogs and classifies devices connecting to the network, grouping them into segments to isolate potentially risky ones. It uses AI/ML to establish normal device behavior and detect anomalies, applying granular controls based on zero trust principles. Device Intelligence integrates with incident response tools to generate security alerts based on predefined criteria. Netskope's Advanced Analytics maps an organization's data flows across web and cloud services, characterizing data by category and sensitivity. Advanced Analytics also assesses cloud risk by cataloguing and characterizing cloud app usage, and the product dashboard allows administrators to track security trends by number of apps accessed, threats detected, policies triggered, and users impacted.	

Control	Requirements(s)	Netskope Response	Products
	b. Distribute copies of the plans and communicate subsequent changes to the plans to include chief privacy and ISSO and/or similar role; c. Review the plans at least annually; d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and e. Protect the plans from unauthorized disclosure and modification.		
PL-4	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy; b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system; c. Review and update the rules of behavior at least annually; and d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge at least annually and when the rules are revised or changed.	Netskope's CASB monitors and logs SaaS and IaaS activities, providing data on user, device, instance, and action. It enforces real-time activity-level and data loss prevention controls, including requesting business justifications for risky actions or offering policy training. Netskope's Next Gen Secure Web Gateway (NG-SWG) integrates with NIST-compliant identity providers to extend SSO/MFA across web and cloud apps, decoding and logging over 100 activities. NG-SWG establishes user activity baselines to detect anomalies, applying detailed policy controls based on activity or data type. Context-aware responses to risky behavior can include stepped-up MFA, policy violation notifications, and cybersecurity training referrals. The NG-SWG also generates customizable reports and alerts for SIEM integration to aid in incident response, ensuring non-repudiation of user actions. The Standard User and Entity Behavior Analytics (UEBA) module tracks user behavior across web and cloud services, creating normal behavior baselines to identify anomalies and adapt policy controls accordingly. The Advanced UEBA includes more ML-based detection models and introduces the User Confidence Index (UCI), a dynamic risk score used to adjust policies, recommend training, and mitigate insider threats. UCI data can be shared via Netskope's Cloud Exchange for broader threat intelligence.	• CASB • NG-SWG • UEBA • Advanced UEBA
	PL-4(1): Include in the rules of behavior, restrictions on: (a) Use of social media, social networking sites, and external sites/applications; (b) Posting organizational information on public websites; and (c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.		

Control	Requirements(s)	Netskope Response	Products
PL-8	a. Develop security and privacy architectures for the system that: 1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information; 2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals; 3. Describe how the architectures are integrated into and support the enterprise architecture; and 4. Describe any assumptions about, and dependencies on, external systems and services; b. Review and update the architectures at least annually and when a significant change occurs to reflect changes in the enterprise architecture; and c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions. **PL-8 Additional FedRAMP Requirements and Guidance:** **(b) Guidance**: Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F.	Netskope helps organizations establish a secure network architecture aligned with industry-standard cybersecurity and data privacy best practices. This includes a "defense-in-depth" strategy that reduces interactions between security layers, ensuring they function independently. The Netskope platform, when properly customized and configured, mitigates risks to organizational operations, assets, individuals, and third parties. Netskope's products support layered security structures that prevent dependencies between design layers. Private Access, one of Netskope's offerings, provides remote access to on-premises or cloud-hosted private apps from any device globally. It integrates with NIST-compliant third-party identity providers for secure authentication, uses end-to-end encryption to protect data, and applies zero trust principles to control access and privileges strictly. Additionally, Private Access logs all access attempts and enforces organizational policies on failed login attempts.	• All products • Private Access
PL-10	Select a control baseline for the system. **PL-10 Additional FedRAMP Requirements and Guidance:** **Requirement**: Select the appropriate FedRAMP Baseline.	Netskope's Cloud Access Security Broker (CASB) aids in asset inventory, acquisition strategy, third-party risk management, and business continuity planning by identifying and assessing both managed and unmanaged apps and cloud services. Netskope's Next Generation Secure Web Gateway (NG-SWG) integrates with identity providers for SSO/MFA across web and cloud apps, and it can detect and log multiple activities to monitor for anomalous behavior, applying granular policy controls and generating reports for incident response. Finally, Netskope's Device Intelligence classifies devices connecting to the network and uses AI/ML to detect anomalies, applying access controls in line with zero trust principles and generating alerts for incident response.	• CASB • NG-SWG • Device Intelligence
PL-11	Tailor the selected control baseline by applying specified tailoring actions.		

PERSONNEL SECURITY

Control	Requirements(s)	Netskope Response	Products
PS-1	a. Develop, document, and disseminate to organization-defined personnel or roles: 1. Organization-level; mission/ business process-level; system-level personnel security policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the personnel security policy and procedures; and c. Review and update the current personnel security: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes.	Netskope enforces organizational policies and aids communication through pop-up banners/coaching pages that notify employees of potential policy infringements. Netskope's CASB helps with asset inventory, acquisition strategy, third-party risk management, and business continuity planning by identifying and assessing managed and unmanaged apps and cloud services. Netskope's NG-SWG integrates with NIST-compliant identity providers, extending SSO/MFA across cloud apps and services, decoding inline activities, detecting anomalous behavior, applying granular controls, and generating reports. User and Entity Behavior Analytics (UEBA) tracks and detects anomalous behavior, adapting policies based on risk. And Advanced UEBA employs more ML-based anomaly detection models and provides a User Confidence Index for adapting policies. Private Access ensures secure remote access to private apps with end-to-end encryption and granular controls. Netskope's Advanced Analytics maps data flows, assesses cloud risks, and tracks security trends within a dashboard.	• CASB • NG-SWG • Public Cloud Security • UEBA • Private Access • Advanced Analytics • Advanced UEBA
PS-2	a. Assign a risk designation to all organizational positions; b. Establish screening criteria for individuals filling those positions; and c. Review and update position risk designations at least annually.	Advanced User and Entity Behavior Analytics (UEBA) integrates numerous ML-based anomaly-detection models, surpassing Standard UEBA. It includes a User Confidence Index (UCI), a dynamic and quantifiable risk score based on user behavior over time. This index aids in adapting policies, controls, and recommending security training to detect and mitigate insider threats. Additionally, UCI can integrate with Netskope's Cloud Exchange to share insider threat information via the Netskope Cloud Risk Exchange.	• CASB • NG-SWG • Advanced UEBA • CTE • UCI

Control	Requirements(s)	Netskope Response	Products
PS-3	a. Screen individuals prior to authorizing access to the system; and b. Rescreen individuals in accordance with national security clearances; a reinvestigation is required during the fifth (5th) year for top secret security clearance, the tenth (10th) year for secret security clearance, and the fifteenth (15th) year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the fifth (5th) year. There is no reinvestigation for other moderate risk positions or any low risk positions.	Netskope's products do not map to this requirement.	
	PS-3(3): Verify that individuals accessing a system processing, storing, or transmitting information requiring special protection: (a) Have valid access authorizations that are demonstrated by assigned official government duties; and (b) Satisfy personnel screening criteria – as required by specific information.		
PS-4	Upon termination of individual employment: a. Disable system access within one (1) hour; b. Terminate or revoke any authenticators and credentials associated with the individual; c. Conduct exit interviews that include a discussion of organization-defined information security topics; d. Retrieve all security-related organizational system-related property; and e. Retain access to organizational information and systems formerly controlled by the terminated individual.	Netskope offers various products, including CASB, NG-SWG, DLP, and ZTNA Next, all which support role-based access control (RBAC) to assist organizations in enforcing access management policies based on the principle of least privilege. This ensures that users have the minimum necessary access required for their roles, enhancing security across multiple platforms. Netskope Device Intelligence identifies, catalogs, and classifies all managed and unmanaged devices connecting to the organization's network, and groups devices into network segments to isolate risky devices. Netskope's Device Intelligence's AI/ML engine creates a baseline of normal behavior at the device level, detects anomalous behavior, and can apply granular access and activity controls in accordance with zero trust principles. Device Intelligence can be integrated with the organization's incident response tools to generate security alerts based on criteria set by the organization.	• CASB • NG-SWG • DLP • Private Access • Device Intelligence

Control	Requirements(s)	Netskope Response	Products
	PS-4(2): Use organization-defined automated mechanisms to notify access control personnel responsible for disabling access to the system of individual termination actions; disable access to system resources.		
PS-5	a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiate organization-defined transfer or reassignment actions within twenty-four (24) hours; c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notify access control personnel responsible for the system within twenty-four (24) hours.	Netskope's suite of security solutions, including CASB, NG-SWG, DLP, and ZTNA Next, all support role-based access control (RBAC) to enforce organizational access management policies based on the principle of least privilege. These tools help ensure that users have the minimal level of access necessary, enhancing security and compliance across the organization.	• CASB • NG-SWG • DLP • Private Access
PS-6	a. Develop and document access agreements for organizational systems; b. Review and update the access agreements at least annually; and c. Verify that individuals requiring access to organizational information and systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or at least annually and any time there is a change to the user's level of access.	Netskope's products do not map to this requirement.	
PS-7	a. Establish personnel security requirements, including security roles and responsibilities for external providers; b. Require external providers to comply with personnel security policies and procedures established by the organization; c. Document personnel security requirements;	Netskope's CASB and NG-SWG assist with asset acquisition and third-party risk management by inventorying all managed and unmanaged apps and cloud services in the organization's IT ecosystem. Netskope's Cloud Confidence Index (CCI) scores SaaS applications to help organizations evaluate the risk of using various vendors' applications or cloud services. The assessment criteria encompass the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, among other factors.	• CASB • NG-SWG • Cloud Confidence Index (CCI)

Control	Requirements(s)	Netskope Response	Products
	d. Require external providers to notify access control personnel responsible for the system and/or facilities, as appropriate of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges immediately for terminations; within twenty-four (24) hours for transfers; and e. Monitor provider compliance with personnel security requirements.		
PS-8	a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and b. Notify the ISSO and/or similar role within the organization within twenty-four (24) hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.	Netskope's Next Gen 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 applications. It decodes and logs over 100 inline activities, establishing a baseline of user behavior to detect anomalies. NG-SWG applies granular, context-aware policies in response to risky behavior, such as requiring additional authentication or suggesting safer alternatives. It generates customizable reports and alerts for incident response and assists in non-repudiation assertions. The Standard User and Entity Behavior Analytics (UEBA) module establishes baselines of normal user behavior and detects deviations using sequential rules, adjusting user access and privileges accordingly. The Advanced UEBA module enhances this with multiple machine learning models and introduces the User Confidence Index (UCI), a dynamic risk score used to adapt policies and recommend security training for mitigating insider threats. UCI data can also be shared via Netskope's Cloud Risk Exchange to enhance threat detection across platforms.	• CASB • NG-SWG • UEBA • Advanced UEBA
PS-9	Incorporate security and privacy roles and responsibilities into organizational position descriptions.	Netskope's products do not map to this requirement.	

RISK ASSESSMENT

Control	Requirements(s)	Netskope Response	Products
RA-1	a. Develop, document, and disseminate to organization-defined personnel or roles: 1. Organization-level; mission/ business process-level; system-level risk assessment policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and c. Review and update the current risk assessment: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes.	Netskope enforces organizational policies by using pop-up banners and coaching pages to notify employees of potential policy infringements. It scores SaaS applications with its Cloud Confidence Index (CCI) to help organizations assess risks, considering factors such as security policies, certifications, audits, and privacy concerns. Netskope's CASB aids in asset inventory, acquisition strategy, third-party risk management, and business continuity by identifying and assessing managed and unmanaged apps based on their usage and risk levels. Netskope's Advanced Analytics maps data flows across web and cloud services, categorizing data by sensitivity and assessing cloud risks. The product dashboard allows administrators to track security trends, including the number of apps accessed, threats detected, policies triggered, and users impacted.	• CASB • NG-SWG • Public Cloud Security • Cloud Confidence Index (CCI) • Advanced Analytics
RA-2	a. Categorize the system and information it processes, stores, and transmits; b. Document the security categorization results, including supporting rationale, in the security plan for the system; and c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.	Netskope products offer controls to identify and protect information assets, including assets across web and cloud applications, cloud infrastructure, on-premises servers, and endpoint devices. These controls can be used to create an inventory of information assets across managed and unmanaged devices using DLP discovery controls. Netskope products are able to characterize SaaS, IaaS, and web usage across an entire enterprise including remote access connections to on-premises apps and services. This includes the monitoring of non-corporate devices accessing corporate SaaS applications and users accessing non-corporate SaaS applications from IT-managed devices. IT and Security teams are able to map communication and data flows to an exceptional degree of accuracy.	• CASB • NG-SWG • Public Cloud • Security • Private Access • DLP • Device • Intelligence

Control	Requirements(s)	Netskope Response	Products
		Netskope will not only map where data is flowing, including for company and personal app instances, but also provide the necessary controls to contain data flows when unmanaged devices are being used and unmanaged services are being adopted by end-users.	
RA-3	a. Conduct a risk assessment, including: 1. Identifying threats to and vulnerabilities in the system; 2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and 3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information; b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments; c. Document risk assessment results in a security assessment report; d. Review risk assessment results at least annually and whenever a significant change occurs; e. Disseminate risk assessment results to organization-defined personnel or roles; and f. Update the risk assessment annually or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system. **RA-3 Additional FedRAMP Requirements and Guidance:** **Guidance:** Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F. **(e) Requirement:** Include all Authorizing Officials; for JAB authorizations to include FedRAMP.	Netskope's Cloud Security solutions, including its Cloud Confidence Index (CCI), help organizations assess and manage the risk of using various SaaS applications and cloud services by evaluating security policies, certifications, and more. Netskope's Cloud Access Security Broker (CASB) aids in asset inventory, acquisition strategy, third-party risk management, and business continuity by identifying apps and cloud services, assessing their criticality. Advanced User and Entity Behavior Analytics (UEBA) uses ML-based anomaly detection models to assign a dynamic risk score to users, aiding in insider threat detection and mitigation. Meanwhile, Advanced Analytics maps data flows and assesses cloud risk, providing insight via a comprehensive dashboard. Standard Threat Protection defends against known and new malware, phishing, and web threats, integrating with Netskope's other security tools to form a comprehensive, layered defense.	• CASB • NG-SWG • Public Cloud Security • Cloud Confidence Index (CCI) • RBI • Advanced Analytics • Advanced UEBA • Threat Protection

Control	Requirements(s)	Netskope Response	Products
	RA-3(1): (a) Assess supply chain risks associated with organization-defined systems, system components, and system services; and (b) Update the supply chain risk assessment at an organization-defined frequency, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in supply chain.		
RA-5	a. Monitor and scan for vulnerabilities in the system and hosted applications monthly for operating system/infrastructure; monthly for web applications (including APIs) and databases and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyze vulnerability scan reports and results from vulnerability monitoring; d. Remediate legitimate vulnerabilities; high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate-risk vulnerabilities mitigated within ninety (90) days from date of discovery; low risk vulnerabilities mitigated within one hundred and eighty (180) days from date of discovery in accordance with an organizational assessment of risk;	Netskope's Cloud Threat Exchange is a tool for near real-time threat ingestion, curation, and sharing. It enables Netskope customers and partners to bidirectionally share indicators of compromise (IoCs) like malicious URLs and file hashes and can be configured to automatically share IoCs with an organization's SIEM tool. Netskope products can assist in identifying vulnerable OS and browsers for devices through NG-SWG and CASB including IoT, OT, and traditional devices through Device Intelligence. Advanced Analytics maps data flows and assesses cloud risk by cataloguing cloud app usage. Its dashboard tracks security trends, including the number of apps accessed, threats detected, and policies triggered. This comprehensive approach ensures organizations maintain robust cloud security and compliance. Netskope's Private Access offers secure remote access to on-premises or cloud-hosted private applications from any device, anywhere. It integrates with NIST-compliant third-party identity providers for secure authentication and uses end-to-end encryption to protect data during use and transmission. Private Access applies granular access controls based on zero trust principles and logs all access attempts, enabling the enforcement of organizational policies regarding failed login attempts. Netskope products provide a User Confidence Index (UCI) and behavior-based analytics on user activities, which can help organizations identify internal threats including detecting data bulk uploads, downloads, and deletions, plus proximity, failed logins, shared credentials, rare events, risky countries, and data exfiltration between company and personal SaaS instances. Netskope Advanced Threat Protection can detect external malware/ransomware from web and cloud services and can analyze to block in real time. Netskope provides detailed analysis of the malware type, which can help organizations understand the types of threats and threat actors impacting their organization. Netskope's Cloud Log Shipper can send event and alert logs to the organization's SIEM or SOAR tool, and the Cloud Ticket Orchestrator can generate service tickets and automate workflows to facilitate response and remediation.	• NG-SWG • CASB • Private Access • Public Cloud Security • CTE • CLS • CTO • Device Intelligence • Advanced Analytics • Advanced UEBA • Advanced Threat Protection • Cloud Exchange • Threat Protection

Control	Requirements(s)	Netskope Response	Products
	e. Share information obtained from the vulnerability monitoring process and control assessments with organization-defined personnel or roles to help eliminate similar vulnerabilities in other systems; and f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned. **RA-5 Additional FedRAMP Requirements and Guidance:** **Guidance:** See the FedRAMP Documents page > Vulnerability Scanning Requirements https://www.FedRAMP.gov/documents/ **Guidance**: Informational findings from a scanner are detailed as a returned result that holds no vulnerability risk or severity, and for FedRAMP, does not require an entry onto the POA&M or entry onto the RET during any assessment phase. Warning findings, on the other hand, are given a risk rating (low, moderate, high, or critical) by the scanning solution and should be treated like any other finding with a risk or severity rating for tracking purposes onto either the POA&M or RET depending on when the findings originated (during assessments or during monthly continuous monitoring). If a warning is received during scanning, but further validation turns up no actual issue, then this item should be categorized as a false positive. If this situation presents itself during an assessment phase (initial assessment, annual assessment, or any SCR), follow guidance on how to report false positives in the Security Assessment Report (SAR). If this situation happens during monthly continuous monitoring, a deviation request will need to be submitted per the FedRAMP Vulnerability Deviation Request Form.		

Control	Requirements(s)	Netskope Response	Products
	Warnings are commonly associated with scanning solutions that also perform compliance scans, and if the scanner reports a "warning" as part of the compliance scanning of a CSO, follow guidance surrounding the tracking of compliance findings during either the assessment phases (initial assessment, annual assessment, or any SCR) or monthly continuous monitoring as it applies. Guidance on compliance scan findings can be found by searching on "Tracking of Compliance Scans" in FAQs. **(a) Requirement**: An accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually. **(d) Requirement**: If a vulnerability is listed among the CISA Known Exploited Vulnerability (KEV) Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog), the KEV remediation date supersedes the FedRAMP parameter requirement. **(e) Requirement**: To include all Authorizing Officials; for JAB authorizations to include FedRAMP.		
	RA-5(2): Update the system vulnerabilities to be scanned within twenty-four (24) hours prior to running scans.		
	RA-5(3): Define the breadth and depth of vulnerability scanning coverage.		
	RA-5(4): Determine information about the system that is discoverable and notify appropriate service provider personnel and follow procedures for organization and service provider-defined corrective actions.		
	RA-5(5): Implement privileged access authorization to all components that support authentication for all scans.		
	RA-5(8): Review historic audit logs to determine if a vulnerability identified in an organization-defined system has been previously exploited within an organization-defined time period.		

Control	Requirements(s)	Netskope Response	Products
	RA-5(8) Additional FedRAMP Requirement: **Requirement**: This enhancement is required for all high (or critical) vulnerability scan findings. RA-5(11): Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.		
RA-7	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	Netskope's Cloud Confidence Index (CCI) evaluates SaaS applications based on factors like security policies, certifications, audit capabilities, and legal/privacy concerns, helping organizations assess risks.	• CASB • NG-SWG • Public Cloud Security • Cloud Confidence Index (CCI) • CTO
RA-9	Identify critical system components and functions by performing a criticality analysis for organization-defined systems, system components, or system services at organization-defined decision points in the system development life cycle.	The Netskope platform allows the organization to identify and prioritize critical services based on the intensity of their usage by the organization including devices, web and cloud services, and remote access.	• All products

SYSTEM AND SERVICES ACQUISITION

Control	Requirements(s)	Netskope Response	Products
SA-1	a. Develop, document, and disseminate to organization-defined personnel or roles: 1. Organization-level; mission/ business process-level; system-level system and services acquisition policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	Netskope enforces organizational policies and notifies employees of potential infringements through pop-up banners/coaching pages. It evaluates SaaS applications using its Cloud Confidence Index (CCI), assessing vendor security policies, certifications, and risks. Netskope's Cloud Access Security Broker (CASB) manages asset inventory, acquisition strategy, third-party risk, and business continuity by identifying and assessing managed and unmanaged apps and cloud services. Advanced Analytics maps data flows and assesses cloud risk by cataloguing cloud app usage. Its dashboard tracks security trends, including the number of apps accessed, threats detected, and policies triggered. This comprehensive approach ensures organizations maintain robust cloud security and compliance.	• CASB • NG-SWG • Public Cloud Security • Cloud Confidence Index (CCI) • Advanced Analytics • CTO

Control	Requirements(s)	Netskope Response	Products
	2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and c. Review and update the current system and services acquisition: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes.		
SA-2	a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning; b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.	Netskope's products do not map to this requirement.	
SA-3	a. Acquire, develop, and manage the system using organization-defined system development life cycle that incorporates information security and privacy considerations; b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle; c. Identify individuals having information security and privacy roles and responsibilities; and d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.	Netskope's CASB and NG-SWG help manage assets, acquisition strategies, third-party risks, and business continuity by identifying and assessing managed and unmanaged apps and cloud services. Netskope Device Intelligence identifies, catalogs, and classifies all devices, both managed and unmanaged, that connect to an organization's network. Netskope's Cloud Confidence Index (CCI) evaluates SaaS applications based on critical criteria like security policies, certifications, audit capabilities, legal, and privacy concerns, aiding organizations in risk assessment.	• CASB • NG-SWG • CCI • Device Intelligence

Control	Requirements(s)	Netskope Response	Products
SA-4	Include the following requirements, descriptions, and criteria, explicitly or by reference, using standardized contract language; organization-defined contract language in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements; c. Security and privacy assurance requirements; d. Controls needed to satisfy the security and privacy requirements. e. Security and privacy documentation requirements; f. Requirements for protecting security and privacy documentation; g. Description of the system development environment and environment in which the system is intended to operate; h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and i. Acceptance criteria. **SA-4 Additional FedRAMP Requirements and Guidance:** **Guidance:** The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred. See https://www.niap-ccevs.org/Product/index.cfm or https://www.commoncriteriaportal.org/products/.	Netskope's CASB and NG-SWG help manage assets, acquisition strategies, third-party risks, and business continuity by identifying and assessing managed and unmanaged apps and cloud services. Netskope's Cloud Confidence Index (CCI) evaluates SaaS applications based on critical criteria like security policies, certifications, audit capabilities, legal, and privacy concerns, aiding organizations in risk assessment.	• CASB • NG-SWG • Public Cloud Security • Cloud Confidence Index (CCI)

Control	Requirements(s)	Netskope Response	Products
	Requirement: The service provider must comply with Federal Acquisition Regulation (FAR) Subpart 7.103, and Section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 (Pub. L. 115-232), and FAR Subpart 4.21, which implements Section 889 (as well as any added updates related to FISMA to address security concerns in the system acquisitions process).		
	SA-4(1): Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.	Netskope assesses the risk of SaaS applications and cloud services using its Cloud Confidence Index (CCI), which evaluates criteria like security policies, certifications, audit capabilities, and legal concerns. Its Cloud Access Security Broker (CASB) and Next Gen Secure Web Gateway (NG-SWG) utilize a data loss prevention (DLP) engine that safeguards data across web, cloud apps, and devices through machine learning and context-aware policies. This DLP system enforces role-based access and protects data in real time through actions like encryption or obfuscation. Netskope Device Intelligence identifies and classifies devices on the network, creates behavior baselines, detects anomalies, and applies zero trust principles for granular access control. It integrates with incident response tools to generate security alerts tailored to organizational criteria.	• CASB • NG-SWG • Cloud Confidence Index (CCI) • DLP • Device Intelligence
	SA-4(2): Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: at a minimum to include security-relevant external system interfaces; high-level design; low-level design; source code or network and data flow diagram; organization-defined design/ implementation information at an organization-defined level of detail.	Netskope's Cloud Confidence Index (CCI) rates SaaS applications on security, compliance, and privacy, helping organizations assess risks. Their Cloud Access Security Broker (CASB) and Next Generation Secure Web Gateway (NG-SWG) incorporate data loss prevention (DLP), utilizing machine learning to protect data across web, cloud, and endpoint devices in real time. DLP enforces role-based access, ensures backup integrity, and supports forensic investigations. Device Intelligence catalogs and classifies network devices, creating security baselines and detecting anomalies. It applies zero trust principles and integrates with incident response tools for security alerts. Overall, Netskope provides comprehensive data security and cloud posture management, ensuring compliance and mitigating risks across cloud services and devices.	• CASB • NG-SWG • Public Cloud Security • Cloud Confidence Index (CCI) • DLP • Device Intelligence
	SA-4(5): Require the developer of the system, system component, or system service to: (a) Use the DoD STIGs to establish configuration settings; Center for Internet Security up to Level 2 (CIS Level 2) guidelines shall be used if STIGs are not available; custom baselines shall be used if CIS is not available; and (b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.	Netskope's Device Intelligence identifies, catalogs, and classifies all devices, managed and unmanaged, connected to the organization's network. It segments devices to isolate risks and uses AI/ML to detect anomalous behavior by creating a baseline of normal operations. Device Intelligence also integrates with incident response tools to trigger security alerts based on predefined criteria, applying granular access and activity controls aligned with zero trust principles. This comprehensive approach ensures continuous protection and dynamic response to potential threats.	• NG-SWG • CASB • Public Cloud Security • Device Intelligence

Control	Requirements(s)	Netskope Response	Products
	SA-4(9): Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.	Netskope Device Intelligence identifies, catalogs, and classifies all devices, both managed and unmanaged, on an organization's network, grouping risky devices into isolated segments. Using AI/ML, it establishes normal device behavior, detects anomalies, and enforces granular access controls following zero trust principles. It integrates with incident response tools to generate security alerts based on organizational criteria.	• Device Intelligence
	SA-4(10): Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.	Netskope's CASB and NG-SWG, integrated with a robust data loss prevention (DLP) engine, offer comprehensive security for organizational data whether it's in use, in transit, or at rest across the web, cloud applications, and endpoint devices. Utilizing machine learning, Netskope's DLP identifies, classifies, and protects sensitive data according to organizational and regulatory requirements. Context-aware policies help protect data by considering users, devices, apps, networks, and actions, enabling real-time protection measures like data obfuscation, file encryption, or action blocking. Additionally, it supports role-based access during incident response and recovery, ensures backup integrity, and maintains log files in dedicated repositories for continuous monitoring and forensic investigations.	• CASB • NG-SWG • DLP
SA-5	a. Obtain or develop administrator documentation for the system, system component, or system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security and privacy functions and mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative or privileged functions; b. Obtain or develop user documentation for the system, system component, or system service that describes: 1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and 3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;	Netskope's NG-SWG integrates with third-party, NIST-compliant identity providers to extend single sign-on (SSO) and multi-factor authentication (MFA) across both managed and unmanaged web and cloud apps. It decodes and logs over 100 activities inline, creating a baseline of user behavior to detect anomalies and apply granular policy controls. These controls go beyond simple "allow" or "block" rules, responding to risky behaviors with actions like stepped-up MFA, policy violation notifications, or cybersecurity training referrals. Customizable reports and alerts can be integrated with an organization's SIEM to aid incident response, and detailed logs support non-repudiation of user actions. Netskope's CASB and CCI support asset acquisition and third-party risk management. CASB identifies all managed and unmanaged apps in the organization's IT ecosystem and categorizes them by risk and usage level. CCI assigns each app a risk-based score. Netskope Device Intelligence catalogs and classifies all devices on a network, grouping them into segments to isolate risky ones. Its AI/ML engine establishes normal device behavior baselines, detects anomalies, and enforces granular access controls based on zero trust principles. It integrates with incident response tools to generate alerts based on custom criteria, enhancing network security.	• NG-SWG • CASB • CCI • Device Intelligence

Control	Requirements(s)	Netskope Response	Products
	c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take organization-defined actions in response; and d. Distribute documentation to at a minimum, the ISSO (or similar role within the organization).		
SA-8	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: organization-defined systems security and privacy engineering principles.	The Netskope platform provides a significant amount of visibility to administrators while supporting privacy by design. Netskope products can be configured to secure activity to web, SaaS, IaaS, and egress traffic from on-network and remote users, but also secures app and cloud service activity to the extent that specific user actions (such as share, edit, delete, upload, download, etc.) within cloud apps are recorded. Netskope has the unique ability to decode inline unpublished API calls and JSON streams to secure user activity in real time across apps and cloud services, including by instance (i.e. company vs. personal). Threat protection and data protection (DLP) components are also used to identify activities that may be malicious such as intentionally downloading malicious code or attempting to exfiltrate data. In addition, configuration of public cloud and SaaS services can also be monitored to assist in identifying accidental or intentional misconfigurations. Cloud Exchange can be leveraged to extend and share activity data across an ecosystem of network and security tools.	• All products
SA-9	a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: Appropriate FedRAMP Security Controls Baseline(s) if Federal information is processed or stored within the external system; b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored.	Netskope's CASB helps with asset inventory, acquisition strategy, third-party risk management, and business continuity by identifying and assessing both managed and unmanaged apps and cloud services based on usage and risk. Netskope's NG-SWG integrates with NIST-compliant third-party identity providers, extending SSO/MFA to web and cloud apps. It can decode and log over 100 inline activities, baseline user behavior, and detect anomalies. It applies granular policy controls based on activity, data transmitted, or specific app instances. Beyond simple allow/block rules, it employs context-aware controls, such as stepped-up MFA for risky actions, notifying users of policy violations, suggesting safer alternatives, or referring users to cybersecurity training. NG-SWG can generate reports and alerts based on customizable thresholds, feeding into the organization's SIEM for incident response, and its detailed logging assists in asserting non-repudiation of user actions. Netskope's Cloud Confidence Index (CCI) evaluates SaaS applications to help organizations assess risks associated with using various vendors' applications or cloud services.	• CASB • NG-SWG • Public Cloud Security • CTO • Cloud Confidence Index (CCI) • Advanced Analytics • Device Intelligence • DLP

Control	Requirements(s)	Netskope Response	Products
		The assessment criteria include the vendor's security policies, certifications, audit capabilities, legal and privacy concerns, and other significant factors. Device Intelligence catalogs and classifies all devices on the network, using AI/ML to detect anomalies and apply access controls based on zero trust principles. It integrates with incident response tools for security alerts. Advanced Analytics maps data flows and assesses cloud risk, helping administrators track security trends and app usage through an intuitive dashboard. Netskope provides robust data loss prevention (DLP) through its CASB and NG-SWG solutions, safeguarding data across web, cloud applications, and endpoint devices. The DLP engine employs machine learning to classify and protect sensitive data, enforcing real-time, context-aware policies based on users, devices, and actions. These policies can obfuscate personal data, encrypt sensitive files, or block specific actions. It also supports role-based access during incident responses, maintains backup integrity, and facilitates monitoring and forensic investigations.	
	SA-9(1): (a) Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and (b) Verify that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles].		
	SA-9(2): Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: all external systems where Federal information is processed or stored.		
	SA-9(5): Restrict the location of information processing, information or data, AND system services to U.S./U.S. Territories or geographic locations where there is U.S. jurisdiction based on all high-impact data, systems, or services.		
SA-10	Require the developer of the system, system component, or system service to: a. Perform configuration management during system, component, or service development, implementation, AND operation; b. Document, manage, and control the integrity of changes to organization-defined configuration items under configuration management; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel.	Netskope Device Intelligence identifies and categorizes all devices, both managed and unmanaged, on an organization's network. It segments the network to isolate riskier devices. Using AI/ML, it establishes normal behavior patterns for each device, detects anomalies, and enforces granular access controls aligned with zero trust principles. Device Intelligence can also integrate with incident response tools to generate security alerts based on organizational criteria.	• NG-SWG • CASB • Public Cloud Security • Device Intelligence

Control	Requirements(s)	Netskope Response	Products
	SA-10 Additional FedRAMP Requirements and Guidance: **(e) Requirement**: Track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel, to include FedRAMP.		
SA-11	Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to: a. Develop and implement a plan for ongoing security and privacy assessments; b. Perform unit; integration; system; regression testing/evaluation at an organization-defined frequency at an organization-defined depth and coverage; c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during testing and evaluation.	Netskope's CASB can generate alerts and export them to an organization's security information and event management (SIEM) tool to enable automated incident response and recovery. Event logs help perform lessons learned and produce Progress and Action On Milestones reports. Netskope's Next Gen Secure Web Gateway (NG-SWG) integrates with NIST-compliant third-party identity providers, extending single sign-on (SSO) and multi-factor authentication (MFA) across web and cloud-based apps. The NG-SWG decodes and logs over 100 inline activities and establishes a user activity baseline to detect anomalies, applying granular policy controls based on activity, transmitted data, or app use. Beyond basic "allow" or "block" rules, the NG-SWG's context-aware controls manage risky behavior by requiring enhanced MFA, notifying users of policy violations, or suggesting safer alternatives. It can also provide just-in-time cybersecurity training via third-party vendors. The NG-SWG can generate customizable reports and alerts, feeding them into the organization's SIEM tool to aid incident response. Its detailed event logging ensures non-repudiation of user actions.	• CASB • NG-SWG
	SA-11(1): Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis. **SA-11(1) Additional FedRAMP Requirements:** **Requirement:** The service provider must document its methodology for reviewing newly developed code for the Service in its Continuous Monitoring Plan. If static code analysis cannot be performed (for example, when the source code is not available), then dynamic code analysis must be performed (see SA-11 (8)).	Netskope's products do not map to this requirement.	

Control	Requirements(s)	Netskope Response	Products
	SA-11(2): Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that: a. Uses the following contextual information: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels; b. Employs the following tools and methods: organization-defined tools and methods; c. Conducts the modeling and analyses at the following level of rigor: organization-defined breadth and depth of modeling and analyses; and d. Produces evidence that meets the following acceptance criteria: organization-defined acceptance criteria.		
SA-15	a. Require the developer of the system, system component, or system service to follow a documented development process that: 1. Explicitly addresses security and privacy requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Review the development process, standards, tools, tool options, and tool configurations before first use and annually thereafter to determine if the process, standards, tools, tool options, and tool configurations selected and employed can satisfy the following security and privacy requirements: FedRAMP Security Authorization requirements.	Netskope products can be used to apply controls and baseline assessments required for and by suppliers in line with security requirements. Netskope scores SaaS applications in its Cloud Confidence Index (CCI) and provides many important details that help organizations assess the risk of using each app or cloud service. Criteria include the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more. The visibility provided by the Netskope platform gives the organization a clearer picture of which apps are most critical to their day-to-day operations, as well as the risks of using any given app.	• NG-SWG • CASB • Public Cloud Security • CCI

Control	Requirements(s)	Netskope Response	Products
	SA-15(3): Require the developer of the system, system component, or system service to perform a criticality analysis: (a) At the following decision points in the system development life cycle: organization-defined decision points in the system development life cycle; and (b) At the following level of rigor: organization-defined breadth and depth of criticality analysis.		
SA-16	Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: organization-defined training.	Netskope does not map to this requirement.	
SA-17	Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that: a. Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture; b. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and c. Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.	Netskope does not map to this requirement.	
SA-21	Require that the developer of organization-defined system, system component, or system service: a. Has appropriate access authorizations as determined by assigned organization-defined official government duties; and b. Satisfies the following additional personnel screening criteria: organization-defined additional personnel screening criteria.	Netskope products can be used to manage access to apps and services used during SDLC, such as GitHub and Public Cloud. With instance awareness, services can also be managed to separate development, test, and production environments.	• NG-SWG • CASB • Public Cloud Security • Cloud Firewall • Private Access

Control	Requirements(s)	Netskope Response	Products
SA-22	a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or b. Provide the following options for alternative sources for continued support for unsupported components in-house support; organization-defined support from external providers.	Netskope products can assist in identifying vulnerable OS and browsers for devices through NG-SWG and CASB including IoT, OT, and traditional devices through Device Intelligence.	• NG-SWG • CASB • Public Cloud Security • Device Intelligence

SYSTEM AND COMMUNICATIONS PROTECTION

Control	Requirements(s)	Netskope Response	Products
SC-1	a. Develop, document, and disseminate to organization-defined personnel or roles: 1. Organization-level; mission/ business process-level; system-level system and communications protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and c. Review and update the current system and communications protection: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes.	Netskope provides comprehensive cybersecurity and data privacy solutions throughout the system life cycle, from specification to modification. It enforces organizational policies and facilitates policy communication via pop-up banners/coaching pages to notify employees of potential infringements. Netskope's Cloud Access Security Broker (CASB) aids in asset inventory, acquisition strategy, third-party risk management, and business continuity planning by identifying and assessing the criticality of cloud services and apps. Netskope's Advanced Analytics maps organizational data flows, categorizing data by sensitivity and assessing cloud app risks. Its dashboard tracks security trends, including apps accessed, threats detected, policies triggered, and users impacted.	• CASB • NG-SWG • Public Cloud Security • Advanced Analytics

Control	Requirements(s)	Netskope Response	Products
SC-2	Separate user functionality, including user interface services, from system management functionality.	Netskope's Private Access facilitates remote access to on-premises or cloud-hosted private apps from any device, integrating with NIST-compliant identity providers for secure authentication. It uses end-to-end encryption to protect data and applies granular controls to manage access and privileges based on zero trust principles.	• Private Access
SC-3	Isolate security functions from nonsecurity functions.	Netskope also offers role-based access control that supports role-based access based on an organization's RACI policy or similar requirements to support responsibilities and procedures in the event of a security incident. Multiple levels of access, including data obfuscation, can be used to protect incident data on a need-to-know basis.	• All products
SC-4	Prevent unauthorized and unintended information transfer via shared system resources.	Netskope's CASB and NG-SWG are equipped with a data loss prevention (DLP) engine that secures organizational data across the web, cloud applications, and endpoint devices. Utilizing machine learning, the DLP identifies and protects sensitive data based on organizational and regulatory requirements. Context-aware policies consider user, device, app, network, and action information to protect data in real time through methods like data obfuscation, file encryption, or blocking specific actions. The DLP enforces role-based access during incident response, ensures backup integrity, and holds log files for continuous monitoring and forensic investigations. SkopeAI enhances Netskope's DLP with deep contextual awareness, enabling it to protect unstructured data like images and efficiently detect multifaceted cyber threats such as polymorphic malware, novel phishing domains, zero-day threats, and malicious web content.	• CASB • NG-SWG • DLP • SkopeAI
SC-5	a. Protect against the effects of the following types of denial-of-service events: at a minimum: ICMP (ping) flood, SYN flood, slowloris, buffer overflow attack, and volume attack and; b. Employ the following controls to achieve the denial-of-service objective: organization-defined controls by type of denial-of-service event.	Netskope's Cloud Firewall protects against DDoS, man-in-the-middle, and DNS attacks by inspecting queries for harmful, newly registered, or algorithmically generated domains. Additionally, event logs from Netskope's Cloud Firewall can be integrated with an organization's SIEM tool to aid in incident response and recovery.	• Cloud Firewall
SC-7	a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces b. Implement subnetworks for publicly accessible system components that are physically; logically separated from internal organizational networks; and c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.	Netskope aids in the application of industry-recognized cybersecurity and data privacy practices throughout the life cycle of systems and services, including their specification, design, development, implementation, and modification Netskope's Cloud Firewall enforces security policies for all ports and protocols on egress traffic to web and cloud applications, eliminating the need to backhaul traffic to on-premises security stacks. It protects against DDoS, man-in-the-middle, and DNS attacks by inspecting queries for malicious domains. Event logs from the Cloud Firewall can be integrated with an organization's SIEM tool for enhanced incident response and recovery.	• Cloud Firewall • CASB • NG-SWG • DLP • SkopeAI • Private Access

Control	Requirements(s)	Netskope Response	Products
	SC-7 Additional FedRAMP Requirements and Guidance: **(b) Guidance**: SC-7 (b) should be met by subnet isolation. A subnetwork (subnet) is a physically or logically segmented section of a larger network defined at TCP/IP Layer 3, to both minimize traffic and, important for a FedRAMP Authorization, add a crucial layer of network isolation. Subnets are distinct from VLANs (Layer 2), security groups, and VPCs and are specifically required to satisfy SC-7 part b and other controls. See the FedRAMP Subnets White Paper (https://www.fedramp.gov/assets/resources/documents/FedRAMP_subnets_white_paper.pdf) for additional information.	Private Access offers remote access to private apps hosted on-premises or in the cloud from any device. It integrates with third-party identity providers for secure authentication, uses end-to-end encryption to protect data, and applies detailed access controls based on zero trust principles. Private Access also logs all access attempts and can enforce policies regarding failed login attempts. Netskope's Next Generation Secure Web Gateway (NG-SWG) integrates with NIST-compliant third-party identity providers to extend single sign-on (SSO) and multi-factor authentication (MFA) across both managed and unmanaged web and cloud apps. It can decode and log over 100 inline activities, establishing a user activity baseline to detect anomalies and apply granular policy controls based on activity nature, data being transmitted, or the app instance. Beyond basic "allow" or "block" rules, NG-SWG's context-aware controls can escalate MFA, notify users of policy violations, request business justifications, suggest safer alternatives, or refer users to third-party cybersecurity training. NG-SWG also generates customizable reports and alerts, feeding them into the organization's security information and event management (SIEM) tool for incident response, while its detailed event logging helps in non-repudiation of user actions. Netskope's CASB and NG-SWG, powered by its data loss prevention (DLP) engine, offer robust security for organizational data across various environments, including the web, cloud applications, and endpoint devices. The DLP utilizes machine learning to identify and classify sensitive data based on organizational and regulatory standards. Context-aware policies enable real-time protection by considering user, device, app, network, and action context. This includes actions such as obfuscating personal data, encrypting sensitive files, or blocking specific actions. Netskope's DLP also enforces role-based access, maintains backup integrity, and retains log files for continuous monitoring and forensic investigations. SkopeAI enhances the DLP engine by providing deep contextual awareness, which helps in identifying and protecting unstructured data like images. It also excels in rapidly detecting various security threats, including multivariate attacks, polymorphic malware, novel phishing domains, zero-day threats, and malicious web content.	
	SC-7(3): Limit the number of external network connections to the system.		
	SC-7(4): (a) Implement a managed interface for each external telecommunication service; (b) Establish a traffic flow policy for each managed interface; (c) Protect the confidentiality and integrity of the information being transmitted across each interface; (d) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;		

Control	Requirements(s)	Netskope Response	Products
	(e) Review exceptions to the traffic flow policy [FedRAMP Assignment: at least every ninety (90) days or whenever there is a change in the threat environment that warrants a review of the exceptions] and remove exceptions that are no longer supported by an explicit mission or business need; (f) Prevent unauthorized exchange of control plane traffic with external networks; (g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and (h) Filter unauthorized control plane traffic from external networks.		
	(g) SC-7(5): Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces; for any systems. **SC-7 (5) Additional FedRAMP Requirements and Guidance:** **Guidance**: For JAB Authorization, CSPs shall include details of this control in their Architecture Briefing		
	SC-7(7): Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using organization-defined safeguards.		
	SC-7(8): Route organization-defined internal communications traffic to any network outside of organizational control and any network outside the authorization boundary through authenticated proxy servers at managed interfaces.		
	SC-7(10): (a) Prevent the exfiltration of information; and (b) Conduct exfiltration tests [Assignment: organization-defined frequency].		

Control	Requirements(s)	Netskope Response	Products
	SC-7(12): Implement Host Intrusion Prevention System (HIPS), Host Intrusion Detection System (HIDS), or minimally a host-based firewall at organization-defined system components.		
	SC-7(18): Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.		
	SC-7(20): Provide the capability to dynamically isolate organization-defined system components from other system components.		
	SC-7(21): Employ boundary protection mechanisms to isolate organization-defined system components supporting organization- defined missions and/ or business functions.		
SC-8	Protect the confidentiality AND integrity of transmitted information. **SC-8 Additional FedRAMP Requirements and Guidance:** **Guidance:** For each instance of data in transit, confidentiality AND integrity should be through cryptography as specified in SC-8 (1), physical means as specified in SC-8 (5), or in combination. For clarity, this control applies to all data in transit. Examples include the following data flows: • Crossing the system boundary • Between compute instances - including containers • From a compute instance to storage • Replication between availability zones • Transmission of backups to storage • From a load balancer to a compute instance • Flows from management tools required for their work – e.g., log collection, scanning, etc.	Netskope's CASB and NG-SWG offer comprehensive data security using a robust data loss prevention (DLP) engine, which safeguards data across the web, cloud applications, and endpoints. The DLP uses machine learning to identify and protect sensitive data, applying context-aware policies based on user, device, app, and network information. This includes obfuscating personal data, encrypting sensitive files, and role-based access controls during incident response, ensuring backup integrity, and aiding forensic investigations. Netskope's NG-SWG integrates with NIST-compliant identity providers and extends SSO/MFA to web and cloud apps. It monitors over 100 inline activities, detects anomalies, and applies context-aware policies, such as requiring multi-factor authentication for risky behavior. It also notifies users of policy violations and provides alternatives or cybersecurity training. NG-SWG can generate reports and alerts for SIEM tools and facilitate incident response through detailed event logging. Netskope's Private Access enables secure remote access to private apps from any device, using end-to-end encryption and zero trust principles. It integrates with NIST-compliant identity providers for secure authentication, enforces policies on failed logins, and logs all access attempts, ensuring secure and controlled access.	• CASB • NG-SWG • DLP • Private Access

Control	Requirements(s)	Netskope Response	Products
	The following applies only when choosing SC-8 (5) in lieu of SC-8 (1). FedRAMP-Defined Assignment / Selection Parameters SC-8 (5)-1 [a hardened or alarmed carrier Protective Distribution System (PDS) when outside of Controlled Access Area (CAA)] SC-8 (5)-2 [prevent unauthorized disclosure of information AND detect changes to information] **Guidance**: SC-8 (5) applies when physical protection has been selected as the method to protect confidentiality and integrity. For physical protection, data in transit must be in either a Controlled Access Area (CAA), or a Hardened or alarmed PDS. hardened or alarmed PDS: Shall be as defined in SECTION X - CATEGORY 2 PDS INSTALLATION GUIDANCE of CNSSI No.7003, titled PROTECTED DISTRIBUTION SYSTEMS (PDS). Per the CNSSI No. 7003 Section VIII, PDS must originate and terminate in a Controlled Access Area (CAA). Controlled Access Area (CAA): Data will be considered physically protected, and in a CAA if it meets Section 2.3 of the DHS's Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. CSPs can meet Section 2.3 of the DHS's recommended practice by satisfactory implementation of the following controls: PE-2 (1), PE-2 (2), PE-3 (2), PE-3 (3), PE-6 (2), and PE-6 (3). Note: When selecting SC-8 (5), the above SC-8(5), and the above referenced PE controls must be added to the SSP. CNSSI No.7003 can be accessed here: https://www.dcsa.mil/Portals/91/documents/ctp/nao/CNSSI_7003_PDS_September_2015.pdf DHS		

Control	Requirements(s)	Netskope Response	Products
	Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies can be accessed here: https://us-cert.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_Defense_in_Depth_Strategies_S508C.pdf.		
	SC-8(1): Implement cryptographic mechanisms to prevent unauthorized disclosure of information AND detect changes to information during transmission. **SC-8 (1) Additional FedRAMP Requirements and Guidance:** **Guidance**: See M-22-09, including "Agencies encrypt all DNS requests and HTTP traffic within their environment." SC-8 (1) applies when encryption has been selected as the method to protect confidentiality and integrity. Otherwise refer to SC-8 (5). SC-8 (1) is strongly encouraged. **Guidance**: Note that this enhancement requires the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13.) **Guidance**: When leveraging encryption from the underlying IaaS/PaaS: While some IaaS/PaaS services provide encryption by default, many require encryption to be configured and enabled by the customer. The CSP has the responsibility to verify encryption is properly configured. **Requirement**: Please ensure SSP Section 10.3 Cryptographic Modules Implemented for Data At Rest (DAR) and Data In Transit (DIT) is fully populated for reference in this control.		
SC-10	Terminate the network connection associated with a communications session at the end of the session or after no longer than ten (10) minutes of inactivity for privileged sessions and no longer than fifteen (15) minutes of inactivity for user sessions.	Netskope's products do not map to this requirement.	

Control	Requirements(s)	Netskope Response	Products
SC-12	Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: In accordance with Federal requirements. **SC-12 Additional FedRAMP Requirements and Guidance:** **Guidance**: See references in NIST 800-53 documentation. **Guidance**: Must meet applicable Federal Cryptographic Requirements. See References Section of control. **Guidance**: Wildcard certificates may be used internally within the system, but are not permitted for external customer access to the system.	Netskope's products do not map to this requirement.	
	SC-12(1): Maintain availability of information in the event of the loss of cryptographic keys by users.		
SC-13	a. Determine the organization-defined cryptographic uses; and b. Implement the following types of cryptography required for each specified cryptographic use: FIPS-validated or NSA-approved cryptography. **SC-13 Additional FedRAMP Requirements and Guidance:** **Guidance**: This control applies to all use of cryptography. In addition to encryption, this includes functions such as hashing, random number generation, and key generation. Examples include the following: • Encryption of data • Decryption of data • Generation of one-time passwords (OTPs) for MFA • Protocols such as TLS, SSH, and HTTPS The requirement for FIPS 140 validation, as well as timelines for acceptance of FIPS 140-2, and 140-3 can be found at the NIST Cryptographic Module Validation Program (CMVP). https://csrc.nist.gov/projects/cryptographic-module-validation-program.	Netskope's products do not map to this requirement.	

Control	Requirements(s)	Netskope Response	Products
	Guidance: For NSA-approved cryptography, the National Information Assurance Partnership (NIAP) oversees a national program to evaluate Commercial IT Products for Use in National Security Systems. The NIAP Product Compliant List can be found at the following location: https://www.niap-ccevs.org/Product/index.cfm **Guidance**: When leveraging encryption from underlying IaaS/PaaS: While some IaaS/PaaS provide encryption by default, many require encryption to be configured, and enabled by the customer. The CSP has the responsibility to verify encryption is properly configured. • **Guidance**: Moving to non-FIPS CM or product is acceptable when: • FIPS validated version has a known vulnerability • Feature with vulnerability is in use • Non-FIPS version fixes the vulnerability • Non-FIPS version is submitted to NIST for FIPS validation • POA&M is added to track approval, and deployment when ready **Guidance**: At a minimum, this control applies to cryptography in use for the following controls: AU-9(3), CP-9(8), IA-2(6), IA-5(1), MP-5, SC-8(1), and SC-28(1).		
SC-15	a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: no exceptions for computing devices; and b. Provide an explicit indication of use to users physically present at the devices. **SC-15 Additional FedRAMP Requirements and Guidance::** **Requirement**: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.	Netskope Device Intelligence identifies and categorizes all devices, both managed and unmanaged, on an organization's network. It groups devices into segments to isolate high-risk ones. Using AI/ML, it establishes normal behavior patterns at the device level and detects anomalies, applying detailed access and activity controls based on zero trust principles. It can also integrate with incident response tools to generate security alerts according to the organization's predefined criteria.	• Device Intelligence

Control	Requirements(s)	Netskope Response	Products
SC-17	a. Issue public key certificates under an organization-defined certificate policy or obtain public key certificates from an approved service provider; and b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.	Netskope's products do not map to this requirement.	
SC-18	a. Define acceptable and unacceptable mobile code and mobile code technologies; and b. Authorize, monitor, and control the use of mobile code within the system.	Netskope Device Intelligence tracks, classifies, and segregates all managed and unmanaged devices on an organization's network. Using AI/ML, it establishes normal device behavior patterns and identifies anomalies, enabling precise access and activity controls based on zero trust principles. It can also integrate with incident response tools to trigger security alerts based on predefined criteria.	• Device Intelligence
SC-20	a. Provide additional data origin authentication and integrity verification of artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace. **SC-20 Additional FedRAMP Requirements and Guidance:** **Guidance**: SC-20 applies to use of external authoritative DNS to access a CSO from outside the boundary. **Guidance**: External authoritative DNS servers may be located outside an authorized environment. Positioning these servers inside an authorized boundary is encouraged. **Guidance**: CSPs are recommended to self-check DNSSEC configuration through one of many available analyzers such as Sandia National Labs (https://dnsviz.net).	Netskope's products do not map to this requirement.	

Control	Requirements(s)	Netskope Response	Products
	Requirement: Control Description should include how DNSSEC is implemented on authoritative DNS servers to supply valid responses to external DNSSEC requests. **Requirement**: Authoritative DNS servers must be geolocated in accordance with SA-9 (5).		
SC-21	Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. **SC-21 Additional FedRAMP Requirements and Guidance:** **Guidance**: Accepting an unsigned reply is acceptable. **Guidance**: SC-21 applies to use of internal recursive DNS to access a domain outside the boundary by a component inside the boundary. DNSSEC resolution to access a component inside the boundary is excluded. **Requirement**: Control description should include how DNSSEC is implemented on recursive DNS servers to make DNSSEC requests when resolving DNS requests from internal components to domains external to the CSO boundary. • If the reply is signed, and fails DNSSEC, do not use the reply • If the reply is unsigned: CSP chooses the policy to apply. **Requirement**: Internal recursive DNS servers must be located inside an authorized environment. It is typically within the boundary, or leveraged from an underlying IaaS/PaaS.	Netskope's products do not map to this requirement.	

Control	Requirements(s)	Netskope Response	Products
SC-22	Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.	Netskope's products do not map to this requirement.	
SC-23	Protect the authenticity of communications sessions.	Netskope's NG-SWG seamlessly integrates with NIST-compliant third-party identity providers, extending SSO/MFA to both managed and unmanaged apps. It monitors and logs over 100 inline activities, establishing a baseline to detect anomalies, and applies granular policies based on activity type or data transmitted. Beyond simple "allow" or "block" rules, its context-aware controls can enforce additional MFA or notify users of policy violations, suggesting safer alternatives or cybersecurity training. Configurable for reports and alerts, NG-SWG data can feed into an organization's SIEM tool to aid incident response and non-repudiation. Netskope's Private Access provides secure remote access to private apps, integrating with NIST-compliant third-party identity providers for authentication, offering end-to-end encryption, and applying zero trust principles to limit access and privileges. It logs access attempts and enforces organizational policies on failed logins, ensuring security for data in both use and motion.	• NG-SWG • Private Access
SC-24	Fail to an organization-defined known system state for the following failures on the indicated components while preserving organization-defined system state information in failure: list of organization-defined types of system failures on organization-defined system components.	Netskope's NewEdge private cloud network implements a high-availability cloud-based architecture allowing operations to continue in the event of a failure at any node including ability to both scale up and scale down on demand.	• All products
SC-28	Protect the confidentiality AND integrity of the following information at rest: organization-defined information at rest. **SC-28 Additional FedRAMP Requirements and Guidance:** **Guidance**: The organization supports the capability to use cryptographic mechanisms to protect information at rest. **Guidance**: When leveraging encryption from underlying IaaS/PaaS: While some IaaS/PaaS services provide encryption by default, many require encryption to be configured, and enabled by the customer. The CSP has the responsibility to verify encryption is properly configured. **Guidance**: Note that this enhancement requires the use of cryptography in accordance with SC-13.	Netskope's CASB and NG-SWG solutions, powered by the company's data loss prevention (DLP) engine, secure organizational data across the web, cloud applications, and endpoint devices. Utilizing machine learning, Netskope's DLP identifies, classifies, and protects sensitive data according to organizational and regulatory standards, applying real-time, context-aware policies. This can include obfuscating personal data, encrypting sensitive files, or blocking specific actions. The DLP also enforces role-based access during incident response, ensures backup integrity, and maintains log files for continuous monitoring and forensic investigations. Netskope's Device Intelligence identifies and classifies all devices on the network, segmenting risky devices to ensure zero trust principles. Its AI/ML engine establishes a baseline of normal device behavior, detects anomalies, and enforces granular access and activity controls. Device Intelligence integrates with incident response tools to generate security alerts based on predefined criteria.	• CASB • NG-SWG • DLP • Device Intelligence

Control	Requirements(s)	Netskope Response	Products
	SC-28(1): Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on all information system components storing Federal data or system data that must be protected at the High or Moderate impact levels: organization-defined information. **SC-28 (1) Additional FedRAMP Requirements and Guidance:** **Guidance**: Organizations should select a mode of protection that is targeted towards the relevant threat scenarios. Examples: A. Organizations may apply full disk encryption (FDE) to a mobile device where the primary threat is loss of the device while storage is locked. B. For a database application housing data for a single customer, encryption at the file system level would often provide more protection than FDE against the more likely threat of an intruder on the operating system accessing the storage. C. For a database application housing data for multiple customers, encryption with unique keys for each customer at the database record level may be more appropriate.		
SC-39	Maintain a separate execution domain for each executing system process.	Netskope's products do not map to this requirement.	
SC-45	Synchronize system clocks within and between systems and system components.	Netskope's products do not map to this requirement.	
	SC-45(1): (a) Compare the internal system clocks at least hourly with http://tf.nist.gov/tf-cgi/servers.cgi; and (b) Synchronize the internal system clocks to the authoritative time source when the time difference is greater than any difference. **SC-45(1) Additional FedRAMP Requirements and Guidance:**		

Control	Requirements(s)	Netskope Response	Products
	Guidance: Synchronization of system clocks improves the accuracy of log analysis. **Requirement**: The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server. **Requirement**: The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.		

SYSTEM AND INFORMATION INTEGRITY

Control	Requirements(s)	Netskope Response	Products
SI-1	a. Develop, document, and disseminate to organization-defined personnel or roles: 1. Organization-level; mission/ business process-level; system-level system and information integrity policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and x	Netskope aids organizations in implementing recognized cybersecurity and data privacy practices across system life cycles, enforcing organizational policies, and notifying employees of potential policy infringements through pop-up banners and coaching pages. Netskope's Cloud Access Security Broker (CASB) helps with asset inventory, acquisition strategy, third-party risk management, and business continuity planning by inventorying and assessing managed and unmanaged apps and cloud services' criticality. Netskope's Cloud Security Posture Management (CSPM) continuously monitors mission-critical IaaS platforms to prevent misconfigurations and safeguard against data exfiltration, integrating with Cloud Ticket Orchestrator for automated remediation. Netskope's SaaS Security Posture Management (SSPM) performs similar functions for SaaS, offering alerts with step-by-step remediation and integration with Cloud Ticket Orchestrator. Additionally, previously detected misconfigurations can be used to create new security rules. Netskope's Advanced Analytics maps and categorizes data flows across web and cloud services, assesses cloud risk, and tracks security trends, helping administrators manage security more effectively.	• CASB • NG-SWG • Public Cloud Security • Advanced Analytics

Control	Requirements(s)	Netskope Response	Products
	c. Review and update the current system and information integrity: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes.		
SI-2	a. Identify, report, and correct system flaws; b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Install security-relevant software and firmware updates within within thirty (30) days of release of updates; and d. Incorporate flaw remediation into the organizational configuration management process.	Netskope's Cloud Confidence Index (CCI) scores SaaS applications, helping organizations assess risk based on security policies, certifications, audit capabilities, and legal/privacy concerns. Netskope's Device Intelligence identifies and classifies all devices connecting to an organization's network, isolating risky ones into network segments. It uses AI/ML to establish normal device behavior, detect anomalies, and apply zero trust principles with granular controls. It also integrates with incident response tools to generate security alerts based on the organization's criteria.	• CASB • NG-SWG • Public Cloud Security • Cloud Confidence Index (CCI) • Device Intelligence
	SI-2(2): Determine if system components have applicable security-relevant software and firmware updates installed using organization-defined automated mechanisms at least monthly.		
	SI-2(3): (a) Measure the time between flaw identification and flaw remediation; and (b) Establish the following benchmarks for taking corrective actions: organization-defined benchmarks.		
SI-3	a. Implement signature based and non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;	Netskope's Cloud Confidence Index (CCI) evaluates SaaS applications based on vendor security, certifications, audit capabilities, legal and privacy concerns, among others. Netskope's Public Cloud Security, equipped with Advanced DLP, scans for hidden malware, enhancing security. The Remote Browser Isolation feature contains risky websites in a sandbox, safeguarding the network from malware. Private Access provides secure, encrypted remote access to private apps, supporting zero trust principles and logging access attempts.	• CASB • NG-SWG • Public Cloud Security • Cloud Confidence Index (CCI) • RBI • Private Access

Control	Requirements(s)	Netskope Response	Products
	c. Configure malicious code protection mechanisms to: 1. Perform periodic scans of the system at least weekly and real-time scans of files from external sources to include endpoints and network entry and exit points as the files are downloaded, opened, or executed in accordance with organizational policy; and 2. To include blocking and quarantining malicious code; and send alert to administrator or defined security personnel near real time in response to malicious code detection; and d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.	Advanced Threat Protection includes detailed malware detection techniques like deobfuscation and multi-stage sandboxing, whereas Standard Threat Protection covers known malware, phishing, and web filtering. Device Intelligence classifies and monitors devices, uses AI/ML to detect anomalies, and applies zero trust access controls. Netskope's integration of machine learning in SkopeAI enhances the DLP engine, allowing it to protect unstructured data and detect sophisticated threats, ensuring comprehensive security for varied organizational needs.	• Advanced DLP • Advanced Threat Protection • Device Intelligence • SkopeAI
SI-4	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: organization-defined monitoring objectives; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through the following techniques and methods: organization-defined techniques and methods; c. Invoke internal monitoring capabilities or deploy monitoring devices: 1. Strategically within the system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Analyze detected events and anomalies;	Netskope's Cloud Access Security Broker (CASB) monitors and logs activities in SaaS and IaaS services, applying real-time activity controls and data loss prevention measures, including requesting business justifications for risky actions and referring users for further training. The Next Gen Secure Web Gateway (NG-SWG) detects over 100 inline activities, establishing user behavior baselines to identify and mitigate risks using granular policies. It responds dynamically to risky behaviors by requiring multi-factor authentication or suggesting safer alternatives. The Cloud Firewall secures egress traffic, disrupts DNS attacks, and integrates with SIEM tools for incident response. Private Access facilitates secure remote access to private apps with zero trust principles and integrates with identity providers. And Cloud Ticket Orchestrator automates incident response workflows.	• CASB • NG-SWG • Public Cloud Security • Cloud Firewall • Private Access • CTO

Control	Requirements(s)	Netskope Response	Products
	e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; f. Obtain legal opinion regarding system monitoring activities; and g. Provide organization-defined system monitoring information to organization-defined personnel or roles as needed; organization-defined frequency. **SI-4 Additional FedRAMP Requirements and Guidance:** **Guidance**: See US-CERT Incident Response Reporting Guidelines.		
	SI-4(1): Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.	Netskope's User and Entity Behavior Analytics (UEBA) tracks user behaviors across various apps, establishes behavioral baselines, detects anomalies, and adjusts access based on risk. Standard Threat Protection safeguards against known malware and employs machine learning and sandboxing for real-time threat detection. Advanced Threat Protection enhances these capabilities with deobfuscation, file unpacking, and multi-stage sandboxing to counter new malware. Additionally, Netskope Threat Protection integrates with Cloud Threat Exchange and other security services, offering a comprehensive, layered defense strategy. Device Intelligence identifies and classifies devices on the network, creating behavioral baselines at the device level to spot anomalies and apply strict access controls in line with zero trust principles. This tool can also integrate with incident response systems to trigger security alerts.	• CASB • NG-SWG • UEBA • Advanced Threat Protection • Device Intelligence • Threat Protection
	SI-4(2): Employ automated tools and mechanisms to support near real-time analysis of events.	Netskope's Data loss prevention (DLP) can detect and prevent the sharing of passwords and other authenticators with unauthorized parties. Additionally, the Cloud Ticket Orchestrator lets organizations automate security workflows by creating rules that generate service tickets in response to security alerts. This tool can automate much of an organization's incident response and recovery, including enforcing role-based access controls for all involved teams and members.	• CASB • NG-SWG • Advanced DLP • CTO
	SI-4(4): (a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic; (b) Monitor inbound and outbound communications traffic continuously for organization-defined unusual or unauthorized activities or conditions.	Netskope's Next Generation Secure Web Gateway (NG-SWG) integrates with NIST-compliant third-party identity providers to extend SSO/MFA across various web and cloud apps. It decodes and logs over 100 activities, establishes user activity baselines to detect anomalies, and applies granular policy controls. NG-SWG's context-aware controls can respond to risky behaviors with enhanced multi-factor authentication, user notifications, policy violation alerts, requests for business justifications, or cybersecurity training referrals. It generates customizable reports and alerts for incident response, aiding in user action non-repudiation.	• NG-SWG • Advanced Threat Protection • Device Intelligence • Threat Protection • Cloud Firewall

Control	Requirements(s)	Netskope Response	Products
		Netskope's Standard Threat Protection safeguards against known malware, uses machine learning to detect new threats, and offers real-time phishing detection, sandboxing, and web filtering. It integrates with Netskope's threat intelligence feeds and security tools like Remote Browser Isolation, Cloud Firewall, and User and Entity Behavior Analytics for a comprehensive security solution. Advanced Threat Protection (ATP) includes deobfuscation, recursive file unpacking, and multi-stage sandboxing to combat emerging malware. Netskope's Device Intelligence identifies, catalogs, and classifies all network devices, isolating risky ones and using AI/ML to detect and manage anomalies according to zero trust principles. Device Intelligence integrates with incident response tools to generate security alerts. Netskope's Cloud Firewall applies organizational security policies to egress traffic to the web or cloud applications, for all ports and protocols, without the need to backhaul traffic to an on-premises security stack. Netskope's Cloud Firewall disrupts DDoS, man-in-the-middle, and other forms of DNS attacks by inspecting queries for malicious, newly registered, or algorithmically generated domains. Event logs generated by Netskope's Cloud Firewall can be integrated with the organization's SIEM tool to facilitate incident response and recovery.	
	SI-4(5): Alert organization-defined personnel or roles when the following system-generated indications of compromise or potential compromise occur: organization-defined compromise indicators. **SI-4 (5) Additional FedRAMP Requirements and Guidance:** **Guidance**: In accordance with the incident response plan.	Netskope Device Intelligence manages and classifies all devices connecting to an organization's network, grouping them to isolate risky ones. Using AI/ML, it establishes normal behavior baselines, detects anomalies, and enforces detailed access controls following zero trust principles. It can also integrate with incident response tools to trigger security alerts based on organizational criteria. Netskope's Advanced Analytics maps an organization's data flows across web and cloud services, characterizing data by category and sensitivity. Advanced Analytics also assesses cloud risk by cataloguing and characterizing cloud app usage, and the product dashboard allows administrators to track security trends by number of apps accessed, threats detected, policies triggered, and users impacted. Netskope's Cloud Log Shipper exports event and alert logs from Netskope's NG-SWG, CASB, Private Access, Cloud Firewall, and Cloud and SaaS Security Posture Management tools to the organization's SIEM or other incident response tool. Netskope's Cloud Ticket Orchestrator allows organizations to create rules that automatically generate service tickets and automate workflows in response to security alerts. Properly configured, Cloud Ticket Orchestrator can automate much of an organization's incident response and recovery plan, including enforcing role-based access controls for all teams and team members involved in incident response.	• NG-SWG • CASB • Device Intelligence • Advanced Analytics • CLS • CTO

Control	Requirements(s)	Netskope Response	Products
	SI-4(10): Make provisions so that organization-defined encrypted communications traffic is visible to organization-defined system monitoring tools and mechanisms. **SI-4 (10) Additional FedRAMP Requirements and Guidance:** **Requirement**: The service provider must support Agency requirements to comply with M-21-31 (https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf) and M-22-09 (https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf).	Netskope's Next Gen Secure Web Gateway (NG-SWG) integrates with NIST-compliant identity providers to extend single sign-on (SSO) and multi-factor authentication (MFA) across web and cloud apps. It decodes and logs over 100 inline activities, creating a baseline of user behavior to identify anomalies and apply detailed policy controls. These controls go beyond simple "allow" or "block" rules, addressing risky behavior by requiring additional authentication, notifying users of potential policy violations, suggesting safer alternatives, or directing them to cybersecurity training. NG-SWG generates customizable reports and alerts, which can be integrated into an organization's security information and event management (SIEM) tool for incident response. Its detailed event logging also supports non-repudiation of user actions.	• NG-SWG • UEBA
	SI-4(11): Analyze outbound communications traffic at the external interfaces to the system and selected organization-defined interior points within the system to discover anomalies.	Netskope's Cloud Access Security Broker (CASB) provides real-time monitoring and logging of activities across SaaS and IaaS services, enabling detailed control and data loss prevention by requiring business justifications or policy training actions. The Next Gen Secure Web Gateway (NG-SWG) integrates with third-party identity providers and extends SSO/MFA to both managed and unmanaged apps. It logs over 100 activities, detects anomalies using user activity baselines, and applies context-aware controls for risks, such as enhanced MFA or policy violations notifications. NG-SWG also facilitates incident responses by creating detailed logs and customizable alerts. Netskope's User and Entity Behavior Analytics (UEBA) tracks behavior across web and cloud apps, establishes normal activity baselines, and detects anomalies. Adaptive policy controls adjust access based on behavior riskiness. The Advanced UEBA uses additional machine learning models and assigns a dynamic User Confidence Index (UCI) score to each user for better risk assessment and insider threat mitigation, integrating this with the Netskope Cloud Risk Exchange for information sharing. Device Intelligence classifies all devices on a network and isolates risky ones. It uses AI/ML to set behavioral baselines, detect anomalies, and enforce zero trust principles. Cloud Ticket Orchestrator automates incident response by generating service tickets and workflows and is part of the Netskope Cloud Exchange included in all deployments.	• CASB • NG-SWG • UEBA • Advanced UEBA • Device Intelligence • CTO
	SI-4(12): Alert organization-defined personnel or roles using organization-defined automated mechanisms when the following indications of inappropriate or unusual activities with security or privacy implications occur: organization-defined activities that trigger alerts.	Netskope Device Intelligence identifies and categorizes all devices on the network, using AI/ML to establish normal behavior baselines, detect anomalies, and enforce granular access controls based on zero trust principles. It can also integrate with incident response tools for real-time security alerting.	• NG-SWG • CASB • Public Cloud Security • Device Intelligence • CTO

Control	Requirements(s)	Netskope Response	Products
		The Cloud Ticket Orchestrator automates incident response by generating service tickets and automating workflows based on security alerts, enforcing role-based access controls. It is a standard feature of Netskope's Cloud Exchange and streamlines an organization's incident response and recovery plans.	• NG-SWG • UEBA
	SI-4(14): Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.	Netskope Device Intelligence catalogs all managed and unmanaged devices on the network, isolates risky devices, and uses AI/ML to establish normal device behavior and detect anomalies. It applies granular controls to enforce zero trust principles, and integrates with incident response tools to trigger security alerts based on organizational criteria.	• Device Intelligence
	SI-4(16): Correlate information from monitoring tools and mechanisms employed throughout the system.	Netskope's Cloud Log Shipper exports logs from various Netskope tools to an organization's SIEM or incident response systems. The Cloud Risk Exchange component ingests and normalizes risk scores for users, devices, and applications from third-party vendors like Crowdstrike, KnowBe4, and ServiceNow, and implements adaptive controls based on organizational policies to mitigate risks. Cloud Threat Exchange enables near real-time sharing and curation of threat indicators, such as malicious URLs and file hashes, among Netskope customers and partners.	• Cloud Exchange
	SI-4(18): Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: organization-defined interior points within the system.	Netskope offers comprehensive data security through its CASB and NG-SWG, bolstered by a data loss prevention (DLP) engine that safeguards organizational data across the web, cloud apps, and endpoints. Using machine learning, Netskope's DLP identifies, classifies, and protects sensitive data per regulatory and organizational requirements with real-time policies that respond to user behavior and device context. This includes actions like obfuscating personal data, encrypting files, and blocking risky actions. Netskope's Cloud Firewall applies organizational security policies to egress traffic to the web or cloud applications, for all ports and protocols, without the need to backhaul traffic to an on-premises security stack. Netskope's Cloud Firewall disrupts DDoS, man-in-the-middle, and other forms of DNS attacks by inspecting queries for malicious, newly registered, or algorithmically generated domains. Event logs generated by Netskope's Cloud Firewall can be integrated with the organization's SIEM tool to facilitate incident response and recovery. Netskope's Public Cloud Security can include Advanced DLP, which enhances standard DLP by scanning IaaS Storage for hidden malware, further securing the cloud environment. SkopeAI, leveraging machine learning, enhances Netskope's DLP by providing deep contextual awareness to protect unstructured data like images and detects advanced threats, polymorphic malware, novel phishing domains, zero-day threats, and malicious content efficiently.	• CASB • NG-SWG • Cloud Firewall • Public Cloud Security • DLP • Advanced DLP • CTO • SkopeAI

Control	Requirements(s)	Netskope Response	Products
	SI-4(19): Implement organization-defined additional monitoring of individuals who have been identified by organization-defined sources as posing an increased level of risk.	Netskope products can enforce additional controls for personnel who are deemed to be high-risk users, for example those who may be leaving an organization. This could include adding a user to a more restrictive set of controls when their risk profile increases.	• NG-SWG • CASB • Advanced UEBA
	SI-4(20): Implement the following additional monitoring of privileged users: organization-defined additional monitoring.	Netskope's solutions, including CASB, NG-SWG, DLP, and ZTNA Next, support the implementation of role-based access control (RBAC) to align with the principle of least privilege for effective organizational access management. Netskope's Advanced User and Entity Behavior Analytics (UEBA) employs advanced machine learning models to detect anomalies. It includes the User Confidence Index (UCI), a risk score based on user behavior, which helps adapt policies, controls, and recommend security training to mitigate insider threats. The UCI can also integrate with Netskope's Cloud Exchange to share insider threat information across platforms	• NG-SWG • CASB • Private Access • Advanced UEBA • Cloud Exchange
	SI-4(22): (a) Detect network services that have not been authorized or approved by organization-defined authorization or approval processes; and (b) Audit; Alert organization-defined personnel or roles when detected.	Netskope's CASB can identify and classify all managed and unmanaged apps and cloud services in use in the organization's IT ecosystem. Policies can be crafted to block the use of unsanctioned apps, and event and alert logs can be exported to the organization's SIEM or SOAR tool using Netskope's Cloud Log Shipper. Netskope's Cloud Ticket Orchestrator can generate service tickets and automate workflows. Netskope's Advanced Analytics maps data flows across the organization, giving admins further visibility into the volume of usage of unsanctioned apps and services.	• CASB • CLS • CTO • Advanced Analytics
	SI-4(23): Implement the following host-based monitoring mechanisms at organization-defined system components: organization-defined host-based monitoring mechanisms.	The Netskope platform can assist monitoring for adverse events across the ecosystem of networks, public cloud, SaaS, and devices.	• All products
SI-5	a. Receive system security alerts, advisories, and directives from US-CERT and Cybersecurity and Infrastructure Security Agency (CISA) Directives on an ongoing basis; b. Generate internal security alerts, advisories, and directives as deemed necessary; c. Disseminate security alerts, advisories, and directives to include system security personnel and administrators with configuration/ patch-management responsibilities; organization-defined elements within the organization; organization-defined external organizations; and d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.	Netskope's Private Access offers secure remote access to private applications hosted on-premises or in the cloud from any device, anywhere. It integrates with NIST-compliant identity providers for secure authentication, uses end-to-end encryption, and applies zero trust principles to manage access and privileges. Private Access also logs all access attempts and enforces policies on failed logins. Netskope's Cloud Risk Exchange gathers risk scores for users, devices, and apps from third-party vendors like Crowdstrike and ServiceNow. It normalizes these scores based on policies and risk tolerance, applying adaptive controls to mitigate risks associated with high-risk entities. Netskope's Cloud Threat Exchange facilitates near real-time threat sharing among Netskope customers and partners, allowing for the exchange of malicious indicators like URLs and file hashes. It can automatically share these indicators with an organization's SIEM tool.	• Private Access • CRE • CTE

Control	Requirements(s)	Netskope Response	Products
	SI-5 Additional FedRAMP Requirements and Guidance: **Requirement**: Service Providers must address the CISA Emergency and Binding Operational Directives applicable to their cloud service offering per FedRAMP guidance. This includes listing the applicable directives and stating compliance status.		
	SI-5(1): Broadcast security alert and advisory information throughout the organization using organization-defined automated mechanisms.	Activity logs and alerts can be exported to other platforms (such as SIEM and SOAR platforms) with the Cloud Log Shipper tool or used to automatically create service tickets with Netskope's Cloud Ticket Orchestrator (CTO) tool. Proxy transaction events can be streamed to cloud storage or SIEMs in near real time.	• Cloud Exchange
SI-6	a. Verify the correct operation of organization-defined security and privacy functions; b. Perform the verification of the functions specified in SI-6a system transitional states to include upon system startup and/or restart; upon command by user with appropriate privilege; at least monthly; c. Alert system administrators and security personnel to failed security and privacy verification tests; and d. Shut the system down; restart the system; alternative actions(s) when anomalies are discovered.	For specialized roles, such as system administrators, Netskope also provides support for alerting on misconfigurations and vulnerabilities with recommendations on how to remediate.	• NG-SWG • CASB • Public Cloud Security
SI-7	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: organization-defined software, firmware, and information; and b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: organization-defined actions.	Netskope's Private Access provides secure remote access to on-premises or cloud-hosted private apps from any device, leveraging third-party identity providers for authentication, using end-to-end encryption, and applying zero trust principles. Private Access logs access attempts and enforces policies on failed logins. Netskope Device Intelligence identifies and categorizes both managed and unmanaged devices connecting to a network. It groups devices into segments to isolate risky ones and uses AI/ML to establish normal behavior, detect anomalies, and enforce detailed access controls based on zero trust principles. Additionally, it can integrate with incident response tools to generate security alerts based on organizational criteria.	• Public Cloud Security • Private Access • CTO • Device Intelligence
	SI-7(1): Perform an integrity check of organization-defined software, firmware, and information at startup; at security relevant events; at least monthly.		

Control	Requirements(s)	Netskope Response	Products
	SI-7(2): Employ automated tools that provide notification to the ISSO and/or similar role within the organization upon discovering discrepancies during integrity verification.		
	SI-7(5): Automatically shut the system down; restart the system; implement organization-defined controls when integrity violations are discovered.		
	SI-7(7): Incorporate the detection of the following unauthorized changes into the organizational incident response capability: organization-defined security-relevant changes to the system.		
	SI-7(15): Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: all software and firmware inside the boundary.		
SI-8	a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures. **SI-8 Additional FedRAMP Requirements and Guidance:** **Guidance**: When CSO sends email on behalf of the government as part of the business offering, Control Description should include implementation of Domain-based Message Authentication, Reporting & Conformance (DMARC) on the sending domain for outgoing messages as described in DHS Binding Operational Directive (BOD) 18-01. https://cyber.dhs.gov/bod/18-01/. **Guidance**: CSPs should confirm DMARC configuration (where appropriate) to ensure that policy=reject and the rua parameter includes reports@dmarc.cyber.dhs.gov. DMARC compliance should be documented in the SI-08 control implementation solution description, and list the FROM: domain(s) that will be seen by email recipients.	Netskope's Public Cloud Security, enhanced with Advanced DLP, scans IaaS Storage for hidden malware to protect the cloud environment. Advanced Threat Protection builds on Standard Threat Protection by adding de-obfuscation, recursive file unpacking, and multi-stage sandboxing to detect new malware. Standard Threat Protection safeguards against known malware, uses machine learning to detect new threats, and offers real-time phishing detection, corroborative sandboxing, and web filtering. It also integrates with Cloud Threat Exchange and other Netskope security tools like Remote Browser Isolation, Cloud Firewall, and User and Entity Behavior Analytics for a layered security approach. SkopeAI enhances the DLP engine's ability to understand and protect unstructured data, including images, and quickly detects various threats, including polymorphic malware, new phishing domains, zero-day threats, and malicious web content.	• NG-SWG • CASB • Public Cloud Security • Advanced DLP • Advanced Threat Protection • Threat Protection • SkopeAI • RBI

Control	Requirements(s)	Netskope Response	Products
	SI-8(2): Automatically update spam protection mechanisms organization-defined frequency.		
SI-10	Check the validity of the following information inputs: organization-defined information inputs to the system. **SI-10 Additional FedRAMP Requirements and Guidance:** **Requirement**: Validate all information inputs and document any exceptions.	Netskope's Private Access offers secure remote access to on-premises or cloud-hosted private applications from any device and location. It integrates with NIST-compliant third-party identity providers for secure authentication and employs end-to-end encryption to safeguard data both in use and in transit. Utilizing zero trust principles, Private Access applies granular controls to limit access and privileges. Additionally, it logs all access attempts and enforces organizational policies regarding failed login attempts for enhanced security.	• Private Access
SI-11	a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and b. Reveal error messages only to the ISSO and/or similar role within the organization.	Netskope's products do not map to this requirement.	
SI-12	Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements.	Netskope's CASB (Cloud Access Security Broker) and NG-SWG (Next Gen Secure Web Gateway) leverage a robust data loss prevention (DLP) engine to secure organizational data across web, cloud applications, and endpoint devices. The DLP uses machine learning for the identification, classification, and protection of sensitive data as per organizational and regulatory requirements. Real-time protection is offered through context-aware policies that consider users, devices, apps, networks, and actions, enabling actions like data obfuscation, encryption, or blocking. The DLP also manages role-based access during incidents, ensures backup integrity, and maintains log files for continuous monitoring and forensic investigations.	• CASB • NG-SWG • Public Cloud Security • DLP
SI-16	Implement the following controls to protect the system memory from unauthorized code execution: organization-defined controls.	Netskope's products do not map to this requirement.	

SUPPLY CHAIN RISK MANAGEMENT

Control	Requirements(s)	Netskope Response	Products
SR-1	a. Develop, document, and disseminate to chief privacy and ISSO and/or similar role or designees: 1. Organization-level; mission/ business process-level; system-level supply chain risk management policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and c. Review and update the current supply chain risk management: 1. Policy at least annually and following organization-defined events; and 2. Procedures at least annually and following significant changes.	Netskope's product suite includes a number of products that can assist with asset acquisition and supply chain risk management. For example, Netskope's NG-SWG and CASB can identify managed and unmanaged apps in the organization's IT ecosystem, and its Cloud Confidence Index scores apps and cloud services by risk level. Meanwhile, Advanced Analytics maps data flows across the organization's network, helping to identify mission-critical apps and cloud services. Finally, Cloud Security Posture Management and SaaS Security Posture Management detect and remediate misconfigured access controls in those mission-critical IT assets.	• All products
SR-2	a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services organization-defined systems, system components, or system services.	Netskope's Cloud Confidence Index (CCI) rates SaaS applications based on criteria like security policies, certifications, audit capabilities, and legal/privacy concerns, helping organizations assess vendor risk. Netskope's CASB and NG-SWG aid in asset inventory, acquisition strategy, third-party risk management, and business continuity planning by identifying and evaluating managed and unmanaged apps and cloud services, based on usage and risk.	• CASB • NG-SWG • Cloud Confidence Index (CCI) • Advanced Analytics • Device Intelligence

Control	Requirements(s)	Netskope Response	Products
	a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services organization-defined systems, system components, or system services b. Review and update the supply chain risk management plan at least annually or as required to address threat, organizational, or environmental changes; and c. Protect the supply chain risk management plan from unauthorized disclosure and modification. SR-2(1): Establish a supply chain risk management team consisting of organization- defined personnel, roles, and responsibilities to lead and support the following SCRM activities: organization-defined supply chain risk management activities.	Netskope Device Intelligence tracks and categorizes all devices on a network, isolating risky ones and using AI/ML to establish normal behavior baselines, detect anomalies, and enforce zero trust-based access and activity controls. It integrates with incident response tools to generate security alerts. Netskope's Advanced Analytics monitors data flows across web and cloud services, categorizing data by type and sensitivity, and assessing cloud risk by app usage. Its product dashboard helps administrators track security trends, such as the number of accessed apps, detected threats, triggered policies, and impacted users.	
SR-3	a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of organization-defined system or system component in coordination with organization-defined supply chain personnel; b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: organization-defined supply chain controls; and c. Document the selected and implemented supply chain processes and controls in security and privacy plans; supply chain risk management plan; organization-defined document. **SR-3 Additional FedRAMP Requirements and Guidance:** **Requirement**: CSOs must document and maintain the supply chain custody, including replacement devices, to ensure the integrity of the devices before being introduced to the boundary.	Netskope's Cloud Confidence Index (CCI) scores SaaS applications by evaluating vendor security policies, certifications, audit capabilities, and legal/privacy concerns, helping organizations assess application risks. Netskope Device Intelligence catalogs both managed and unmanaged devices on a network, segregating risky ones into isolated segments. It uses AI/ML to establish normal device behavior and detect anomalies, applying zero trust access controls. This intelligence integrates with incident response tools for customizable security alerts. Cloud Risk Exchange aggregates risk scores from third-party vendors like Crowdstrike and ServiceNow, normalizes them according to organizational policies, and enforces adaptive controls to mitigate risks from users, apps, and devices.	• CASB • NG-SWG • Cloud Confidence Index (CCI) • Device Intelligence • CRE

Control	Requirements(s)	Netskope Response	Products
SR-5	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: organization-defined acquisition strategies, contract tools, and procurement methods.	Netskope products discover cloud apps, including unmanaged apps, in use in the enterprise and can categorize them by usage and risk score. This gives the organization a clearer picture of which apps are most critical to their day-to-day operations, as well as the risks of using any given app.	• NG-SWG • CASB • CCI
SR-6	Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide at least annually. **SR-6 Additional FedRAMP Requirements and Guidance:** **Requirement**: CSOs must ensure that their supply chain vendors build and test their systems in alignment with NIST SP 800-171 or a commensurate security and compliance framework. CSOs must ensure that vendors are compliant with physical facility access and logical access controls to supplied products.	Netskope evaluates SaaS applications using its Cloud Confidence Index (CCI), considering security policies, certifications, audit capabilities, legal, and privacy concerns to help organizations assess risks.	• CASB • NG-SWG • Public Cloud Security • Cloud Confidence Index (CCI) • CTO
SR-8	Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises and results of assessment or audits. **SR-8 Additional FedRAMP Requirements and Guidance:** **Requirement**: CSOs must ensure and document how they receive notifications from their supply chain vendor of newly discovered vulnerabilities including zero-day vulnerabilities.	Netskope products can be used to apply controls and baseline assessments required for and by suppliers in line with security requirements. Netskope CASB and Public Cloud Security can audit web and cloud applications and provide metadata to understand if suppliers are using underlying cloud infrastructure to support supply chain discovery. Netskope also offers reverse proxy capabilities to protect cloud applications along with Netskope's Zero Trust Network Access (Private Access) to manage suppliers' access to organizational assets	• CASB • Private Access • Public Cloud Security
SR-9	Implement a tamper protection program for the system, system component, or system service. **SR-9 Additional FedRAMP Requirements and Guidance:** **Requirement**: CSOs must ensure vendors provide authenticity of software and patches supplied to the service provider including documenting the safeguards in place.	Netskope Data loss prevention tool helps ensure that only approved public updates related to incident recovery are released, using machine learning to accurately and reliably identify, classify, and protect sensitive and critical data across an organization.	• NG-SWG • DLP

Control	Requirements(s)	Netskope Response	Products
	SR-9(1): Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.	Netskope products can be used to manage access to apps and services used during SDLC, such as GitHub and Public Cloud. With instance awareness, services can also be managed to separate development, test, and production environments.	• NG-SWG • CASB • Public Cloud Security • Private Access • Cloud Firewall
SR-10	Inspect the following systems or system components at random; at organization-defined frequency, upon organization-defined indications of need for inspection to detect tampering: organization-defined systems or system components.	Netskope's products do not map to this requirement.	
SR-11	a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and b. Report counterfeit system components to source of counterfeit component; organization-defined external reporting organizations; organization-defined personnel or roles. **SR-11 Additional FedRAMP Requirements and Guidance:** **Requirement**: CSOs must ensure that their supply chain vendors provide authenticity of software and patches and the vendor must have a plan to protect the development pipeline.	Netskope's products do not map to this requirement.	
	SR-11(1): Train organization-defined personnel or roles to detect counterfeit system components (including hardware, software, and firmware).		
	SR-11(2): Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: all.		

Control	Requirements(s)	Netskope Response	Products
SR-12	Dispose of organization-defined data, documentation, tools, or system components using the following techniques and methods: organization-defined techniques and methods.	Netskope's products do not map to this requirement.	

Netskope, a leader in modern security and networking, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for people, devices, and data anywhere they go. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications—providing security and accelerating performance without trade-offs. Visit netskope.com.