netskope

Compliance Series

UK Telecommunications (Security) Act

Code of Practice Mapping Guide of Netskope Products

TABLE OF CONTENTS

INTRODUCTION

This document provides a mapping of the Telecommunications Security Act (TSA) to the associated controls available from Netskope.

This document includes a mapping table that includes measures from Section 3: Technical guidance measures from the Telecommunications Security Code of Practice. This document does not provide legal guidance on how to comply with the TSA however includes products that may be suitable to provide measures to meet the requirements and obligations for the provider.

TSA CODE OF PRACTICE MAPPING TO NETSKOPE

Specific technical measures from section 3 of the Code of Practice are set out below, grouped by the date by which they are expected to be completed.

As per the Code of Practice, it should be noted, however, that the extent to which each technical guidance measure can contribute to ensuring compliance with any specific regulation will depend on the facts of each case. The mapping of measures to products in this section is therefore only indicative and non-exhaustive.

Measure Number	Description	Netskope Control	Netskope Products
Overarching security measures Completed by 31 March 2024 (Tier 1) or 31 March 2025 (Tier 2)			
M1.01	Providers shall maintain accurate records of all externally facing systems.	Netskope has the capability to create an inventory of cloud-based services and devices that are used by the organisation that are externally facing.	• CASB • Device Intelligence
M1.03	Equipment in the exposed edge shall not host sensitive data or security critical functions.	Netskope has the ability to scan for sensitive data in systems and devices along with providing a Zero Trust Network Access (ZTNA) capability to prevent exposure of systems.	• CASB • CSPM • SSPM • ZTNA
M1.04	Physical and logical separation shall be implemented between the exposed edge and security critical functions. Note that this measure may not be necessary once datasets and functions can be cryptographically-protected from compromise.	Netskope provides a Zero Trust Network Access (ZTNA) capability to prevent exposure of systems.	• ZTNA
M1.05	Security boundaries shall exist between the exposed edge and critical or sensitive functions that implement protective measures.	Netskope provides a Zero Trust Network Access (ZTNA) capability to prevent exposure of systems.	• ZTNA
M1.06	Equipment in the exposed edge shall not be able to impact operation or routing within the core network. As an example, the exposed edge shall not be a PE-node within the provider's IP Core.	Netskope provides a Zero Trust Network Access (ZTNA) capability to prevent exposure of systems.	• ZTNA

Measure Number	Description	Netskope Control	Netskope Products
Management plane 1 Completed by 31 March 2024 (Tier 1) or 31 March 2025 (Tier 2)			
M2.03	Privileged access shall be via secure, encrypted, and authenticated protocols whenever technically viable.	Netskope provides a Zero Trust Network Access (ZTNA) capability to prevent exposure of systems.	• ZTNA
M2.04	Management protocols that are not required shall be disabled on all network functions and equipment.	Netskope provides a Zero Trust Network Access (ZTNA) capability to prevent exposure of systems.	• ZTNA
Third party supplier measures 1 Completed by 31 March 2024 (Tier 1) or 31 March 2025 (Tier 2)			
M4.01	The provider shall ensure the risks included in Regulation 7(3) are assessed prior to contract, and this assessment is documented. This assessment shall inform both risk management and procurement processes.	Netskope offer a Cloud Confidence Index (CCI) capability that assesses the security and compliance controls of cloud services (third party suppliers). Netskope CCI includes a 78,000+ list of cloud service providers with a risk rating 0-100 assessed against certifications, standards, data protection, access control, auditability, DR/BCP, legal/privacy, attack surface management.	• CASB (Applicable to Cloud services only)
M4.02	During procurement of equipment, prior to contract award, it is recommended that providers should, as a minimum, use the guidance contained in NCSC's vendor security assessment to assess third party suppliers (as contained in Annex B).	Netskope offer a Cloud Confidence Index (CCI) capability that assesses the security and compliance controls of cloud services (third party suppliers).	• CASB (Applicable to Cloud services only)

Measure Number	Description	Netskope Control	Netskope Products
Supporting business processes Completed by 31 March 2024 (Tier 1) or 31 March 2025 (Tier 2)			
M5.01	The provider shall implement appropriate business processes. In order to achieve this, providers shall have regard to implementing the parts of the CAF that define the provider's business processes. These are contained within Annex C. These are: A1-Governance; A2-Risk Management; A3-Asset Management; B5-Resilient Networks and Systems; B6-Staff Awareness and Training; D1-Response and Recovery Planning; D2-Lessons Learned.	Netskope offers direct or supplementary controls that can assist with supporting business processes including providing governance, risk reporting, asset management, resilient networks and access control and staff awareness/ training. Netskope provides controls and reporting capabilities across many of the NCSC CAF guidance including: • Managing security risk (reporting) • Protecting against cyber attack (identity and access control, device management, data security, system security, resilient networks and systems, staff awareness and training) • Detecting cyber security events (monitoring, logs, alerts, incidents, proactive security event discovery).	• All Products

Measure Number	Description	Netskope Control	Netskope Products
Third party supplier measures 3 Completed on all new contracts after 31 March 2024 (Tier 1), 31 March 2025 (Tier 2), and on all contracts by 31 March 2027 (All providers)			
M10.20	Providers shall maintain an up-to-date list of all third-party administrator personnel that are able to access its network, including their roles, responsibilities and expected frequency of access.	Netskope provides a Zero Trust Network Access (ZTNA) capability to manage access to systems, applications, services. ZTNA reporting is available to produce a list of personnel accessing services and baselining activity.	• ZTNA
M10.21	Providers shall have the contractual right to control the members of third-party administrator personnel who are involved in the provision of the third-party administrator services, including to require the third-party administrator to ensure that any member of personnel no longer has access to the network.	Netskope provides a Zero Trust Network Access (ZTNA) capability to manage access to systems, applications, services. ZTNA reporting is available to produce a list of personnel accessing services and baselining activity.	• ZTNA
M10.22	Providers shall not allow routine, direct access to network equipment by third party administrators. Access shall be via mediation points owned and operated by the provider.	Netskope provides a Zero Trust Network Access (ZTNA) capability to manage access to systems, applications, services. ZTNA reporting is available to produce a list of personnel accessing services and baselining activity.	• ZTNA
M10.23	Providers shall implement and enforce security enforcing functions at the boundary between the third-party administrator network and the provider network.	Netskope provides a Zero Trust Network Access (ZTNA) capability to manage access to systems, applications, services. ZTNA reporting is available to produce a list of personnel accessing services and baselining activity.	• ZTNA
M10.31	Providers shall ensure that the elements of the provider network that are accessible by the third-party administrator shall be the minimum required to perform its contractual function.	Netskope provides a Zero Trust Network Access (ZTNA) capability to manage access to systems, applications, services. ZTNA reporting is available to produce a list of personnel accessing services and baselining activity.	• ZTNA
M10.32	Providers shall both log and record all third-party administrator access into its networks.	Netskope provides a Zero Trust Network Access (ZTNA) capability to manage access to systems, applications, services. ZTNA reporting is available to produce a list of personnel accessing services and baselining activity.	• ZTNA

Measure Number	Description	Netskope Control	Netskope Products
Management plane 3 Completed by 31 March 2027			
M11.14	A device that is not necessary to perform network management or support management operations shall not be able to logically access the management plane.	Netskope provides a Zero Trust Network Access (ZTNA) capability to manage access to systems, applications, services. Netskope offer Device Intelligence services to identify rogue devices.	• Device Intelligence • ZTNA
M11.24	A PAW shall only have access to the internet to the extent it is needed to carry out changes to security critical functions, and such access shall be secured (e.g. via VPN).	Netskope provides a Zero Trust Network Access (ZTNA) capability to manage access to systems, applications, services. Netskope offer Device Intelligence services to identify rogue devices.	• Device Intelligence • ZTNA
M11.25	The PAW shall only have access to internal-only business systems (e.g. not corporate email).	Netskope provides a Zero Trust Network Access (ZTNA) capability to manage access to systems, applications, services. Netskope offer Device Intelligence services to identify rogue devices.	• Device Intelligence • ZTNA
Virtualisation 1 Completed by 31 March 2027			
M13.20	Privileged access to the virtualisation fabric shall only be available over authenticated and encrypted channels.	Netskope provides a Zero Trust Network Access (ZTNA) capability to manage access to systems, applications, services. ZTNA reporting is available to produce a list of personnel accessing services and baselining activity.	• ZTNA

Measure Number	Description	Netskope Control	Netskope Products
Network Oversight Functions Completed by 31 March 2027			
M15.03	Any workstations or functions (e.g. jump boxes) through which it is possible to make administrative changes to network oversight functions shall be rebuilt from an up-to-date known-good software state on a yearly-basis. This applies to the workstation or function's operating systems and above.	Netskope provides a Zero Trust Network Access (ZTNA) capability to manage access to systems, applications, services. Netskope ZTNA solution is based on software-defined network components including a software publisher that can be deployed as required.	• ZTNA
M15.04	Network oversight functions shall run on trusted platforms.	Netskope provides a Zero Trust Network Access (ZTNA) capability to manage access to systems, applications, services. The solution is built on zero trust principles.	• ZTNA
M15.06	Network oversight functions shall only be managed by a minimal set of trusted privileged users.	Netskope provides for Role-Based Access Control (RBAC) to ensure least privilege is applied.	• ZTNA
M15.07	The management functions (e.g. jump box) used to manage network oversight functions shall only be accessible from designated PAWs.	Netskope provides a Zero Trust Network Access (ZTNA) capability to manage access to systems, applications, services. Netskope offer Device Intelligence services to identify rogue devices.	• ZTNA

Measure Number	Description	Netskope Control	Netskope Products
Monitoring and analysis 1 Completed by 31 March 2027			
M16.04	Asset management and network monitoring systems shall be kept up to date to enable security staff to identify and track down anomalies within networks. This shall include comprehensive details of normal system and traffic behaviour (e.g. source and destination, frequency of communication, protocols and ports used, and expected bandwidth consumed).	Netskope provides a Zero Trust Network Access (ZTNA) capability to manage access to systems, applications, services. ZTNA reporting is available to produce a list of personnel accessing services, baselining activity and identify anomalies.	• ZTNA • Advanced Analytics
M16.06	Providers shall monitor physical and logical interfaces between networks that operate at different trust levels, as well as between groups of network functions (e.g. core networks and access networks).	Netskope provides a Zero Trust Network Access (ZTNA) capability to manage access to systems, applications, services. ZTNA reporting is available to produce a list of personnel accessing services, baselining activity and identify anomalies.	• ZTNA • Advanced Analytics
M16.13	Network-based and host-based sensors shall be deployed and run throughout networks to obtain traffic to support security analysis.	Netskope provides a Zero Trust Network Access (ZTNA) capability to manage access to systems, applications, services. ZTNA reporting is available to produce a list of personnel accessing services, baselining activity and identify anomalies.	• ZTNA • Advanced Analytics
M16.21	Indications of potential anomalous activity, and potential malicious activity, shall be promptly assessed, investigated, and addressed.	Netskope provides a Zero Trust Network Access (ZTNA) capability to manage access to systems, applications, services. ZTNA reporting is available to produce a list of personnel accessing services, baselining activity and identify anomalies.	• ZTNA • Advanced Analytics

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.