netskope

Compliance Series

Family Educational Rights and Privacy Act (FERPA)

Using the Netskope Platform to Assist with FERPA Compliance

TABLE OF CONTENTS

INTRODUCTION

The Family Educational Rights and Privacy Act (FERPA) prohibits the unauthorized disclosure of students' educational records by any educational institution that receives funds administered by the U.S. Secretary of Education. While neither the law nor its accompanying regulations specify any particular security controls for safeguarding educational records, the Department of Education (ED) has furnished educational institutions with guidance - in the form of a Data Governance Checklist and a Data Security Checklist -that do specify recommended controls.

HOW TO USE THIS GUIDE

The Netskope platform consists of a suite of tools integrated into a unified Secure Access Service Edge architecture. The tables below break down the Data Security Checklist and Data Governance Checklist,mapping each recommended control to the appropriate Netskope product(s).

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

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

DATA GOVERNANCE CHECKLIST

Category	Control	Netskope controls	Products
Decision-making authority	Establish an organizational structure with different levels of data governance,and specify roles and responsibilities at various levels.	Netskope can enforce customizable, configurable, and automated cyber security and data privacy policies based on an organization's risk and regulatory requirements.	• All products
	Identify data stewards responsible for coordinating data governance activities and assign each to a specific domain of activity.	Netskope's CASB and NG-SWG can inventory cloud apps and services in use in the organization's IT ecosystem, facilitating the identification of data stewards. Netskope's Advanced Analytics maps data flows across web and cloud services, categorizing data by type and sensitivity. It assesses cloud risk by analyzing cloud app usage and provides a dashboard for administrators to monitor security trends. This includes tracking the number of accessed apps, detected threats, triggered policies, and impacted users.	• CASB • NG-SWG • Advanced Analytics
	Clearly define and communicate data stewards' roles, responsibilities, and accountability for data decision making, management, and security.	Netskope's Advanced Analytics maps and categorizes an organization's data flows across web and cloud services by sensitivity and category. It also evaluates cloud risk by cataloging and characterizing cloud app usage. The product dashboard enables administrators to monitor security trends, including the number of apps accessed, threats detected, policies triggered, and users impacted.	• CASB • NG-SWG • Advanced Analytics
	Give data stewards the authority to quickly and efficiently correct data problems while still ensuring that their access to personally identifiable information (PII) is minimized.	Netskope's security solutions, including CASB and NG-SWG, utilize a Data Loss Prevention (DLP) engine to secure data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying and protecting sensitive data according to organizational and regulatory standards, applying context-aware policies to manage data in real time. This includes obfuscating personal data, encrypting files, or blocking specific actions, while enforcing role-based access and maintaining backup integrity. Netskope's Cloud Security Posture Management (CSPM) monitors IaaS platforms to prevent misconfigurations and data exfiltration, aligning usage with organizational policies and regulatory standards. It continuously scans cloud storage buckets, sends alerts, and automates remediation via the Cloud Ticket Orchestrator. Similarly, the SaaS Security Posture Management (SSPM) ensures appropriate use of SaaS functions, detects misconfigurations, provides remediation steps, and integrates with the Cloud Ticket Orchestrator for enhanced automation and security improvements. Additionally, ZTNA Next offers secure remote access to both on-premises and cloud-hosted private applications. It integrates with NIST-compliant identity providers, uses end to- end encryption, and applies zero trust principles to control access and privileges, logging all access attempts and enforcing policies on login failures.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • ZTNA Next • CTO

Category	Control	Netskope controls	Products
Standard policies and procedures	Identify policy priorities affecting key data governance rules, and secure agreement on priorities from key stakeholders.	Netskope helps ensure compliance with organizational policies by communicating and tracking acknowledgement of policies across its products. Netskope's CASB inventories managed and unmanaged apps and cloud services in the organization's IT ecosystem, and characterizes them by usage and risk. The Cloud Confidence Index provides a risk-based score to apps and cloud services, helping the organization identify gaps between the organization's data governance requirements and the policies or capabilities of key third parties.	• All products • CASB • CCI
	Clearly define and document standard policies and procedures about all aspects of data governance and the data management life cycle, including collection, maintenance, usage, and dissemination.	Netskope's CASB and NG-SWG, powered by its Data Loss Prevention (DLP) engine, offer robust security for data across the web, cloud apps, and endpoint devices. Utilizing machine learning, Netskope's DLP identifies, classifies, and protects sensitive data according to organizational and regulatory standards. With real-time, context-aware policies, it can obfuscate personal data, encrypt sensitive files, or block specific actions to safeguard data. It also enforces role-based data access during incident response, ensures backup integrity, and retains log files for continuous monitoring and forensic investigations. Netskope's Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations and ensure compliance with organizational policies and regulatory standards. It scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for automated alerting and remediation. Similarly, Netskope's SaaS Security Posture Management (SSPM) monitors SaaS functions to prevent misconfigurations and ensure consistent data use. SSPM provides step-by-step remediation instructions and integrates with the Cloud Ticket Orchestrator for automated responses. Detected misconfigurations can be converted into new rules to enhance security.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO
	Put in place policies and procedures to ensure that all data are collected, managed, stored, transmitted, used, reported, and destroyed in a way that preserves privacy and ensures confidentiality and security.	Netskope allows organizations to enforce customized cyber security and data privacy policies. These policies can be tailored, configured, and automated according to the company's risk and regulatory requirements.	• All products
	Conduct an assessment to ensure the long-term sustainability of the proposed or established data governance policies and procedures, including adequate staffing, tools, technologies, and resources..	The Netskope platform can assist organizations in defining the scope of security tests and exercises, and maximizing their effectiveness. Advanced Analytics maps data flows throughout the organisation's network, highlighting threats detected, policies triggered, and users affected. And Netskope's CASB inventories all unmanaged apps and devices within the ICT environment, categorising them by usage and risk level.	• CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • Advanced Analytics • CTO

Category	Control	Netskope controls	Products
		Together, these tools give the organisation a deeper understanding of the scope of the attack surface and potential critical points of failure. Netskope's Cloud Security Posture Management and SaaS Security Posture Management continuously monitor for misconfigurations in critical IaaS and SaaS services, and can integrate with Netskope's Cloud Ticket Orchestrator to facilitate automated remediation of misconfigured access controls.	
	Maintain a written plan outlining processes for monitoring compliance with established policies and procedures.	Netskope's Cloud Security Posture Management (CSPM) ensures the security of IaaS platforms by continuously monitoring for misconfigurations and compliance deviations. It scans cloud storage to prevent data exfiltration and integrates with the Cloud Ticket Orchestrator to send alerts and automate remediation. Additionally, Netskope's SaaS Security Posture Management (SSPM) monitors SaaS functions for misconfigurations and compliance issues, offering step-by-step remediation guidance. SSPM can also generate service tickets and automate fixes through the Cloud Ticket Orchestrator, converting previous misconfigurations into new security rules. Netskope's Advanced Analytics tracks data flows across web and cloud services, assessing cloud risk and categorizing data by sensitivity. Administrators can monitor security trends and risk metrics through the Advanced Analytics dashboard.	• CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • Advanced Analytics • CTO
	Document and communicate data governance policies and procedures in an open and accessible way to all stakeholders, including staff, data providers, and the public.	Netskope enforces organizational policies and aids in communication and acknowledgment of these policies through pop-up banners and coaching pages. These notifications alert employees of potential policy infringements in accordance with organizational requirements.	• All products
Data inventories	Maintain a current inventory of all computer equipment, software, and data files.	Netskope's CASB and NG-SWG help with asset inventory, acquisition strategy, third-party risk management, and business continuity by identifying and assessing both managed and unmanaged apps and cloud services in an organization's IT ecosystem, evaluating their criticality based on usage and risk.	• CASB • NG-SWG
	Maintain a detailed, up-to-date inventory of all data elements that should be classified as sensitive, PII, or both.	Netskope's CASB and NG-SWG help with asset inventory, acquisition strategy, third-party risk management, and business continuity planning by identifying and cataloging managed and unmanaged apps and cloud services within an organization's IT ecosystem. It assesses these assets' criticality based on their usage and risk levels.	• CASB • NG-SWG
	Classify data records according to risk level for disclosure of PII.	Netskope's CASB and NG-SWG leverage a Data Loss Prevention (DLP) engine to provide comprehensive data security across the web, cloud applications, and endpoint devices.	• CASB • NG-SWG

Category	Control	Netskope controls	Products
		The DLP engine employs machine learning for identifying, classifying, and protecting sensitive data based on organizational and regulatory requirements. Context-aware policies protect data in real-time by actions such as obfuscating personal data, encrypting files, and blocking actions. The DLP also enforces role-based access, ensures backup integrity, and maintains log files for continuous monitoring and investigations. Netskope's Cloud Security Posture Management (CSPM) monitors IaaS platforms to prevent misconfigurations and ensure compliance with organizational, regulatory, and industry standards. CSPM scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for alerts and automated remediation. Similarly, Netskope's SaaS Security Posture Management (SSPM) continuously monitors SaaS functions to prevent misconfigurations, ensuring proper use of assets and data. SSPM provides remediation instructions, integrates with Cloud Ticket Orchestrator for service tickets and automated remediation, and converts detected misconfigurations into new security rules. Both CSPM and SSPM aim to maintain the intended use of organizational data and assets, enhancing overall security posture.	• Public Cloud Security • CSPM • DLP • SSPM • CTO
	Maintain a written policy regarding data inventories outlining what should be included in an inventory and how, when, how often, and by whom it should be updated.	Netskope enables organizations to enforce customizable and automated cyber security and data privacy policies tailored to their specific risk and regulatory needs.	• All products
Data content management	Maintain a clearly documented set of policy, operational, and research needs that justify the collection of specific data elements.	Netskope does not map to this requirement.	
	Regularly review and revise data content management policies to assure that only those data necessary for meeting the documented needs are collected and/or maintained.	Netskope's Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations and ensure compliance with organizational and regulatory standards. It also scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator to automate alerts and remediation efforts. Similarly, Netskope's SaaS Security Posture Management (SSPM) monitors SaaS functions for misconfigurations, providing alerts with remediation instructions, and can also automate remediation through the Cloud Ticket Orchestrator. Detected misconfigurations can be used to formulate new security rules. Netskope's Advanced Analytics maps data flows across web and cloud services, categorizes data by sensitivity, and assesses cloud risks by cataloging cloud app usage. Its dashboard tracks security trends, showing metrics like apps accessed, threats detected, policies triggered, and users impacted..	• CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • Advanced Analytics • CTO

Category	Control	Netskope controls	Products
Standard policies and procedures	Put in place mechanisms to de-identify PII whenever possible.	Netskope's CASB and NG-SWG feature a comprehensive Data Loss Prevention (DLP) engine that secures organizational data across the web, cloud apps, and endpoint devices in use, in transit, or at rest. This DLP leverages machine learning to identify and protect sensitive data according to organizational or regulatory needs. It uses context-aware policies that consider user, device, app, network, and action information to provide real-time data protection, such as obfuscating personal data, encrypting files, or blocking actions. Additionally, it supports role-based data 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
	Establish and communicate policies and procedures for handling records throughout all stages of the data lifecycle, including acquiring, maintaining, using, and archiving or destroying data.	Netskope enforces organizational policies and aids communication through pop-up banners and coaching pages. Beyond simple "allow" or "block" rules, Netskope's NG-SWG and CASB can notify employees about potential policy violations, suggest safer alternatives, and refer users to third party vendors for cyber security training. Using machine learning, Netskope's DLP identifies and protects sensitive data, employing context-aware policies to manage user actions in real-time, ensuring data security and compliance. It facilitates role-based access, ensures backup integrity, and supports continuous monitoring and forensic investigations. Netskope's Cloud Security Posture Management (CSPM) continuously monitors and prevents misconfigurations in IaaS platforms, ensuring compliance with access policies and standards. CSPM scans cloud storage to prevent data exfiltration and integrates with Cloud Ticket Orchestrator for automated remediation. Similarly, Netskope's SaaS Security Posture Management (SSPM) monitors critical SaaS functions, preventing misconfigurations and ensuring proper data use. SSPM provides remediation instructions and integrates with Cloud Ticket Orchestrator for alert-based automation. It also converts past misconfigurations into new security rules, enhancing organizational security.	• All products • CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CTO
Data quality	Maintain policies and procedures to ensure that data are accurate, complete, timely, and relevant to stakeholder needs.	Netskope's CASB (Cloud Access Security Broker) and NG-SWG (Next-Gen Secure Web Gateway) integrate a robust Data Loss Prevention (DLP) engine designed to secure organizational data across web, cloud applications, and endpoint devices. This DLP employs machine learning to identify and protect sensitive data in line with organizational and regulatory standards. Context-aware policies use information about users, devices, apps, networks, and actions to provide realtime data protection, such as data obfuscation, file encryption, and action blocking. Additionally, Netskope's DLP enforces role-based access during incident responses, ensures backup integrity, and maintains log files for continuous monitoring and forensic investigations.	• CASB • NG-SWG • DLP

Category	Control	Netskope controls	Products
	Conduct regular data quality audits to ensure strategies for enforcing quality control are up-to date and that any corrective measures undertaken in the past have been successful in improving data quality..	The Netskope platform assists organizations in optimizing security tests and exercises. It does so by defining the scope of these activities through comprehensive inventorying of all unmanaged apps and devices within an ICT environment and assigning them risk-based scores.	• All products
Data access	Maintain policies and procedures to restrict and monitor staff data access, limiting what data can be accessed by whom, including assigning differentiated levels of access based on job descriptions and responsibilities.	Netskope offers comprehensive cyber security and data privacy management, customizable to organizational and regulatory requirements. Netskope's Cloud Access Security Broker (CASB) and Next- Gen Secure Web Gateway (NG-SWG) monitor activity in SaaS and IaaS services, applying real-time controls like data loss prevention (DLP), business justifications, and training. Netskope's DLP engine secures data across various environments, using machine learning for sensitive data protection and context-aware policies for real-time intervention, including data obfuscation and encryption. The Advanced DLP scans IaaS storage for hidden malware. Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) continuously monitor mission-critical platforms and prevent misconfigurations. CSPM integrates with the Cloud Ticket Orchestrator to automate remediation, and SSPM converts past misconfigurations into new security rules. NG-SWG and ZTNA Next integrate with NIST-compliant identity providers and use multi-factor authentication for granular policy controls. They can respond to risky behavior with escalated authentication and provide comprehensive event logging for incident response. Advanced User and Entity Behavior Analytics (UEBA) with a User Confidence Index helps detect insider threats by adapting policies and recommending training. Advanced Analytics maps data flows, assesses cloud risk, and provides a dashboard for tracking security trends.	• All products • CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • ZTNA Next • Advanced Analytics • Advanced DLP • Advanced UEBA • CTO
	Establish internal procedural controls to manage user data access, including security screenings, training, and confidentiality agreements for staff with PII access privileges.	Netskope's CASB (Cloud Access Security Broker) monitors and logs activities in SaaS and IaaS services, detailing user, device, instance, and actions. It applies real-time, activity-level controls and data loss prevention (DLP), not just blocking actions but also requiring business justifications for risky actions or providing organization policy training. Netskope's NG-SWG (Next-Generation Secure Web Gateway) integrates with NIST-compliant third-party identity providers to extend SSO (Single Sign-On) and MFA (Multi-Factor Authentication) across web and cloud apps. It logs over 100 inline activities and establishes user activity baselines to detect anomalies, applying specific policy controls based on activity nature, transmitted data, or app instances. It employs context-aware controls beyond simple "allow" or "block" rules, such as requiring enhanced MFA, policy violation notifications, business justifications, suggesting safer alternatives, or directing users to cyber security training.	• CASB • NG-SWG

Category	Control	Netskope controls	Products
		NGSWG can also generate customizable reports and alerts for integration into SIEM tools for incident response, and its detailed logging aids in asserting non-repudiation of user actions.	
	Maintain policies and procedures to restrict and monitor staff data access, limiting what data can be accessed by whom, including assigning differentiated levels of access based on job descriptions and responsibilities. Maintain policies and procedures to restrict and monitor data access of authorized users to ensure the conditions of their access to data in the system are consistent with those outlined in the data governance plan, including which data elements can be accessed, for what period of time, and under what conditions.	Netskope's suite of cyber security solutions enforce organization-defined policies for cyber security and data privacy, customizable to meet various risk and regulatory requirements. Netskope's Next-Generation Secure Web Gateway (NG-SWG) integrates with NIST-compliant identity providers to extend SSO/MFA across web and cloud apps, and enhances security with anomaly detection and context-aware controls. Netskope's Cloud Access Security Broker (CASB) monitors user activities in SaaS and IaaS services, applying real-time data loss prevention (DLP) controls and context-aware policies. The DLP engine uses machine learning to classify and protect sensitive data across web, cloud applications, and endpoints, enforcing role-based access, ensuring backup integrity, and facilitating continuous monitoring and forensic investigations. Netskope's Cloud Security Posture Management prevents IaaS and SaaS misconfigurations, ensuring compliance with organizational and regulatory standards, and integrates with Cloud Ticket Orchestrator for automated remediation. Advanced DLP in Netskope's Public Cloud Security scans IaaS storage for hidden malware, while Role-Based Access Control enforces the least privilege principle. Advanced User Entity and Behavior Analytics detect insider threats with ML-based anomaly models and User Confidence Index scores. And Advanced Analytics maps data flows and assesses cloud risks, providing comprehensive security visibility through a detailed dashboard.	• All products • CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • ZTNA Next • Advanced Analytics • Advanced DLP • Advanced UEBA • CTO
Data security and risk management	Develop a comprehensive security framework, including administrative, physical, and technical procedures for addressing data security issues.	Netskope enables the enforcement of an organization's cyber security and data privacy policies. These policies can be tailored, configured, and automated according to specific risk and regulatory requirements.	• All products
	Undertake a risk assessment, including an evaluation of the risks and vulnerabilities related to both intentional misuse of data by malicious individuals and inadvertent disclosure by authorized users..	Netskope's Cloud Access Security Broker (CASB) helps with asset inventory, acquisition strategy, risk management, and business continuity by identifying and assessing managed and unmanaged apps and cloud services within an organization, and its Cloud Confidence Index (CCI) scores cloud apps and services based on security, certifications, audit capabilities, legal and privacy concerns. Cloud Security Posture Management (CSPM) monitors IaaS platforms to prevent misconfigurations, secure data usage, and integrate with Cloud Ticket Orchestrator for automated remediation. Similarly, Netskope's SaaS Security Posture Management (SSPM) continuously monitors SaaS functions to prevent and remediate misconfigurations. It can also convert detected misconfigurations into new security rules.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • RBI • SSPM • Advanced Analytics • Advanced UEBA

Category	Control	Netskope controls	Products
		Remote Browser Isolation is a built-in feature of the NG-SWG that uses a secure container to protect networks from malware on risky websites. And Standard Threat Protection guards against known and new malware, phishing, and integrates with other security tools. Advanced User and Entity Behavior Analytics (UEBA) uses machine learning to detect anomalies, provide user risk scores, and inform security policies and training. Device Intelligence identifies all devices on a network, detects anomalies, and applies zero-trust principles, while Advanced Analytics maps and categorizes data flows, and assesses cloud risk. Lastly, Cloud Risk Exchange normalizes risk scores across users, devices, and apps, enforcing adaptive controls to mitigate risks.	• Device Intelligence • Threat Protection • CRE • CTO
	Put in place a plan to mitigate risks associated with intentional and inadvertent data breaches.	Netskope's Cloud Confidence Index (CCI) evaluates SaaS applications based on various criteria, such as security policies, certifications, audit capabilities, and legal/privacy concerns, helping organizations assess the risk of using cloud services. Netskope's CASB and NG-SWG use a robust Data Loss Prevention (DLP) engine, leveraging machine learning to protect sensitive data across platforms by enforcing real-time, context-aware policies. The DLP supports role-based access, backup integrity, and continuous monitoring for forensic investigations. Netskope's Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms to prevent misconfigurations and ensure compliance with regulations, scanning cloud storage buckets to prevent data exfiltration. CSPM integrates with Cloud Ticket Orchestrator for automated remediation. Similarly, the SaaS Security Posture Management (SSPM) oversees SaaS functions to avoid misconfigurations, generating alert-based service tickets and automating remediation. Remote Browser Isolation contains risky websites in secure containers to prevent malware infections, while Advanced User Entity and Behavior Analytics (UEBA) uses machine learning models to detect anomalies, providing a dynamic User Confidence Index (UCI) for adaptive policies and insider threat mitigation. Netskope's Standard Threat Protection offers a multi-layered defense against malware and phishing by integrating threat intelligence and automation with other security services.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • DLP • RBI • SSPM • Advanced UEBA • Threat Protection • CTO
	Regularly monitor and audit data security.	Netskope's Cloud Security Posture Management (CSPM) continuously monitors critical IaaS platforms for misconfigurations and adheres to organizational and regulatory standards. CSPM also scans cloud storage to prevent data exfiltration, integrates with Cloud Ticket Orchestrator for alerts and auto-remediation. Netskope's SaaS Security Posture Management (SSPM) performs similar functions for SaaS assets, providing remediation steps and generating service tickets via Cloud Ticket Orchestrator. Netskope's Cloud Firewall applies security policies to egress traffic, mitigating DNS attacks and supporting integration with SIEM tools.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Firewall • SSPM • Advanced Analytics

Category	Control	Netskope controls	Products
		Advanced Analytics tracks data flows and assesses cloud risk, while Cloud Risk Exchange standardizes risk scores from third-party vendors, enforcing adaptive controls. Cloud Threat Exchange facilitates near real-time threat sharing among customers and partners.	• CRE • CTE • CTO
	Establish policies and procedures to ensure the continuity of data services in an event of a data breach, loss, or other disaster.	Netskope evaluates SaaS applications with its Cloud Confidence Index (CCI), offering vital details to help organizations assess the risk of using various vendors' applications or cloud services. The assessment criteria include the vendor's security policies, certifications, audit capabilities, and considerations regarding legal and privacy concerns. Netskope's Borderless SD-WAN allows organizations to extend their network perimeter to any user on any device, anywhere. With Netskope's Borderless SD-WAN, traffic is steered through Netskope's global New Edge network, allowing high-availability connectivity to web and cloud applications, and enforcement of uniform policy controls with continuous adaptive trust based on context-specific criteria such as user, location, device, app instance, and more.	• CASB • NG-SWG • Cloud Confidence Index (CCI)
	Maintain policies to guide decisions about data exchanges and reporting, including sharing data with educational institutions, researchers, policy makers, parents, and third party contractors.	Netskope's Cloud Access Security Broker (CASB) and Next-Gen Secure Web Gateway (NG-SWG) provide comprehensive monitoring, logging, and activity-level controls for SaaS and IaaS services, including user, device, and action information. CASB enforces real-time data loss prevention and policy training. NG-SWG integrates with NIST-compliant identity providers, extending SSO/MFA across web and cloud apps. It decodes numerous activities, establishes user baselines, and applies context-aware policy controls to detect anomalies and risky behaviors, triggering actions like multi-factor authentication, policy notifications, or training. NG-SWG generates customizable reports and alerts that support incident response and non-repudiation. Advanced User Entity and Behavior Analytics (UEBA) employs numerous ML models to detect anomalies, offering a dynamic User Confidence Index (UCI) to score user risk, adaptable for policy adjustments and security training. This integrates with Netskope's Cloud Exchange to share insider threat intel. Cloud Risk Exchange assimilates risk scores from third-party sources, normalizes them, and enforces adaptive controls to mitigate high-risk users, apps, and devices. Cloud Threat Exchange shares real-time threat intel like malicious URLs and file hashes with Netskope customers and partners, aiding in proactive threat management. Both exchanges are included in all Netskope deployments.	• CASB • NG-SWG • Advanced UEBA • CRE • CTE
	When sharing data, put in place appropriate procedures to ensure that any PII remains strictly confidential and protected from unauthorized disclosure.	Netskope's Cloud Access Security Broker (CASB) monitors and logs SaaS and IaaS activities, including user, device, instance, and action details. It can apply real-time activity-level and data loss prevention controls, such as blocking actions, requesting business justifications for risky actions, or providing policy training.	• CASB • NG-SWG • Advanced UEBA • DLP

Category	Control	Netskope controls	Products
		Netskope's Next-Generation 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 logs over 100 inline activities and uses user behavior baselines to detect anomalies, applying granular policies. NG-SWG can respond to risky behaviors with stricter MFA, notifications, business justification requests, safer alternatives, or just-in-time cyber security training, and reports and alerts can be integrated with SIEM tools. 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. Advanced User Entity and Behavior Analytics (UEBA) uses multiple ML-based anomaly-detection models and includes a User Confidence Index (UCI) that assigns a risk score to users based on their behavior over time. UCI helps adapt policies, recommend security training, and detect insider threats, and can share insider threat information through Netskope's Cloud Exchange..	
	Implement appropriate procedures, such as rounding and cell suppression, to ensure that PII is not inadvertently disclosed in public aggregate reports and that the organization's data reporting practices remain in compliance with applicable local, state, and federal privacy laws and regulations.	Netskope's Cloud Access Security Broker (CASB) and Next-Generation Secure Web Gateway (NG-SWG) incorporate a robust Data Loss Prevention (DLP) engine that secures organizational data across the web, cloud applications, and endpoint devices. Leveraging machine learning, the DLP engine identifies and protects sensitive data according to organizational or regulatory criteria. It applies context-aware policies based on user, device, app, network, and action data to protect information in real-time by obfuscating, encrypting, or blocking actions as necessary. This DLP functionality also enforces role-based data access during incident response, ensures backup integrity, and maintains log files in designated repositories to support ongoing monitoring and forensic investigations.	• CASB • NG-SWG • DLP
	Regularly notify stakeholders about their rights under applicable federal and state data privacy laws.	Netskope does not map to this requirement.	

DATA SECURITY CHECKLIST

Category	Control	Netskope controls	Products
Personnel security	Create an Acceptable Use Policy that outlines appropriate and inappropriate uses of the organization's information and communication technology (ICT) resources.	Netskope's Cloud Access Security Broker (CASB) allows realtime monitoring and logging of activities in SaaS and IaaS services, providing detailed user, device, and action information and implementing data loss prevention controls, including actions such as requiring business justifications or training on policy. Netskope's Next-Gen Secure Web Gateway (NG-SWG) integrates with third-party identity providers, offering SSO/MFA for web and cloud apps. It decodes and logs numerous activities, creates user activity baselines, and detects anomalies. NG-SWG applies detailed policy controls to manage risky behaviors, potentially requiring additional authentication or just-in-time cyber security training. It generates customizable reports and alerts, providing detailed logs for non-repudiation and incident response. Netskope's Cloud Firewall enforces organizational security policies on egress traffic without backhauling, inspecting queries to counter DNS attacks, and integrating logs into SIEM tools for incident handling. Advanced User Entity and Behavior Analytics (UEBA) includes numerous ML-based anomaly-detection models and the User Confidence Index (UCI), a dynamic risk score for users based on behavior. This helps adapt policies, recommend security training, and mitigate insider threats. Lastly, Netskope Device Intelligence identifies and classifies devices connecting to the network, leveraging AI/ML to detect anomalous behaviors and applying granular access controls in line with zero trust principles. It also integrates with incident response tools to generate alerts based on organizational criteria.	• CASB • NG-SWG • Cloud Firewall • Device Intelligence
	Incorporate security policies in job descriptions and specify employee responsibilities associated with maintaining compliance with these policies.	Netskope's CASB enables real-time monitoring of activities in SaaS and IaaS services, logging detailed information and applying immediate controls such as data loss prevention. It can block actions, request business justifications for risky actions, or provide policy training. Netskope's NG-SWG integrates with NIST-compliant identity providers, extending SSO/MFA across apps and services. It decodes over 100 inline activities, detects anomalies based on user behavior, and enforces granular policies. Beyond "allow" or "block," it can require multi-factor authentication or notify users of policy violations, suggesting safer alternatives or training. NG-SWG can generate alerts and reports for SIEM tools and supports non-repudiation of user actions. Advanced User Entity and Behavior Analytics (UEBA) includes numerous ML-based anomaly-detection models and the User Confidence Index (UCI), a dynamic risk score for users based on behavior. This helps adapt policies, recommend security training, and mitigate insider threats. UCI can integrate with Netskope's Cloud Exchange to share insider threat information.	• CASB • NG-SWG • Advanced UEBA

Category	Control	Netskope controls	Products
	Conduct regular checks and trainings to ensure employee understanding of the terms and conditions of their employment.	Netskope provides comprehensive tools for enforcing cyber security and data privacy policies across its product suite. It raises employee awareness through pop-up banners and coaching pages that notify of policy infringements, request justifications for risky actions, and refer users to third-party vendors for further training. Netskope's CASB monitors and logs SaaS and IaaS activities, applying real-time data loss prevention and activity-level controls that request justifications or provide training instead of merely blocking actions. Netskope's NG-SWG integrates with third-party identity providers to extend SSO and MFA to managed and unmanaged web and cloud apps. It decodes numerous inline activities, establishes user behavior baselines to detect anomalies, and applies context-aware policy controls. These controls can prompt multi-factor authentication, notify users of policy violations, suggest safer alternatives, or recommend training. NG-SWG can also generate customizable reports and alerts, feeding them into the organization's SIEM for incident response, with detailed logs aiding in proving user actions. Advanced User Entity and Behavior Analytics (UEBA) enhances threat detection using various ML-based models and incorporates the User Confidence Index (UCI) for dynamic risk assessment. This helps adapt policies, mitigate insider threats, and recommend security training, with UCI data sharable via Netskope's Cloud Risk Exchange.	• All products • CASB • NG-SWG • Advanced UEBA
	Confirm the trustworthiness of employees through the use of personnel security screenings, policy training, and binding confidentiality agreements.	Netskope's CASB provides comprehensive monitoring and logging of activities in SaaS and IaaS services, capturing details on user, device, instance, and actions. It enables realtime data loss prevention and activity-level controls, allowing not only blocking actions but also soliciting business justifications or delivering policy training. Netskope's NG-SWG integrates with NIST-compliant identity providers and extends SSO/MFA to both managed and unmanaged web and cloud apps. It decodes and logs over a hundred inline activities, establishes user activity baselines, and detects anomalies. The tool applies granular policy controls and offers context-aware responses like stepped-up MFA, policy violation notifications, safer action suggestions, or third-party cyber security training referrals. NG-SWG's customizable reporting and alerting facilitate incident response and support non-repudiation through detailed event logging. Advanced UEBA leverages numerous ML-based anomaly detection models and includes a User Confidence Index (UCI), a dynamic risk score for users. This index helps in adapting policies, recommending training, and mitigating insider threats. UCI also integrates with Netskope's Cloud Exchange to share insider threat information. Overall, Netskope's suite offers robust security controls, anomaly detection, and policy enforcement to enhance organizational security and compliance.	• CASB • NG-SWG • Advanced UEBA

Category	Control	Netskope controls	Products
Physical security	Secure and monitor access to any areas where sensitive data are stored and processed.	Netskope does not map to this requirement.	• All products • CASB • NG-SWG • Advanced UEBA
Network mapping	Map the organization's network in order to capture applications and associated data, and map the dependencies between applications, data, and network layers, and highlight potential vulnerabilities.	Netskope platform implements a defense-in-depth strategy to secure the organization's network and data. Netskope's Advanced Analytics provides detailed mapping of data flows across the organization's network, assessing cloud risk by categorizing data and cloud app usage by sensitivity. The analytics dashboard helps administrators monitor vulnerabilities and security trends by tracking app access, threats detected, policies triggered, and users affected. Netskope's CASB manages asset inventory, acquisition strategies, third-party risks, and business continuity by identifying and assessing managed and unmanaged apps' criticality based on usage and risk. NG-SWG integrates with identity providers, applies granular policies to detect anomalous behavior, and facilitates incident response by feeding data into SIEM tools. ZTNA Next provides secure remote access based on zero trust principles, supports encrypted data transfer, and enforces login policies. Device Intelligence monitors and classifies network connected devices, detects anomalies, and enhances security through zero trust principles and incident response integration. Cloud Security Posture Management continuously monitors IaaS platforms to prevent misconfigurations, ensure compliance with access policies and regulations, prevent data exfiltration, and automates remediation via integration with Cloud Ticket Orchestrator. SaaS Security Posture Management monitors SaaS functions for misconfigurations, integrates with Cloud Ticket Orchestrator, and continuously improves security rules. Netskope's Data Loss Prevention protects data across web, cloud apps, and devices using machine learning to identify and classify sensitive data. Enforces real-time protection policies and supports incident response and recovery.	• All products • CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • ZTNA Next • Device Intelligence • CTO
Inventory of assets	Create an inventory of all managed and unmanaged devices used in the organization's computing environment.	Netskope's CASB and NG-SWG support asset inventory, acquisition strategy, third-party risk management, and business continuity planning by cataloging both managed and unmanaged apps and cloud services within an organization's IT infrastructure, assessing their importance based on usage and risk level.	• CASB • NG-SWG
Authentication	Use multi-factor authentication for remote users and privileged "super users."	Netskope's NG-SWG integrates with NIST-compliant third party identity providers, extending multi-factor authentication across both managed and unmanaged web and cloud services. Granular access controls can be configured to require stepped-up multi-factor authentication for certain users or actions.	• NG-SWG • ZTNA Next

Category	Control	Netskope controls	Products
		Netskope's ZTNA Next provides secure remote access to private apps through end-to-end encryption and integrates with NIST-compliant third-party identity providers to enforce multi-factor authentication.	
Provide a layered defense	Employ a "defense in depth" architecture that uses a wide spectrum of tools arrayed in a complementary fashion.	Netskope assists organizations in implementing a network security architecture that's aligned with industry- recognized cyber security and data privacy best practices. This includes a "defense-in-depth" strategy that minimizes interactions between security layers, allowing them to function independently. Properly customized and configured, the Netskope platform addresses risk to organizational operations, assets, individuals, and third parties. Netskope's Borderless SD-WAN extends network perimeters to any user or device, using Netskope's global New Edge network for high-availability connectivity and adaptive trust enforcement based on specific criteria. Netskope's Cloud Firewall secures egress traffic to web or cloud applications, protecting against DDoS, man-in-the middle, and DNS attacks. It allows traffic inspection without backhauling to on-prem security stacks and integrates with SIEM tools for incident response and recovery. Netskope's Cloud Security Posture Management (CSPM) continuously monitors and scans IaaS platforms and cloud storage buckets to prevent misconfigurations and data exfiltration, ensuring compliance with organizational and regulatory standards. CSPM integrates with Netskope's Cloud Ticket Orchestrator for automated alerts and remediation. Netskope's SaaS Security Posture Management (SSPM) provides similar protection for mission-critical SaaS functions, offering alerts with remediation instructions and integration with Cloud Ticket Orchestrator for automated service tickets. Detected misconfigurations can be converted into new security rules.	• Public Cloud Security • CSPM • Cloud Firewall • SD-WAN • SSPM • CTO
Secure configurations	Test all hardware and software before connecting it to the network.	Netskope's SaaS Security Posture Management (SSPM) continuously monitors critical SaaS functions to prevent misconfigurations and ensure compliance with access management policies and regulatory standards. SSPM provides remediation instructions and can integrate with Netskope's Cloud Ticket Orchestrator to automate service tickets and remediation efforts. Misconfigurations can be converted into new rules to improve security. Netskope Device Intelligence manages and classifies all devices on the network, isolates risky devices into segments, and uses AI/ML to establish normal behavior baselines and detect anomalies. It applies access and activity controls based on zero trust principles and integrates with incident response tools to generate security alerts.	• CASB • NG-SWG • Public Cloud Security • SSPM • UEBA • Device Intelligence • CTO
	Continuously scan system components to ensure they remain in a secure state.	Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) continuously monitor mission-critical IaaS and SaaS platforms, respectively, to prevent misconfigurations and ensure compliance with organizational, regulatory, and industry standards.	• Public Cloud Security • CSPM • SSPM

Category	Control	Netskope controls	Products
		CSPM also scans cloud storage to prevent data exfiltration, while SSPM provides remediation instructions and can create rules from previously detected misconfigurations. Netskope's Device Intelligence identifies and manages all devices connecting to the network, isolating risky devices and detecting anomalies with an AI/ML engine. It applies zero trust principles and integrates with incident response tools for security alert generation.	• Device Intelligence • CTO • ZTNA Next
	Establish a comprehensive change management program to analyze and address security and privacy risks introduced by new technology or business processes.	Netskope scores SaaS applications in its Cloud Confidence Index (CCI) and provides many important details that help organizations assess the risk of using each vendor's application or cloud service. Criteria include the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more. Netskope's Cloud Security Posture Management (CSPM) continuously monitors an organization's critical IaaS platforms to prevent misconfigurations and ensure compliance with access management policies, regulatory, and industry standards. It routinely scans cloud storage buckets to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator to send alerts and automate remediation. Netskope's SaaS Security Posture Management (SSPM) similarly monitors SaaS functions to prevent misconfigurations and ensure proper use of assets and data. SSPM provides detailed remediation instructions and can also integrate with the Cloud Ticket Orchestrator to create service tickets from alerts and automate fixes. Additionally, SSPM allows previously detected misconfigurations to be converted into new security rules.	• Public Cloud Security • CSPM • SSPM • CTO • CCI
Access control	Require strong passwords and multiple levels of user authentication.	Netskope's NG-SWG and ZTNA Next integrate with NIST compliant identity providers to extend SSO/MFA across web and cloud apps. Adaptive and granular access controls can be configured to require stepped-up multi-factor authentication for certain users or actions.	• NG-SWG • ZTNA Next
	Set limits on the duration of data access, locking access after a session timeout.	Netskope's ZTNA Next provides remote access to on-prem or cloud-hosted private apps from any device, anywhere. ZTNA Next 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.	• ZTNA Next
	Limit logical access to sensitive data and resources.	Netskope's NG-SWG and ZTNA Next integrate with NIST compliant identity providers to extend SSO/MFA across web and cloud apps. Adaptive and granular access controls can be configured to require stepped-up multi-factor authentication for certain users or actions. Netskope's CASB and NG-SWG capture detailed information about users, devices, and actions, and incorporate Netskope's DLP engine to protect sensitive data in real time. Device Intelligence identifies, catalogs, and classifies all devices connecting to the network, uses AI/ML to establish normal behavior baselines, detects anomalies, and enforces granular controls, integrating with incident response tools for security alerts.	• CASB • NG-SWG • ZTNA Next • Device Intelligence • P-DEM

Category	Control	Netskope controls	Products
		Proactive Digital Experience Management provides comprehensive visibility into user experience from endpoints to the cloud, facilitates automated troubleshooting, and allows for proactive diagnosis and mitigation of performance issues.	
	Limit administrative privileges.	Netskope's ZTNA Next enables secure remote access to private applications, whether hosted on-premises or in the cloud, from any device. It integrates with NIST-compliant identity providers for secure authentication, employs end-to-end encryption, and uses granular controls to enforce zero trust principles, such as limiting access and privileges. ZTNA Next also logs all access attempts and enforces policies on failed logins. 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 a baseline of normal device behavior, detects anomalies, and enforces zero trust-based access and activity controls. Device Intelligence can integrate with incident response tools to trigger security alerts based on predefined criteria.	• ZTNA Next • Device Intelligence
	Use role-based access control to define specified roles and privileges for users.	Netskope's security suite includes Cloud Access Security Broker (CASB), Next-Generation Secure Web Gateway (NGSWG), and Cloud Security Posture Management (CSPM), all utilizing a comprehensive Data Loss Prevention (DLP) engine. This DLP ensures data security across web, cloud apps, and devices using machine learning to classify and protect sensitive information. Context-aware policies and role-based access control (RBAC) enforce data protection in real-time. CSPM continuously monitors IaaS platforms to prevent misconfigurations and integrates with Cloud Ticket Orchestrator for alerting and automated remediation. SaaS Security Posture Management (SSPM) does similarly for SaaS functions, providing step-by-step remediation instructions. ZTNA Next offers secure remote access with granular controls and RBAC, integrating with third-party identity providers and logging access attempts. Advanced User and Entity Behavior Analytics (UEBA) employs ML models for anomaly detection, generating a User Confidence Index to adapt policies and mitigate insider threats. This comprehensive system supports consistent organizational access management based on the principle of least privilege.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • ZTNA Next • Advanced UEBA • CTO
	Segregate sensitive data to which only the most privileged users have access in a separate server. If segregation isn't possible, utilize other additional protections - like encryption - to secure sensitive data.	Netskope's Cloud Access Security Broker (CASB) and Next-Gen Secure Web Gateway (NG-SWG) leverage a Data Loss Prevention (DLP) engine to secure organizational data across various environments, including the web, cloud applications, and endpoint devices. Netskope's Borderless SD-WAN supports network segmentation, and Device Intelligence identifies, catalogs, and classifies connected devices, segmenting risky ones and applying zero trust principles to control access based on behavioral anomalies.	• CASB • NG-SWG • DLP • SD-WAN

Category	Control	Netskope controls	Products
		The DLP engine employs machine learning for identifying, classifying, and protecting sensitive data in accordance with organizational or regulatory requirements. It uses context aware policies, which consider user, device, app, network, and action information to protect data in real-time through methods like obfuscating personal data, encrypting files, or blocking specific actions. Additionally, Netskope's DLP enforces role-based access during incident response, ensures backup integrity, and maintains logs for ongoing monitoring and forensic investigations. Netskope's CASB can also generate alerts for Security Incident and Event Management (SIEM) tools, supporting automated incident response and recovery processes. The event logs help in performing lessons learned analyses and creating Progress and Action On Milestones reports.	
Firewalls and Intrusion Detection/ Prevention Systems (IDPS)	Use a firewall to protect networks from unauthorized access.	Netskope's Cloud Firewall applies security policies to outbound traffic to the web or cloud without requiring traffic backhaul to on-premises security stacks. It disrupts DDoS, man-in-the-middle, and DNS attacks by inspecting queries for malicious activity. Event logs from the Cloud Firewall can be integrated with the organization's SIEM tool to aid incident response and recovery. Netskope's Borderless SD-WAN extends network perimeters to any user on any device, anywhere, by steering traffic through its global New Edge network. This ensures high availability connectivity to web and cloud applications and enforces uniform policy controls with adaptive trust based on context-specific criteria like user, location, device, and app instance.	• Cloud Firewall • SD-WAN
	Use IDPS systems to monitor for and detect malicious activity on the network, report on security incidents and take remediating measures.	Netskope's Cloud Firewall enforces organizational security policies on egress traffic without needing to reroute through an on-premises stack, defending against DDoS, DNS attacks, and more by inspecting domain queries. Event logs can be integrated with SIEM tools for incident response. Netskope's User Entity and Behavior Analytics (UEBA) monitors user activity across web and cloud services, setting baselines for normal behavior to detect anomalies, and enacting adaptive policy controls based on the riskiness of each user's actions. Netskope's Standard Threat Protection shields against known malware, employs machine learning to spot new threats, and includes real-time phishing detection and web filtering. Integrations with Netskope's other tools and threat intelligence feeds create a comprehensive defense-in-depth security strategy. Advanced Threat Protection enhances Standard Threat Protection with features like de-obfuscation, recursive file unpacking, and multi-stage sandboxing to counteract new malware. Device Intelligence identifies, catalogs, and classifies connected devices, segmenting risky ones and applying zero trust principles to control access based on behavior anomalies.	• CASB • NG-SWG • Cloud Firewall • UEBA • Advanced Threat Protection • Device Intelligence • Threat Protection

Category	Control	Netskope controls	Products
Patch management	Roll out software updates and patches on a regular basis.	Netskope evaluates SaaS applications through its Cloud Confidence Index (CCI), assessing risks based on security policies, certifications, audit capabilities, and legal concerns. Cloud Security Posture Management (CSPM) continuously monitors IaaS platforms and cloud storage to prevent misconfigurations and data exfiltration, integrating with Netskope's Cloud Ticket Orchestrator for automated alerts and remediation. Similarly, their SaaS Security Posture Management (SSPM) ensures SaaS functions comply with organizational policies and standards, providing detailed misconfiguration remediation steps and integration with the Cloud Ticket Orchestrator for automation. Netskope's Standard Threat Protection guards against known and new malware, offering real-time phishing detection and corroborative sandboxing. It integrates with multiple Netskope tools and threat intelligence feeds for a comprehensive, multi-layered security solution. Netskope's Advanced Threat Protection goes beyond standard measures, featuring techniques like de-obfuscation and multi-stage sandboxing to detect new malware. Device Intelligence identifies, classifies, and segments all devices on the network, using AI/ML to detect and control anomalous behavior, aligning with zero trust principles and integrating with incident response tools.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • SSPM • Advanced • Threat Protection Device • Intelligence Threat • Protection • CTO
Shut down unnecessary services	Shut down all ports and services that are not required in the computing environment.	Netskope's Cloud Firewall applies security policies to egress traffic without backhauling and protects against DNS attacks by inspecting queries. Its logs can integrate with SIEM tools for better incident response. Netskope's Cloud Security Posture Management (CSPM) ensures the continuous monitoring of mission-critical IaaS platforms to prevent misconfigurations and deviations from access policies or regulatory standards, thereby securing the intended use of these platforms and their data. CSPM also scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for alerting and automated remediation. Similarly, Netskope's SaaS Security Posture Management (SSPM) monitors SaaS functions to prevent misconfigurations, providing remediation instructions and integrating with the Cloud Ticket Orchestrator for automated responses. SSPM can convert detected misconfigurations into new security rules. Netskope Device Intelligence identifies, catalogs, and classifies all devices on the network, using AI/ML to detect behavioral anomalies and enforce granular access controls aligned with zero trust principles. It also integrates with incident response tools to generate security alerts.	• Public Cloud Security • CSPM • Cloud Firewall • SSPM • Device Intelligence • CTO
	Continuously monitor for the use of unapproved ports, protocols, and services.	Netskope's Cloud Security Posture Management (CSPM) continuously monitors an organization's critical IaaS platforms to prevent misconfigurations and ensure compliance with access management policies and regulatory standards. It routinely scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator to send alerts and automate remediation.	• Public Cloud Security • CSPM • SSPM • CTO

Category	Control	Netskope controls	Products
		Similarly, Netskope's SaaS Security Posture Management (SSPM) continuously monitors critical SaaS functions to prevent misconfigurations and ensure compliance. SSPM alerts include step-by-step remediation instructions and can be integrated with the Cloud Ticket Orchestrator to automate service tickets and remediation. Misconfigurations can also be converted into new rules to enhance security.	
Mobile devices	Encrypt any sensitive data stored on laptops, smart phones, or other mobile devices.	Netskope's CASB and NG-SWG feature a powerful Data Loss Prevention (DLP) engine that secures organizational data across web, cloud applications, and endpoint devices. Utilizing machine learning, Netskope's DLP identifies, classifies, and protects sensitive data based on organizational and regulatory requirements, and applies real-time, context aware policies. These include obfuscating personal data, encrypting files, and enforcing role-based access during incident response. Netskope's Device Intelligence identifies and classifies all devices on the network, grouping them into segments to isolate risks. Its AI/ML engine establishes a baseline of normal behavior, detects anomalies, and enforces zero trust principles through granular access controls. It also integrates with incident response tools to generate alerts based on predefined criteria.	• CASB • NG-SWG • DLP • Device Intelligence
Emailing confidential data	Do not email unprotected PII or sensitive data. Desensitize data prior to transmission, or encrypt the data files or email transmissions themselves.	Netskope's CASB and NG-SWG are equipped with Netskope's Data Loss Prevention engine which provides comprehensive security for organizational data in use, in transit, or at rest across the web, public and private cloud applications, and endpoint devices. Netskope'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. Netskope's DLP can be used to enforce role-based access to data during incident response and recovery, ensure the integrity of backups, and hold log files in dedicated repositories to facilitate continuous monitoring as well as internal or regulatory forensic investigations. Netskope's Standard User Entity and Behavior Analytics monitors user behavior across various web and cloud applications, establishes a baseline of normal activity, and uses sequential rules to identify abnormal behavior. Adaptive policy controls adjust access and privileges based on the risk level of a user's actions and deviations from the norm.	• CASB • NG-SWG • UEBA • Advanced Threat • Protection Threat Protection
Incident handling	Maintain an incident recovery plan to contain and recover from security incidents.	Netskope's integrated security suite facilitates efficient incident management. The Data Loss Prevention (DLP) engine utilizes machine learning to secure data in use, transit, or at rest by implementing context-aware policies. This engine is integral to preventing data leaks and ensuring compliance through actions like data obfuscation and encryption. The NG-SWG and CASB extend granular policy controls across web and cloud applications, detecting anomalous behavior and risky actions, and exporting logs to the organization's SIEM tool for incident response.	• CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • CLS • CTO

Category	Control	Netskope controls	Products
		Cloud Security Posture Management and SaaS Security Posture Management continuously check mission-critical platforms to prevent misconfigurations and data exfiltration, scanning routines, and alerting for deviations. The Cloud Log Shipper exports comprehensive event logs for detailed incident analysis, and Cloud Ticket Orchestrator automates incident response workflows, enhancing role based access controls and integrating with service tickets to streamline recovery efforts.	
	Establish procedures for users, security personnel, and managers that define their appropriate roles and actions during a security incident.	Netskope offers a suite of security tools designed to enhance incident response and recovery. Netskope's CASB generates alerts and exports them to an organization's SIEM tool for automated incident handling and post-incident analysis. NG-SWG integrates with NIST-compliant identity providers, enabling SSO/MFA across various apps, and it monitors user activity to detect anomalies, applying granular policy controls. NG-SWG can escalate to multi-factor authentication or notify users of policy violations, suggesting safer alternatives, or directing them to cyber security training. It also provides detailed event logging and generates reports and alerts for SIEM integration. Netskope's Cloud Log Shipper exports logs from multiple tools, including NG-SWG, CASB, and ZTNA Next, to the SIEM for incident management. Cloud Ticket Orchestrator automates service ticket creation and workflow responses to security alerts, enforcing role-based access controls during incident response.	• CASB • NG-SWG • CLS • CTO
	Maintain logs and records to support subsequent forensics investigations.	The Data Loss Prevention (DLP) engine identifies, classifies, and secures sensitive data using context-aware policies, and can hold log files in dedicated repositories to support regulatory compliance and forensics investigations. Other tools generate event logs, alerts, and insights to further support investigators. NG-SWG extends security through integration with third-party identity providers and granular policy controls. User behavior is monitored to detect anomalies, with adaptive policy adjustments enhancing security based on continuous risk assessment. ZTNA Next facilitates secure remote access with end-to-end encryption and zero trust principles. Device Intelligence monitors and manages device behaviors, segregating high-risk devices as needed. Advanced Analytics provides insights into data flows and cloud app usage, aiding in risk assessment. The Cloud Log Shipper streamlines event log management and integrates with SIEM tools, and Cloud Ticket Orchestrator automates incident response workflows, enhancing operational efficiency.	• CASB • NG-SWG • DLP • UEBA • ZTNA Next • Advanced Analytics • Device Intelligence • CLS • CTO

Category	Control	Netskope controls	Products
Audit and compliance monitoring	Periodically engage auditors to provide independent assessments of the organization's data protection capabilities and procedures.	The Netskope platform assists organizations in optimizing security tests and exercises by identifying critical digital assets and defining the scope of the attack surface. CASB, NGSWG, and Device Intelligence inventory all unmanaged apps and devices within the ICT environment, and the Cloud Confidence Index assigns them risk-based scores. Advanced UEBA uses machine learning to assess the riskiness of user behavior and assign users a User Confidence Index based on their behavior over time.	• All products • CASB • NG-SWG • Device Intelligence • CCI • Advanced UEBA

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