netskope

Compliance Series

Trusted Information Security Assessment Exchange (TISAX)

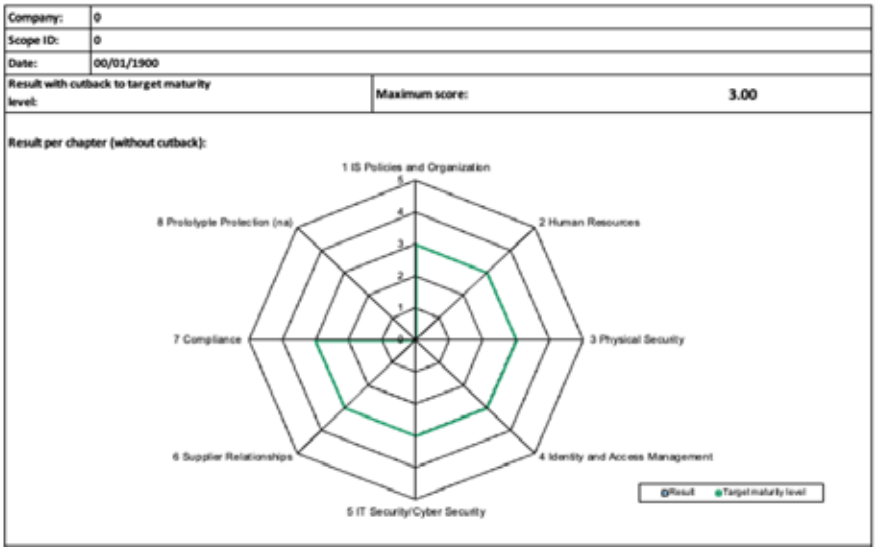
Control Mapping to Netskope Products

TABLE OF CONTENTS

INTRODUCTION

Information Security Assessment
Results

VDA | Verband der Automobilindustrie



The Trusted Information Security Assessment Exchange (TISAX) is an industry standard used by European automotive manufacturers and their business partners. It is largely based on the ISO 27001 standard. Though technically voluntary, European automotive manufacturers generally require their service providers, suppliers, or other business partners to comply with its requirements.

Those requirements are laid out in the TISAX Information Security Assessment (ISA) questionnaire. The process of certification begins with performing a self-assessment to identify any gaps between ISA requirements and organizational policies and capabilities. Once the self-assessment has been completed and any gaps remediated, the organization must retain an outside auditor to verify compliance.

Both the self-assessment and the subsequent audit assess the organization's information security policies and capabilities according to six maturity levels. These range from Level 0 (Incomplete) to Level 5 (Optimizing). A passing score requires the attainment of at least Level 3 (Established).
See diagram below.

HOW TO USE THIS GUIDE

This guide uses the most recent version of the TISAX ISA questionnaire, version 6.0.3. The ISA questionnaire consists of the Information Security Assessment (Sections 1 through 7), Additional Prototype Protection requirements (Section 8), and Additional requirements for Data Protection (Section 9). This guide omits Section 3 and Section 8, since these concern physical and environmental controls to which Netskope does not map.

Each requirement is broken down into **requirements that must be met**, requirements that should be met, additional requirements for high protection needs, ***and additional requirements for very high protection needs***. This guide will use the convention of bold face, plain, italics, and bold italics, respectively, to indicate the nature of the requirement.

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 Access
Threat/Risk Sharing	Cloud Threat Exchange (CTE) Cloud Risk Exchange (CRE)
IT/IoT/OT Security	Device Intelligence
Digital Experience Management	P-DEM

ADMINISTRATIVE CONTROLS

Control#	Requirements(s)	Netskope Controls	Products
1	**Information Security Policies and Organization**		
1.1	**Information Security Policies**		
1.1.1	**The Requirements for information security have been determined and documented:** • **The requirements are adapted to the organization's goals.** • **A policy is prepared and is released by the organization.** **The policy includes objectives and the significance of information security within the organization.** The information security requirements based on the strategy of the organization, legislation, and contracts are considered in the policy. The policy indicates consequences in case of non-conformance. Other relevant security policies are established. Periodic review and, if required, revision of the policies are established. The policies are made available to employees in a suitable form. Employees and external business partners are informed of any changes relevant to them.	The Netskope platform can enforce information security policies defined by the organization. It can also track acknowledgement and understanding of those policies through pop-up banners and coaching pages. Beyond simple allow or block rules, the Netskope platform can also inform users of potential policy violations, request a business justification for risky actions, or refer users for just-in-time cybersecurity training from third-party vendors.	• All products
1.2	**Organization of Information Security**		
1.2.1	**The scope of the ISMS is defined.** **The organization's requirements for the ISMS are determined.** **The organizational management has commissioned and approved the ISMS.** **The ISMS provides the organizational management with suitable monitoring and control means.** **Applicable controls have been determined.** **The effectiveness of the ISMS is regularly reviewed by the management.**	Netskope can assist organizations in defining the scope of their information security policies. Netskope's product suite inventories and assigns risk scores to applications, users, and devices. It builds a baseline of normal behavior for users and devices, and can detect anomalies and adjust privileges in real time.	• All products

Control#	Requirements(s)	Netskope Controls	Products
1.2.2	**Responsibilities for information security within the organization are defined, documented, and assigned.** **The responsible employees are defined and qualified for their task.** **The required resources are available.** **The contact persons are known within the organization and to relevant business partners.** There is a definition and documentation of an adequate information security structure within the organization. • Other relevant security roles are considered. *An appropriate organizational separation of responsibilities should be established in order to avoid conflicts of interest.*	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. This ensures users have only the permissions necessary for their roles, enhancing security across various platforms. Netskope's CASB monitors SaaS and IaaS activities, providing real-time data loss prevention and user training on policies. NG-SWG extends SSO/MFA to web and cloud apps, logging user activities, and uses context-aware controls to respond to risky behavior, generating reports and integrating with SIEM tools. And the DLP engine secures data across web, cloud apps, and devices using context-aware policies and machine learning for sensitive data protection. This includes role-based access, backup integrity, and log monitoring. Cloud Security Posture Management prevents misconfigurations in IaaS platforms and cloud storage, integrates with Cloud Ticket Orchestrator for alerts and remediation, and prevents data exfiltration. SaaS Security Posture Management ensures SaaS functions align with organizational policies through continuous monitoring and automated remediation. Netskope's Advanced User Entity and 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.	• All products
1.2.3	**Projects are classified while taking into account the information security requirements.** The procedure and criteria for the classification of projects are documented. During an early stage of the project, risk assessment is conducted based on the defined procedure and repeated in case of changes to the project. For identified information security risks, measures are derived and considered in the project. *The measures thus derived are reviewed regularly during the project and reassessed in case of changes to the assessment criteria.*	Netskope can support classification of projects based on data sensitivity, and can control access to cloud and on-prem based project management solutions through user policy management and data loss prevention (DLP) engines.	• NG-SWG • CASB • DLP • ZTNA Next

Control#	Requirements(s)	Netskope Controls	Products
1.2.4	**External services and IT services used are identified.** **The security requirements relevant to the IT service are determined.** **The organization responsible for implementing the requirement is defined and aware of its responsibility.** **Mechanisms for shared responsibilities are specified and implemented.** **The responsible organization fulfills its respective responsibilities.** In case of IT services, configuration has been conceived, implemented, and documented based on the necessary security requirements. The responsible staff is adequately trained. *A list exists indicating the concerned IT services and the respective responsible IT service providers.* *The applicability of the ISA controls has been verified and documented.* *The service configuration is included in the regular security assessments.* *Proof is provided that the IT service providers fulfill their responsibility.* *Integration into local protective measures is established and documented.*	Netskope's products identify and categorize managed and unmanaged apps and services in the organization's IT environment. Netskope's Cloud Confidence Index (CCI) provides a risk-based score to tens of thousands of apps based on dozens of criteria relating to security, auditability, and business continuity. Advanced Analytics offers cybersecurity risk dashboards that can be used to calculate, prioritize, and report on risks to responsible personnel and stakeholders. Netskope's Public Cloud Security can also help identify misconfigurations in public cloud and SaaS services. Netskope's Cloud Security Posture Management and SaaS Security Posture Management continuously monitor these services for misconfigurations, and offer support (including automation in some cases) for remediation.	• CASB • CCI • Advanced Analytics • Public Cloud Security • CSPM • SSPM
1.3	**Asset Management**		
1.3.1	**Information assets and other assets where security is relevant to the organization are identified and recorded.** • **A person responsible for these information assets is assigned.** **The supporting assets processing the information assets are identified and recorded.** • **A person responsible for these supporting assets is assigned.** A catalogue of relevant information assets exists: • The corresponding supporting assets are assigned to each relevant information asset. • The catalogue is subject to regular review.	Several Netskope products support asset inventory. Netskope's Device Intelligence identifies and classifies managed and unmanaged devices connecting to the organization's network. It also assigns devices a risk score based on real-time behavior. Netskope's CASB identifies and classifies managed and unmanaged apps and cloud services in the organization's IT ecosystem, and CCI assigns them risk-based scores. The Netskope platform can also discover, classify, and protect data across web and cloud applications, cloud infrastructure, on-prem servers, and endpoint devices. With Netskope's interactive dashboards, IT administrators gain visibility into asset inventory and categorization, and can generate reports for use by responsible parties.	• Device Intelligence • CASB • CCI • DLP

Control#	Requirements(s)	Netskope Controls	Products
1.3.2	**A consistent scheme for the classification of information assets regarding the protection goal of confidentiality is available.** **Evaluation of the identified information assets is carried out according to the defined criteria and assigned to the existing classification scheme.** **Specifications for the handling of supporting assets depending on the classification of information assets are in place and implemented.** The protection goals of integrity and availability are taken into consideration.	Netskope's Device Intelligence identifies and classifies managed and unmanaged devices connecting to the organization's network. It also assigns devices a risk score based on real-time behavior. Netskope's CASB identifies and classifies managed and unmanaged apps and cloud services in the organization's IT ecosystem, and CCI assigns them risk-based scores. The Netskope platform can also discover, classify, and protect data across web and cloud applications, cloud infrastructure, on-prem servers, and endpoint devices. With Netskope's interactive dashboards, IT administrators gain visibility into asset inventory and categorization, and can generate reports for use by responsible parties.	• Device Intelligence • CASB • CCI • DLP
1.3.3	**External IT services are not used without explicit assessment and implementation of the information security measurements.** • **A risk assessment of the external IT services is available.** • **Legal, regulatory, and contractual requirements are considered.** **The external IT services have been harmonized with the protection needs of the processed information assets.** Requirements regarding the procurement, commissioning, and release associated with the use of external IT services are determined and fulfilled. A procedure for release in consideration of the protection needs is established. External IT services and their approval are documented. It is verified at regular intervals that only approved external IT services are used.	Netskope can assist enforcement of this requirement by identifying—and implementing automated policies to restrict access to—all unmanaged apps and services currently in use in the organization's IT environment (also known as "Shadow IT"). Moreover, Netskope's CCI provides a risk-based score to tens of thousands of apps based on their security, auditability, and business continuity capabilities. These tools can be used to generate reports to support and document decisions regarding the adoption or rejection of external IT services.	• CASB • CCI

Control#	Requirements(s)	Netskope Controls	Products
1.3.4	**Software is approved before installation or use. The following aspects are considered:** • **Limited approval for specific use cases or roles** • **Conformance to the information security requirements** • **Software use rights and licensing** • **Source/reputation of the software** **Software approval also applies to special purpose software such as maintenance tools.** The types of software such as firmware, operating systems, applications, libraries, and device drivers to be managed are determined. Repositories of managed software exist. The software repositories are protected against unauthorized manipulation. Approval of software is regularly reviewed. Software versions and patch levels are known. ***Additional requirements for software use are determined.***	Netskope can restrict access to software download sites and perform continuous assessment of cloud services across IT, IoT, and OT systems.	• NG-SWG • CASB • Device Intelligence
1.4	**Information Security Risk Management**		
1.4.1	**Risk assessments are carried out both at regular intervals and in response to events.** **Information security risks are appropriately assessed.** **Information security risks are documented.** **A responsible person is assigned to each information security risk. This person is responsible for the assessment and handling of the information security risks.** A procedure is in place defining how to identify, assess, and address security risks within the organization. Criteria for assessment and handling of security risks exist. Measures for handling security risks and the persons responsible for these are specified and documented. • A plan of measures or an overview of their state of implementation is followed. In case of changes to the environment, reassessment is carried out in a timely manner.	NG-SWG and CASB can identify vulnerable operating systems and browsers, and Device Intelligence can assign risk scores to IoT, OT, and personal devices. CCI assigns risk-based scores to managed and unmanaged apps in the organization's IT ecosystem. Additionally, vulnerabilities and misconfigurations can be discovered through scanning of cloud services by Netskope's Cloud Security Posture Management and SaaS Security Posture Management. Netskope's Advanced User and Entity Behavior Analytics (UEBA) features the User Confidence Index, which scores users based on the riskiness of their actions. Finally, Netskope's Cloud Exchange links an organization's incident response tools with up-to-the-minute threat intelligence, and facilitates remediation of vulnerabilities and misconfigurations.	• NG-SWG • CASB • Device Intelligence • CCI • Public Cloud Security • CSPM • SSPM • Advanced UEBA

Control#	Requirements(s)	Netskope Controls	Products
1.5	**Assessments**		
1.5.1	**Observation of policies is verified throughout the organization.** **Information security policies and procedures are reviewed at regular intervals.** **Measures for correcting potential non-conformities are initiated and pursued.** **Compliance with information security requirements is verified at regular intervals.** **The results of the conducted reviews are recorded and retained.** A plan for content and framework conditions of the reviews to be conducted is provided.	Netskope can enforce information security policies defined by the organization. Netskope Security Posture Management (CSPM & SSPM) solutions are available for public cloud services and SaaS applications, giving visibility and control over cloud service security settings to manage according to legal, regulatory, and company policy requirements. CSPM and SSPM alert on misconfigurations, and these 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.	• All products • CSPM • SSPM • CLS • CTO
1.5.2	**Information security reviews are carried out by an independent and competent body at regular intervals and in case of fundamental changes.** **Measures for correcting potential deviations are initiated and pursued.** The results of conducted reviews are documented and reported to the management of the organization.	Netskope can assist organizations in preparing for security reviews. The Netskope platform inventories, classifies, and assigns risk scores to managed and unmanaged apps, cloud services, and devices in the organization's IT ecosystem; maps data flows across organizational networks; and continuously monitors cloud assets for misconfigurations. Netskope's Cloud Exchange allows organizations to get up-to-the-minute cyber threat intelligence, bi-directionally share indicators of compromise with other organizations, and automate security remediation efforts.	• CASB • CCI • Device Intelligence • Advanced Analytics • Public Cloud Security • Cloud Exchange

Control#	Requirements(s)	Netskope Controls	Products
1.6	**Incident and Crisis Management**		
1.6.1	**A definition for a reportable security event or observation exists and is known by employees and relevant stakeholders. The following aspects are considered:** • **Events and observations related to personnel** • **Events and observations related to physical security** • **Events and observations related to IT and cybersecurity** • **Events and observations related to suppliers and other business partners** **Adequate mechanisms based on perceived risks to report security events are defined, implemented, and known to all relevant potential reporters.** **Adequate channels for communication with event reporters exist.** A common point of contact for event reporting exists. Different reporting channels according to perceived severity exist. Employees are obliged and trained to report relevant events. Security event reports from external parties are considered. • An externally accessible way to report security events exists and is communicated. • Reactions to security event reports from external parties are defined. Mechanism to report incidents (and information about how to use them) are accessible to all relevant reporters. A feedback procedure to reporters is established. ***Tests and exercises of event and observation reporting are conducted regularly.***	The Netskope platform can be configured to generate alerts and reports based on criteria defined by the organization. Moreover, Netskope's Advanced Analytics allows IT administrators to analyze events relative to trends and baseline patterns of user or device behavior. And Netskope's Cloud Exchange allows organizations to get up-to-the-minute cyber threat intelligence, bi-directionally share indicators of compromise with other organizations, and automate security remediation efforts.	• NG-SWG • CASB • ZTNA Next • Public Cloud Security • DLP • Advanced Analytics • Cloud Exchange

Control#	Requirements(s)	Netskope Controls	Products
1.6.2	**Reported events are processed without undue delay.** **An adequate reaction to reported security events is ensured.** **Lessons learned are incorporated into continuous improvement.** During processing, reported events are categorized, qualified, and prioritized. Responsibilities for handling of events based on their category are defined and assigned. The following aspects are considered: • Coordination of incidents and vulnerabilities across multiple categories • Qualification and resources • Contact mechanisms based on type and priority • Absence-management A strategy for filing official reports and searching prosecution of potentially criminally relevant aspects of security incidents exists. *Maximum response times based on class, category, and severity are defined.* *Events not processed appropriately according to their priority are escalated.* • *Conditions and thresholds such as maximum reaction times before escalation are defined.* • *Mechanisms, processes, and contacts for escalation are defined.* • *Escalation paths up to the organization's top management are defined.* *Lawful, regulatory, contractual reporting obligations, and respective contact information are known.* *A communication strategy for security-related events exists. The following aspects are considered:* • *To whom to communicate* • *When to communicate* • *Responsibilities for communication* • *Authorization and approval of communication* • *Legal and regulatory restrictions of communication* • *What to communicate* • *How to communicate*	Netskope can be configured to collate and report on events and generate alerts based on a series of suspicious events. Netskope has built in ticketing systems, log analysis, forensic reporting, and advanced analytic capabilities to aid organizations in responding to information security incidents. 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. Multiple levels of access, including data obfuscation, can be applied to protect incident information on a need-to-know basis. Netskope supports continuous improvement of security policies by allowing organizations to incorporate previous remediations into new policies.	• NG-SWG • CASB • ZTNA Next • Public Cloud Security • DLP • Cloud Exchange • Advanced Analytics • CLS • CTO

Control#	Requirements(s)	Netskope Controls	Products
	Procedures for response to supplier security incidents are established. The following aspects are considered: • *Analysis of the impact on the own organization and invocation of appropriate internal mechanisms* • *The need for reporting according to own reporting procedures* ***Handling of events in different categories and priorities is regularly tested.*** • ***Exercises or simulations of rarely occurring categories and priorities.*** • ***Exercises or simulations include escalation mechanisms.***		
1.6.3	**An appropriate plan to react to and recover from crisis situations exists.** • **The required resources are available.** **Responsibilities and authority for crisis management within the organization are defined, documented, and assigned.** **The responsible employees are defined and qualified for their task.** Methods to detect crisis situations are established. • General indications for the existence or imminence of a crisis situation and specific predictable crises are identified. A procedure to invoke and/or escalate crisis management is in place. Strategic goals and their priority in crisis situations are defined and known to relevant personnel. The following aspects are considered: • Ethical priorities • Core business processes • Appropriate information security A crisis management team is defined and approved. The following aspects are considered: • Management commitment • Composition • Structure and roles • Competencies of members • Expectation and authority • Decision-making procedures	Several of Netskope's products can assist organizations in creating business continuity plans. Netskope's CASB and Cloud Confidence Index can identify critical cloud services and applications, and assign them risk-based scores. Netskope's Cloud Threat Exchange—a near real-time threat ingestion, curation, and sharing tool—can be integrated with organizations' IR, SIEM, or SOAR tools to automate disaster recovery workflows or playbooks. Netskope supports business continuity, including recovery from natural disasters or other crisis situations, through implementation of a SASE (Secure Access Service Edge) architecture. Designed with over 100 locations and 99.999% availability, Netskope's NewEdge Network supports high availability of services and is not reliant on public cloud infrastructure.	• CASB • CCI • Cloud Exchange • SASE

Control#	Requirements(s)	Netskope Controls	Products
	Crisis policies and procedures are defined and approved. The following aspects are considered: • Exceptional authorities and decision-making processes beyond the crisis management team • Primary and backup means of communication • Emergency operating procedures • Exceptional organizational structures • Exceptional functions, responsibilities, and authority *Relevant different potential crisis scenarios are identified. The following aspects are considered:* • *Crisis situations with unavailability of key personnel* • *Crisis situations with unavailability of key physical resources* • *Crisis situations with outage of key infrastructure* *Necessary resources and information to handle crises are identified.* • *Appropriate measures to ensure availability of infrastructure or fallback planning and information considering different crisis scenarios are in place.* *A communication strategy for crisis situations exists. The following aspects are considered:* • *To whom to communicate* • *When to communicate* • *Responsibilities for communication* • *Authorization and approval of communication* • *Legal and regulatory restrictions of communication* • *What to communicate* • *Communication channels* • *Instruments to monitor communication* • *Instruction and procedures for employees* *The efficiency, feasibility, and appropriateness of the crisis planning is evaluated regularly.* ***Crisis exercises and simulations involving all relevant decision-makers are conducted regularly.***		

Control#	Requirements(s)	Netskope Controls	Products
2	**Human Resources**		
2.1.1	**Sensitive work fields and jobs are determined.** **The requirements for employees with respect to their job profiles are determined and fulfilled.** **The identity of potential employees is verified.** The personal suitability of potential employees is verified by means of simple methods. An extended suitability verification depending on the respective work field and job is conducted.	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.	• CASB • NG-SWG • ZTNA Next
2.1.2	**A non-disclosure obligation is in effect.** **An obligation to comply with the information security policies is in effect.** A non-disclosure obligation beyond the employment contract or order is in effect. Information security aspects are considered in the employment contracts of the staff. A procedure for handling violations of said obligations is described.	Netskope offers pop-up banners and coaching pages across its suite of products to educate users on organizational information security policies. The Netskope platform builds a baseline of expected user behavior, and can be configured to trigger data loss prevention rules or adjust access privileges in response to risky or anomalous behavior. Netskope also offers controls, reporting, and auditing to manage terminated employees or changes in employment responsibilities.	• All products
2.1.3	**Employees are trained and made aware.** A concept for awareness and training of employees is prepared. The following aspects are considered: • Information security policy • Reports of information security events • Reaction to occurrence of malware • Policies regarding user accounts and login information • Compliance issues of information security • Requirements and procedures regarding the use of non-disclosure agreements when sharing information requiring protection • Use of external IT resources	The Netskope platform doesn't just allow or block specific actions. It also helps users understand the organization's information security policies by alerting users to potential violations, requesting a business justification for risky actions, suggesting safer alternatives, or even referring users to third-party vendors like KnowBe4 for just-in-time cybersecurity training.	• All products

Control#	Requirements(s)	Netskope Controls	Products
	Target groups for training and awareness measures are identified and considered in a training concept. The concept has been approved by the responsible management. Training and awareness measures are carried out both at regular intervals and in response to events. Participation in training and awareness measures is documented. Contact persons for information security are known to employees.		
2.1.4	**The requirements for teleworking are determined and fulfilled. The following aspects are considered:** • **Secure handling of and access to information while considering the protection needs and the contractual requirements applying to private and public surroundings** • **Behavior in private surroundings** • **Behavior in public surroundings** • **Measures for protection from theft** **The organization's network is accessed via a secured connection and strong authentication.** The following aspects are considered: • Measures for travelling • Measures for travelling to security-critical countries *Protective measures against overhearing and viewing are implemented.*	Netskope's Borderless SD-WAN provides site-to-site connectivity including options to segment networks and environments and manage logical access. Netskope's Zero Trust Network Access Next (ZTNA Next) utilizes in-line end-to-end (TLS) encryption for remote users to the web and private cloud applications. It also 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 connection or inbound access rules. ZTNA Next also integrates with NIST-compliant third-party identity providers like Okta to ensure secure authentication of remote users. Granular policy controls can adjust access privileges in real time in response to anomalous or risky behavior.	• SD-WAN • ZTNA Next

TECHNICAL CONTROLS

Control#	Requirements(s)	Netskope Controls	Products
4	**Identity and Access Management**		
4.1	**Identity Management**		
4.1.1	**The requirements for the handling of means of identification over the entire life cycle are determined and fulfilled. The following aspects are considered:** • **Creation, handover, return, and destruction** • **Validity periods** • **Traceability** • **Handling of loss** Means of identification can be produced under controlled conditions only. *The validity of any means of identification is limited to an appropriate period.* *A strategy of blocking or invalidation of means in case of loss is prepared and implemented as far as possible.*	Netskope offers synchronization services that can register users for access to web, cloud, or private application services. Netskope can also integrate into identity services that can control access to web, cloud, and on-prem services.	• NG-SWG • CASB • ZTNA Next • Public Cloud Security
4.1.2	**The procedures for user authentication have been selected based on a risk assessment. Possible attack scenarios have been considered.** **State-of-the-art procedures for user authentication are applied.** User authentication procedures are defined and implemented based on the business-related and security-relevant requirements. • Users are authenticated at least by means of strong passwords according to the state of the art. Superior procedures are used for the authentication of privileged user accounts. *Depending on the risk assessment, authentication procedures and access controls have been enhanced by supplementary measures.* ***Before gaining access to data of very high protection needs, users are authenticated by means of strong authentication according to the state of the art.***	Netskope integrates with third-party identity providers like Okta, Ping, and Google, extending SSO/MFA across web, managed and unmanaged apps, and cloud services, and can detect more than 100 inline actions within cloud services and SaaS applications, such as login, logout, view, browse, post, upload, delete, or download. When an action is detected, such as an upload of company data to a non-managed cloud service or application, Netskope can enforce a stepped-up MFA verification to confirm the activity is being performed by the actual user. Adaptive policy controls can also leverage Netskope's Cloud Confidence Index (CCI) ratings for apps and Netskope's User Confidence Index (UCI) risk scoring for the user to determine what is permitted. Device intelligence can also monitor IoT, OT, and traditional devices for authentication.	• NG-SWG • CASB • ZTNA Next • Public Cloud Security • CCI • Advanced UEBA • Device Intelligence

Control#	Requirements(s)	Netskope Controls	Products
4.1.3	**The creating, changing, and deleting of user accounts is conducted.** **Unique and personalized user accounts are used.** **The use of "collective accounts" is regulated.** **User accounts are disabled immediately after the user has resigned from or left the organization.** **User accounts are regularly reviewed.** **The login information is provided to the user in a secure manner.** **A policy for the handling of login information is defined and implemented. The following aspects are considered:** • **No disclosure of login information to third parties not even to persons of authority under observation of legal parameters** • **No writing down or unencrypted storing of login information** • **Immediate changing of login information whenever potential compromising is suspected** • **No use of identical login information for business and non-business purposes** • **Changing of temporary or initial login information following the first login** **The login information of a personalized user account must be known to the assigned user only.** A basic user account with minimum access rights and functionalities is existent and used. Default accounts and passwords pre-configured by manufacturers are disabled. User accounts are created or authorized by the responsible body. Creating user accounts is subject to an approval process. User accounts of service providers are disabled upon completion of their task. Deadlines for disabling and deleting user accounts are defined. The use of default passwords is technically prevented.	Netskope's NG-SWG, CASB, and ZTNA Next provide auditing and verification of user identities and credentials. Netskope Public Cloud Security provides discovery of identities and credentials in public cloud services including AWS, Azure, and GCP. Netskope's Cloud Security Posture Management and SaaS Security Posture Management also provide security configuration, auditing, compliance, and company checks for user identities in cloud services and managed SaaS apps.	• NG-SWG • CASB • ZTNA Next • Public Cloud Security

Control#	Requirements(s)	Netskope Controls	Products
	Where strong authentication is applied, the use of the medium is secure. User accounts are reviewed at regular intervals. This also includes user accounts in customers' IT systems. Interactive login for service accounts is technically prevented.		
4.2	**Access Management**		
4.2.1	The requirements for the management of access rights are determined and fulfilled. The following aspects are considered: • Procedure for application, verification, and approval • Applying the principle of least privilege • Access rights are revoked when no longer needed	Netskope products provide granular and adaptive policy controls with the ability to allow or block specific activities within an application, ensuring that access control permissions are not granted excessively and adhere to the principle of least privilege. When access to a cloud service or cloud application is granted, administrators can differentiate between personal, third-party, and corporate-owned instances of the same managed app and adjust policy controls accordingly. Activity controls can be implemented for both corporate-owned devices for web, SaaS, Shadow IT, and IaaS/PaaS, as well as personal devices accessing corporate-managed apps and cloud services. 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 and inbound access rules.	• NG-SWG • CASB • ZTNA Next • Public Cloud Security • CSPM • SSPM • Device Intelligence

Control#	Requirements(s)	Netskope Controls	Products
5	**IT Security / Cybersecurity**		
5.1	**Cryptography**		
5.1.1	**All cryptographic procedures used provide the security required by the respective application field according to the recognized industry standard.** • **To the extent legally feasible.** Preparation of technical rules containing requirements for encryption in order to protect information according to its classification. A concept for the application of cryptography is defined and implemented. The following aspects are considered: • Cryptographic procedures • Key strengths • Procedures for the complete life cycle of cryptographic keys, including generation, storage, archiving, retrieval, distribution, deactivation, renewal, and deletion An emergency process for restoring key material is established. *Key sovereignty requirements are determined and fulfilled.*	Netskope can encrypt data at rest within certain cloud applications subject to organizational requirements. Netskope's Data Loss Prevention engine can locate and secure organizational data by, for example, encrypting a sensitive file, or revoking sharing permissions. Netskope's Cloud Security Posture Management continuously monitors an organization's IaaS platforms for misconfigurations, including the use of weak encryption algorithms.	• NG-SWG • CASB • ZTNA Next • Public Cloud Security • DLP

Control#	Requirements(s)	Netskope Controls	Products
5.1.2	**The network services used to transfer information are identified and documented.** **Policies and procedures in accordance with the classification requirements for the use of network services are defined and implemented.** **Measures for the protection of transferred contents against unauthorized access are implemented.** Measures for ensuring correct addressing and correct transfer of information are implemented. Electronic data exchange is conducted using content or transport encryption according to the respective classification. Remote access connections are verified to possess adequate security features and capabilities. *Information is transported or transferred in encrypted form.* • *Where encryption is not feasible, information must be protected by similarly effective measures.* ***Information is transported or transferred in content-encrypted form.***	Netskope's Advanced Analytics maps data flows across the organization's IT ecosystem, giving administrators visibility into the apps and services being used to handle sensitive data. The Netskope platform provides the ability to enforce real-time controls on data in transit across all SaaS, IaaS, and web usage within the enterprise, including widely adopted Shadow IT apps and cloud services and endpoint devices. Netskope's cloud-hosted, enterprise-grade data loss prevention capabilities ensure that data is protected in transit anywhere in the enterprise, including when flowing to and from remote users. Netskope's ZTNA Next can ensure secure access for remote users with in-line end-to-end encryption (TLS) from client to web, cloud, and on-prem application through the Netskope services.	• Advanced Analytics • CASB • DLP • Public Cloud Security • ZTNA Next
5.2	**Operations Security**		
5.2.1	**Information security requirements for changes to the organization, business processes, and IT systems are determined and applied.** A formal approval procedure is established. Changes are verified and assessed for their potential impact on information security. Changes affecting information security are subjected to planning and testing. Procedures for fallback in fault cases are considered. *Compliance with the information security requirements is verified during and after the changes are applied.*	Netskope's Public Cloud Security solutions offer an easy-to-use console that gives administrators the ability to monitor and audit security configurations across all of an organization's cloud apps and services. These tools can check an organization's current cloud security configurations against organizationally defined policies, as well as against common standards and regulatory frameworks like PCI DSS, HIPAA, or GDPR. Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Management identify misconfigurations, and its Cloud Ticket Orchestrator assists remediation by generating service tickets and automating workflows.	• Public Cloud Security • CSPM • SSPM • Cloud Exchange • CTO

Control#	Requirements(s)	Netskope Controls	Products
5.2.2	**The IT systems have been subjected to risk assessment in order to determine the necessity of their separation into development, testing, and operational systems.** **A segmentation is implemented based on the results of risk analysis.** The requirements for development and testing environments are determined and implemented. The following aspects are considered: • Separation of development, testing, and operational systems • No development and system tools on operational systems • Use of different user profiles for development, testing, and operational systems	Netskope's Zero Trust Network Access (ZTNA Next), SD-WAN, and Cloud Firewall capabilities support network segmentation to ensure that development, testing, and operational environments are kept separate.	• ZTNA Next • SD-WAN • Cloud Firewall

Control#	Requirements(s)	Netskope Controls	Products
5.2.3	**Requirements for protection against malware are determined.** **Technical and organizational measures for protection against malware are defined and implemented.** Unnecessary network services are disabled. Access to network services is restricted to necessary access by means of suitable protective measures. Malware protection software is installed and updated automatically at regular intervals. Received files and software are automatically inspected for malware prior to their execution. The entire data contents of all systems is regularly inspected for malware. Data transferred by central gateways is automatically inspected by means of protection software. • Encrypted connections are considered. Measures to prevent protection software from being deactivated or altered by users are defined and implemented. Case-related staff awareness measures. For IT systems operated without the use of malware protection software, alternative measures are implemented.	Netskope NG-SWG decrypts and inspects content. NG-SWG's Advanced Threat Protection provides anti-malware detection, bare-metal and cloud sandboxing, and ML-based detection to detect and prevent malicious code from being executed. It also provides pre-execution analysis and heuristics for more than 3,500 file format families for Windows, Mac OS, Linux, iOS, Android, firmware, Flash, PDF, and other document types. And its Remote Browser Isolation ensures no malicious code is executed in an organization's environment. RBI works by executing web server code in cloud storage containers, and reproducing the resulting webpage as an interactive pixel-rendered image. RBI ensures no executable code makes it from a web server to an end-user's system, essentially creating an "air gap," ensuring complete safety for viewing web pages browsed through RBI. The NG-SWG also provides pop-up warnings and coaching pages to inform users of potential policy violations and enhance awareness of cybersecurity best practices. Netskope API-based IaaS Storage Scan can scan cloud storage buckets and blogs to detect unauthorized changes to cloud storage data, including detecting if legitimate software has been replaced with malware. Netskope's Cloud Security Posture Management continuously scans organizational IaaS platforms for misconfigurations, including unnecessary IaaS network services that should be disabled. Alerts can be exported to the organization's IR, SOAR, or SIEM tools to automate remediation efforts using Netskope's Cloud Log Shipper and Cloud Ticket Orchestrator. Netskope's SD-WAN permits network segmentation to manage logical access and prevent unauthorized activity.	• NG-SWG • CASB • Advanced Threat Protection • Advanced DLP • RBI • Public Cloud Security • CSPM • SSPM

Control#	Requirements(s)	Netskope Controls	Products
5.2.4	**Information security requirements regarding the handling of event logs are determined and fulfilled.** **Security-relevant requirements regarding the logging of activities of system administrators and users are determined and fulfilled.** **The IT systems used are assessed regarding the necessity of logging.** **When using external IT services, information on the monitoring options is obtained and considered in the assessment.** **Event logs are checked regularly for violations and noticeable problems in compliance with the permissible legal and organizational provisions.** A procedure for the escalation of relevant events to the responsible body is defined and established. Event logs are protected against alteration. Adequate monitoring and recording of any actions on the network that are relevant to information security are established. *Information security requirements relevant to security during the handling of event logs are determined and implemented.* *Cases of access during connection and disconnection of external networks are logged.* ***Logging of any access to data of very high protection needs as far as technically feasible and as permissible according to legal and organizational provisions.***	Netskope's NG-SWG, CASB, and ZTNA Next provides detailed logging of all web, cloud, and on-prem access and activity by users, including application events, page events, and alerts. Netskope also integrates with log and SIEM solutions, and can be configured to hold event logs in dedicated repositories for forensic or regulatory compliance requirements. Netskope's Cloud Log Shipper and Cloud Ticket Orchestrator can export event logs to SIEM tools, and Cloud Ticket Orchestrator assists the organization in automating incident response and remediation efforts. Netskope uses role-based access control to protect logs, and maintains an audit trail to prevent tampering. Netskope's Borderless SD-WAN and ZTNA Next log all network connections, and its Cloud Log Shipper and Cloud Ticket Orchestrator can export network event logs to organizational SIEM tools for enhanced visibility into network activity as well as automating remediation efforts.	• NG-SWG • CASB • ZTNA Next • DLP • CTO • CLS
5.2.5	**Information on technical vulnerabilities for the IT systems in use is gathered and evaluated.** **Potentially affected IT systems and software are identified, assessed, and any vulnerabilities are addressed.** An adequate patch management is defined and implemented. Risk minimizing measures are implemented, as necessary. Successful installation of patches is verified in an appropriate manner.	Netskope can inspect cloud infrastructure instances and SaaS services to identify new or existing technical vulnerabilities that exist against industry baselines and can offer auto-remediation where required. In addition, Netskope can identify devices including IT, IOT, and OT services that may have technical vulnerabilities.	• Public Cloud Security • CSPM • SSPM • Device Intelligence

Control#	Requirements(s)	Netskope Controls	Products
5.2.6	**Requirements for auditing IT systems or services are determined.** **The scope of the system audit is specified in a timely manner.** **System or service audits are coordinated with the operator and users of the IT systems or services.** **The results of system or service audits are stored in a traceable manner and reported to the relevant management.** **Measures are derived from the results.** System and service audits are planned, taking into account any security risks they might cause. Regular system or service audits are performed. • Carried out by qualified personnel. • Suitable tools are used for system and service audits. • Performed from the internet and the internal network. Within a reasonable period following completion of the audit, a report is prepared. *For critical IT systems or services, additional system or service audit requirements have been identified and are fulfilled.* ***IT systems and services are regularly scanned for vulnerabilities.*** • ***Suitable protective measures must be implemented for systems and services that may not be scanned.***	Netskope can assist with this requirement. Netskope's CASB and NG-SWG can identify and classify managed and unmanaged cloud apps and services in the organization's IT ecosystem, and categorize them by usage and risk. 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. Cloud Confidence Index assigns all discovered apps and services a risk-based score that accounts for the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more. Netskope's Advanced Analytics maps data flows across the organization, allowing administrators to identify mission-critical cloud apps and services, as well as important unmanaged ("Shadow IT") services. Netskope's Cloud Security Posture Management safeguards mission- critical IaaS platforms by preventing misconfigurations and ensuring compliance with organizational and regulatory standards, including regular scans to avoid data breaches. It integrates with Netskope's Cloud Ticket Orchestrator for alerts and automated remediation. Similarly, Netskope's SaaS Security Posture Management monitors SaaS functions for misconfigurations, provides remediation instructions, and can automate fixes via the Cloud Ticket Orchestrator, converting detected issues into improved security rules.	• CASB • NG-SWG • CCI • Advanced Analytics • Public Cloud Security • CTO
5.2.7	**Requirements for the management and control of networks are determined and fulfilled.** **Requirements regarding network segmentation are determined and fulfilled.** Procedures for the management and control of networks are defined. For a risk-based network segmentation, the following aspects are considered: • Limitations for connecting IT systems to the network • Use of security technologies • Performance, trust, availability, security, and safety considerations • Limitation of impact in case of compromised IT systems • Detection of potential attacks and lateral movement of attackers	Netskope's ZTNA Next, SD-WAN, and Cloud Firewall capabilities support network segmentation. Netskope can also ensure in-line end-to-end encryption (TLS) from client to web and cloud services through Netskope. Netskope offers a secure private access service to on-prem services via ZTNA Next and offers SD-WAN capabilities from hardware or software to securely connect sites. Netskope's Cloud Security Posture Management continuously monitors organizational IaaS platforms for misconfigured security settings, provides instructions for remediation, and integrates with Netskope's Cloud Ticket Orchestrator to automate workflows. By proactively ensuring security configurations are kept up to date, Netskope's CSPM helps limit the impact on any compromised IT system.	• ZTNA Next • Cloud Firewall • SD-WAN • NG-SWG • CASB • Public Cloud Security • DLP

Control#	Requirements(s)	Netskope Controls	Products
	• Separation of networks with different operational purposes • The increased risk due to network services accessible via the internet • Technology-specific separation options when using external IT services • Adequate separation between own networks and customer networks while considering customer requirements • Detection and prevention of data loss/leakage *Extended requirements for the management and control of networks are determined and implemented. The following aspects are considered:* • *Authentication of IT systems on the network* • *Access to the management interfaces of IT systems is restricted* • *Specific risks*	Netskope cloud-hosted, enterprise- grade data loss prevention capabilities identify and protect data in transit anywhere in the enterprise, including when flowing to and from remote users, allowing administrators to detect and track lateral movement by attackers.	
5.2.8	**Critical IT services are identified, and business impact is considered.** **Requirements and responsibilities for continuity and recovery of those IT services are known to relevant stakeholders and fulfilled.** Critical IT systems are identified. • The relevant systems are classified to have the appropriate protection needed. • Adequate and appropriate security measures are implemented. Continuity planning includes at least the following scenarios affecting critical IT systems: • (Distributed) denial of service attacks • Successful ransomware attacks and other sabotage activities • System failure • Natural disaster Continuity planning considers the following cases: • Alternative communication strategies, in case primary communication means are not available • Alternative storage strategies, in case primary storage means are not available • Alternative power and network Continuity planning is regularly reviewed and updated. *Continuity planning includes predefined time frames for resumption of operation in line with requirements.*	The Netskope platform can identify and classify managed and unmanaged cloud apps and services in the organization's IT ecosystem, and the Cloud Confidence Index assigns them a risk-based score that accounts for the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more. Netskope's Advanced Analytics maps data flows across the organization, allowing administrators to identify mission-critical cloud apps and services, as well as important unmanaged ("Shadow IT") services. Netskope's Cloud Firewall protects against distributed denial-of-service (DDoS) attacks by inspecting queries for harmful, newly registered, or algorithmically generated domains. Netskope's Borderless SD-WAN and NewEdge private cloud network 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. Netskope's ZTNA Next, Borderless SD-WAN, and Cloud Firewall support network segmentation, ensuring that backups are stored in a secure environment. And Netskope's DLP engine scans backups to ensure data integrity and the restoration of normal business operations from a known state.	• CASB • CCI • Advanced Analytics • Cloud Firewall • SD-WAN • ZTNA Next • DLP

Control#	Requirements(s)	Netskope Controls	Products
	Appropriate SLAs with external service providers according to continuity planning are in place. *Continuity plans include coordination of contractually agreed communication with business partners.* *Continuity planning is regularly tested including a full recovery and reconstitution of the system to a known state and compliance with defined target times.* *A backup and recovery strategy for critical IT services and information is defined and implemented. The following aspects are considered:* • *Backups are protected against unauthorized modificiation or deletion by malicious software* • *Backups are protected against unauthorized access by malicious software or operators* ***Continuity planning is coordinated with the continuity plans of relevant external service providers.*** ***Continuance of essential mission and business functions with minimal or no loss of operational continuity is possible. The plan for continuance of essential mission and business functions considers the following aspects:*** • ***Alternate operation strategies and necessary separated standby systems to retain and/or resume operation to the extent possible if critical IT services become unavailable*** • ***Alternate storage and backup sites that provide controls equivalent to that of the primary site*** ***Continuity planning is tested regularly. Tests and any lessons learned are documented.***		
5.2.9	**Backup concepts exist for relevant IT systems. The following aspects are considered:** • **Appropriate protective measures to ensure confidentiality, integrity, and availability for data backups** **Recovery concepts exist for relevant IT services.** A backup and recovery concept exists for each relevant IT service. • Dependencies between IT services and the sequence for recovery are considered. *Backup and recovery concepts are methodically reviewed at regular intervals.* *General restore capability is considered and tested.*	Netskope's DLP engine ensures backup integrity by securing data across web, cloud apps, and devices using context-aware policies and machine learning. Furthermore, Netskope's ZTNA Next, Borderless SD-WAN, and Cloud Firewall capabilities support network segmentation, ensuring backups are stored in a secure environment. Role-based access controls protect backups from unauthorized access or modification during incident response and recovery. Finally, Netskope's NewEdge private cloud network offers organizations a high-availability SASE architecture that allows operations to continue even in the event of a natural or man-made disaster.	• DLP • ZTNA Next • SD-WAN • Cloud Firewall

Control#	Requirements(s)	Netskope Controls	Products
	Backup and recovery concepts consider the following aspects: • *Recovery Point Objective* • *Recovery Time Objective* • *Required resources for recovery* • *Avoidance of overload scenarios during recovery* • *Appropriate spatial redundancy* ***Additional backups are performed via offline procedures, immutable backups, or by using isolated IAM technology.*** ***Restore procedures are technically tested in a methodical way at regular intervals.*** ***Geographical redundancy is considered in data backup and recovery concepts.***		
5.3	**System Acquisition, Requirement Management, and Developmenta**		
5.3.1	**The information security requirements associated with the design and development of IT systems are determined and considered.** **The information security requirements associated with the acquisition or extension of IT systems and IT components are determined and considered.** **Information security requirements associated with changes to developed IT systems are considered.** **System approval tests are carried out under consideration of the information security requirements.** Requirement specifications are prepared. The following aspects are considered: • The information security requirements • Vendor recommendations and best practices for secure configuration and implementation • Best practices and security guidelines • Fail safe Requirement specifications are reviewed against the information security requirements. The IT system is reviewed for compliance with specifications prior to productive use. The use of productive data for testing purposes is avoided as far as possible.	Netskope can be used to manage access to apps and services (like GitHub, Public Cloud, etc.) that are utilized as part of a secure software development life cycle. With instance awareness, services can also be managed to separate development, testing, and production environments. Netskope identifies and assigns risk scores to all managed and unmanaged apps and cloud services in the organization's IT ecosystem. Its Cloud Confidence Index (CCI) 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. Netskope's Cloud Security Posture Management and SaaS Security Posture Management continuously monitor organizational IaaS platforms and SaaS applications for security misconfigurations. Both can be integrated with Netskope's Cloud Ticket Orchestrator to automate remediation efforts.	• NG-SWG • CASB • ZTNA Next • Cloud Firewall • SD-WAN • CCI • Public Cloud Security

Control#	Requirements(s)	Netskope Controls	Products
	• Where productive data is used for testing purposes, it shall be ensured that the test system is provided with protective measures comparable to those on the operational system. • Requirements for the life cycle of test data. • Case-related specifications for the generation of test data are defined. ***The security of purpose-built software or significantly customized software is tested*** • ***during commissioning*** • ***in case of significant changes*** • ***or at regular intervals***		
5.3.2	**Requirements regarding the information security of network services are determined and fulfilled.** A procedure for securing and using network services is defined and implemented. The requirements are agreed in the form of SLAs. Adequate redundancy solutions are implemented. *Procedures for monitoring the quality of network traffic are defined and carried out.*	Netskope can audit web and cloud services and offer visibility into direct-to-net traffic flows and network services. Netskope's Cloud Confidence Index can help organizations determine whether to onboard a particular app or service, by assigning it a risk-based score that assesses each vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more. Netskope's Proactive Digital Experience Management (P-DEM) provides visibility and actionable insights on network and cloud performance to ensure the best user and app experience.	• NG-SWG • CASB • Public Cloud Security • CCI • P-DEM
5.3.3	**A procedure for the return and secure removal of information assets from each external IT service is defined and implemented.** A description of the termination process is given, adapted to any changes, and contractually regulated.	Netskope's CASB identifies and catalogues all managed and unmanaged apps and cloud services in the organization's IT ecosystem. This includes assessing activity and reporting on app usage, allowing the organization to ensure certain services are offboarded.	• CASB
5.3.4	**Effective segregation prevents access to own information by unauthorized users of other organizations.** The provider's segregation concept is documented and adapted to any changes. The following aspects are considered: • Separation of data, functions, customer-specific software, operating system, storage system, and network • Risk assessment for the operation of external software within the shared environment	Netskope's ZTNA Next can monitor external service providers' access to internal resources, and along with Netskope's Borderless SD-WAN, can support network segregation. Netskope products can also monitor activity from public cloud and SaaS provider activity logs via API integration, and inline end-user activity for both managed and unmanaged services by identifying user actions (e.g., edit, share, delete, upload, reboot, etc.) via forward proxy.	• ZTNA Next • Public Cloud Security • CASB • CCI • SD-WAN

Control#	Requirements(s)	Netskope Controls	Products
		Reverse proxy capabilities even allow for inline enforcement on non-corporate devices accessing corporate SaaS applications. Netskope's Cloud Confidence Index assigns risk scores to cloud apps and services based on criteria such as include the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more.	

THIRD-PARTY RISK MANAGEMENT

Control#	Requirements(s)	Netskope Controls	Products
6	**Supplier Relationships**		
6.1.1	**Contractors and cooperation partners are subjected to a risk assessment with regard to information security.** **An appropriate level of information security is ensured by contractual agreements with contractors and cooperation partners.** **Where applicable, contractual agreements with clients are passed on to contractors and cooperation partners.** **Compliance with contractual agreements is verified.** Contractors and cooperation partners are contractually obliged to pass on any requirements regarding an appropriate level of information security to their subcontractors. Service reports and documents by contractors and cooperation partners are reviewed. *Proof is provided that the information security level of the supplier is adequate for the protection needs of the information.*	Netskope's CASB and NG-SWG can identify managed and unmanaged apps and cloud services in the organization's IT ecosystem, and Netskope's Cloud Confidence Index (CCI) assigns cloud applications a risk-based score 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, and legal and privacy concerns, among others. Netskope products can also be used to apply controls and baseline assessments required for and by suppliers in line with security requirements.	• NG-SWG • CASB • Public Cloud Security • ZTNA Next • CCI
6.1.2	**The non-disclosure requirements are determined and fulfilled.** **Requirements and procedures for applying non-disclosure agreements are known to all persons passing on information in need of protection.** **Valid non-disclosure agreements are concluded prior to forwarding sensitive information.** **The requirements and procedures for the use of non-disclosure agreements and the handling of information requiring protection are reviewed at regular intervals.** Non-disclosure agreement templates are available and checked for legal applicability. Non-disclosure agreements include the following information: • The persons/organizations involved • The types of information covered by the agreement • The subject of the agreement • The validity period of the agreement • The responsibilities of the obliged party	Netskope supports compliance with non-disclosure agreements by offering transfer controls between web, cloud, and private applications. Netskope's data loss prevention engine offers source and destination controls that identify traffic and data flows between client and web, client and cloud application, client, and private application where configured. These controls can detect and block data transfers to apps—such as unmanaged ("Shadow IT") apps—whose vendors have not entered into non-dislosure agreements with the organization. Reporting is available via Advanced Analytics to report on data flows including cross-border transfers.	• NG-SWG • CASB • ZTNA Next • Public Cloud Security • DLP • Advanced Analytics

Control#	Requirements(s)	Netskope Controls	Products
	Non-disclosure agreements include provisions for the handling of sensitive information beyond the contractual relationship. Options of demonstrating compliance with specifications are defined. A process for monitoring the validity period of temporary non-disclosure agreements and initiating their extension in due time is defined and implemented.		

COMPLIANCE CONTROLS

Control#	Requirements(s)	Netskope Controls	Products
7	**Compliance**		
7.1.1	**Legal, regulatory, and contractual provisions of relevance to information security are determined at regular intervals.** **Policies regarding compliance with the provisions are defined, implemented, and communicated to the responsible parties.** The integrity of records in accordance with the legal, regulatory, or contractual provisions and business requirements is considered.	The Netskope platform allows for the creation of policies that map directly to common industry standards and regulatory frameworks, including ISO, NIST, PCI DSS, HIPAA, GDPR, and many others. Netskope Security Posture Management (CSPM & SSPM) solutions are available for public cloud services and SaaS applications, giving visibility and control over cloud service security settings to manage according to legal, regulatory, and company policy requirements. Netskope's DLP engine offers a legal hold capability that allows organizations to store alert and event logs in dedicated repositories for forensic or regulatory needs.	• All products
7.1.2	**Legal and contractual information security requirements regarding the procedures and processes in the processing of personally identifiable data are determined.** **Regulations regarding the compliance with legal and contractual requirements for the protection of personally identifiable data are defined and known to the entrusted persons.** **Processes and procedures for the protection of personally identifiable data are considered in the information security management system.**	The Netskope platform allows for the creation of policies that map directly to common industry standards and regulatory frameworks, including ISO, NIST, PCI DSS, HIPAA, GDPR, and many others. Netskope Security Posture Management (CSPM & SSPM) solutions are available for public cloud services and SaaS applications, giving visibility and control over cloud service security settings to manage according to legal, regulatory, and company policy requirements.	• All products

DATA PROTECTION

Control#	Requirements(s)	Netskope Controls	Products
9	**Data Protection**		
9.1	**Data Protection Policies**		
9.1.1	A policy is created, regularly updated, and approved by the organization's management.	Netskope can enforce data privacy policies defined by the organization.	• All products
9.2	**Organization of Data Protection**		
9.2.1	**A data protection officer is appointed, if required by Art. 37 of the GDPR.** • **Determination of whether the appointment of a data protection officer is voluntary or mandatory.** • **Otherwise determination of a data protection function or comparable.** **Publication of contact details.** **Integration into the organization's structure.** **Exercise of the control obligations as defined in Art. 39(1)(b) of the GDPR and corresponding documentation.** **Documentation of the data protection status and report to the organization's top management.** **Equipped with sufficient capacities and resources.** • **Determination of whether the data protection function is full-time or part-time.** • **Adequate professional qualification.** • **Regular professional training.** • **Access to specialist literature.** • **Support of the data protection officer by data protection coordinators in the company's organizational units, depending on the company size.**	Netskope does not map to this requirement.	• All products
9.3	**Processing Directory**		
9.3.1	**If required by law, a register of processing activities as defined in Art. 30(1) and/or (2) of the GDPR exists and is up to date.** • **Technical and organizational measures required for processing as required by the information security questionnaire are adequately implemented for the processing activities.** • **There is a process description/sequence description with defined responsibilities.**	Netskope's security solutions, including CASB and NG-SWG, utilise a data loss prevention (DLP) engine to discover personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal data with predefined GDPR definitions. Netskope provides an export capability through the use of Cloud Exchange to assist the data controller in maintaining an accurate and up-to-date record of processing.	• CASB • NG-SWG • Public Cloud Security • DLP • Cloud Exchange

Control#	Requirements(s)	Netskope Controls	Products
9.4	**Data Protection Impact Assessment**		
9.4.1	**Processing activities that require a data protection impact assessment are known.** **Data protection impact assessments are carried out.** • **Responsibilities/tasks and support possibilities in the context of data protection impact assessments are defined and known.**	Netskope can assist with the performance of DPIAs for data processed by Netskope products. Netskope's security solutions, including CASB and NG-SWG, utilise a data loss prevention (DLP) engine to discover and secure personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying and protecting personal data according to organisational and regulatory standards with pre-defined GDPR definitions applying context-aware policies to manage processing of personal data in real time. These context-aware policies include applying automatic encryption of personal data. Netskope's Cloud Security Posture Management (CSPM) monitors IaaS platforms to prevent misconfigurations and ensure personal data security measures are implemented and maintained. CSPM scans cloud storage to prevent data exfiltration and integrates with Netskope's Cloud Ticket Orchestrator for alerts and automated remediation. Netskope's SaaS Security Posture Management (SSPM) continuously monitors SaaS functions to prevent misconfigurations, ensuring protection of personal data. All these products assist the data controller in completing a Data Protection Impact Assessment, in understanding where personal data is processed and what security measures are in place.	• All products
9.5	**Data Transfers**		
9.5.1	**Appropriate processes and workflows for the transmission of data are implemented.** • **Ensuring the consent or the right of objection of the person responsible for subcontracting.**	Netskope does not map to this requirement.	

Control#	Requirements(s)	Netskope Controls	Products
9.5.2	**Applicable contractual obligations to clients are passed on to subcontractors and cooperation partners.** **Compliance with contractual agreements is reviewed.** • **Contact details of the contact persons of the subcontractor are available and up to date.**	Netskope products can be used to apply controls and baseline assessments required for and by suppliers in line with contractually agreed-upon security requirements. Netskope's Cloud Confidence Index (CCI) scores cloud apps and services (potential processors) based on security, certifications, audit capabilities, legal, and privacy concerns. Utilising CCI scoring, a data controller can apply policies to limit and restrict transfers to potential risky processors Netskope can also audit web and cloud applications, and provide metadata to understand if suppliers are using underlying cloud infrastructure to support supply chain discovery.	• CASB • Public Cloud Security • ZTNA Next
9.5.3	**Transfers to third countries are known and systematically recorded.** **Sufficient guarantees are available for data transfers.** **In the case of data transfers to third countries, it is determined whether the consent of the person responsible is to be obtained for each transfer to third countries.**	Netskope's security solutions, including CASB and NG-SWG, utilise a data loss prevention (DLP) engine to discover personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal data according to organisational and regulatory standards with pre-defined GDPR definitions. Advanced Analytics can assist data controllers in understanding and visualising data flows including cross-border transfers. Where organizational data must reside in a particular country or region, organizations can elect to have their data processed and stored in the appropriate Management Plane. Where data must be transferred to third countries, Netskope uses Standard Contractual Clauses and complies with appropriate data privacy frameworks—such as the EU-U.S. Privacy Framework, the Swiss-U.S. Data Privacy Framework, and the UK Extension to the EU-U.S. Data Privacy Framework.	• All products
9.6	**Handling Requests and Incidents**		
9.6.1	**Requests from data subjects are processed in a timely manner.** • **Procedures are in place to assist the controller in responding to data subject requests.** • **Employees are trained to the effect that they must immediately contact the respective person responsible in the event of an incoming request from a data subject and coordinate the further procedure with this person.**	Netskope's security solutions, including CASB and NG-SWG, utilise a data loss prevention (DLP) engine to discover personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal data to assist data controllers with executing data subject access requests (DSAR). DLP can also assist in verifying right to erasure has been performed by using discovery across web, cloud applications, and endpoint devices.	• NG-SWG • CASB • DLP

Control#	Requirements(s)	Netskope Controls	Products
9.6.2	**Data protection incidents are processed in a timely manner.** **The requirements from 1.6 of the information security questionnaire also take into account data protection incidents or, alternatively, there is an emergency plan for dealing with data protection incidents.** • **In addition, procedures are established and documented to ensure the following aspects:** • **Immediate notification to the respective responsible person, as far as their order is affected** • **Documentation of the incident-handling activities** • **Training of employees on the defined measures/ processes** • **Support of the respective controller in the processing of data protection incidents**	Netskope's security solutions, including CASB and NG-SWG, utilise a data loss prevention (DLP) engine to discover personal data across various environments such as web, cloud applications, and endpoint devices. The DLP engine leverages machine learning for identifying personal data according to organisational and regulatory standards with pre- defined GDPR definitions. DLP can assist the controller in determining the scope of the breach, which data subjects are impacted and who should be notified.	• CASB • NG-SWG • DLP
9.7	**Human Resources**		
9.7.1	**Employees whose tasks include the processing of personal data are obliged to maintain confidentiality and to comply with applicable data protection laws.** • **The obligation is documented.**	Netskope uses role-based access controls to ensure only authorized users have access to data based on the needs of their respective roles in the organization. Netskope products provide granular and adaptive policy controls with the ability to allow or block specific activities within an application, ensuring that access control permissions are not granted excessively and adhere to the principle of least privilege.	• All products

Control#	Requirements(s)	Netskope Controls	Products
9.7.2	**Employees are trained and sensitized.** • **Scope, frequency, and content of the training is determined according to the protection needs of the data.** • **Employees in critical areas are instructed and trained specifically for their work.**	Netskope can assist with awareness and training on organizational data protection policies. Beyond simple allow or block rules, the Netskope platform can be configured to notify users of potential policy violations, suggest safer alternatives, request a business justification or a stepped-up MFA for risky actions, or refer the user for just-in-time cybersecurity training.	• All products
9.8	**Instructions**		
9.8.1	**The instructions by the controller regarding the processing of personal data are handled.** **Procedures and measures are in place to ensure that:** • **Received instructions are documented** • **Instructions can be implemented** • **Data is separated by client and specific order or project**	Netskope data loss prevention policies protect data in use, data in transit, and data at rest, and can be customized in accordance with organizational requirements and contractual obligations, and/or adapted to common industry standards and regulatory frameworks.	• All products

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.