netskope

Compliance Series

Digital Operational Resilience Act (DORA)

Mapping the DORA Regulation to Netskope Products

TABLE OF CONTENTS

INTRODUCTION

TIn the wake of the 2008 financial crisis, the EU passed several new regulations designed to mitigate systemic risks in the financial sector. Initially these efforts focused on ensuring adequate capital requirements to withstand future credit crunches. But as the years went by, regulators began to recognize that an increasingly sophisticated cyber threat landscape, combined with the lack of a uniformand robust legal regime for cyber security, also posed a systemic risk to the financial system.

Therefore, the EU passed the Digital Operational Resilience Act (DORA). The purpose of DORA is to mitigate cyber risk in the financial sector by ensuring continuity of economic activity and promoting awareness of any threats to that continuity. DORA seeks to foster a culture of learning and evolution among financial entities and third party vendors of information and communication technology (ICT) products and services, so that together they can continuously improve their ability to meet the objectives of continuity and awareness in the face of threat actors who are also learning and evolving.

SCOPE OF THE LAW

DORA applies to all "financial entities," a category that includes banks, investment firms, insurance companies, and credit ratings agencies, among others. It also applies to the third party vendors of ICT products and services that have been deemed "critical for financial entities." Full details of the scope can be found in Article 2 of the Regulation.

THE FIVE PILLARS OF RESILIENCE

DORA's first 40 Articles (the ones that apply to financial entities and third party ICT vendors) can be arranged in a framework encompassing five major Pillars:

- **ICT Risk Management** - this pillar essentially recapitulates the six functions of the NIST Cybersecurity Framework (Govern, Identify, Protect, Detect, Respond, and Recover). It also includes a seventh function - Communication - designed to promote threat intelligence sharing among financial entities.
- **Incident Management, Classification, and Reporting** - this pillar seeks to harmonize and streamline incident management, classification, and reporting across the financial sector. It prescribes policies for monitoring, logging, and classifying cyber incidents, and articulates criteria for determining when an incident must be reported to regulators.
- **Operational Resilience Testing** - this pillar requires entities to undergo routine, independent testing of their digital operational resilience, and establish policies for addressing any identified weaknesses. Depending on their size, the nature of services they provide, and their risk profile, some entities will have to undergo periodic threat led penetration testing.
- **Information Sharing** - this pillar authorizes financial entities to create arrangements for sharing cyber threat intelligence, provided the data shared is relevant to enhancing digital operational resilience and not protected confidential, sensitive, or personal information.
- **Third Party Risk** - this pillar requires entities to monitor their potential overreliance on particular third party ICT vendors, and assess any risks associated with those vendors' use of subcontractors to fulfill their service agreements. It also articulates standard contractual provisions to govern the relationship between financial entities and third party vendors.

Netskope's products can be deployed and configured to help enterprises with compliance with each Pillar in the DORA regulation.

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 Exchange Cloud Threat Exchange (CTE) Cloud Risk Exchange (CRE)
IT/IoT/OT Security	Device Intelligence
Proactive Digital Experience Management	P-DEM
Third-Party Risk Management/Supply Chain	Cloud Confidence Index (CCI)

The following table will break down each Pillar, Article by Article, mapping specific Netskope productsand use cases to individual regulatory requirements. Only the requirements relevant to Netskope controls have been included, all other requirements have been omitted.

PILLAR I – ICT RISK MANAGEMENT

Article	Requirements	Netskope Control	Netskope products
5	**Governance and Organization** Establish internal governance frameworks for managing cyber risks. Any entity with more than 10 employees must establish a role assessing third party ICT vendor risk, or delegate this responsibility to a member of senior management. Managers must ensure security awareness training is provided to all staff and also complete regular training themselves to understand cyber risk and stay abreast of current cyber threats affecting their business.	Netskope can enforce organizational policies defined by the organization. It can also reinforce regular awareness training through the use of real-time pop-up notifications whenever a user violates a policy. These pop-up notifications can be implemented flexibly, allowing the customer to warn users before a potential violation occurs, block them entirely from carrying out the action, or provide them with real-time coaching, including suggesting safer alternatives or requesting a justification for the action.	All products
6	**Risk Management Framework** Formulate a risk management framework - tailored to each entity's business needs, size, and complexity - to address cyber risks quickly, efficiently, and comprehensively. The framework must be documented and include strategies, policies, procedures, protocols, and tools necessary to secure an entity's ICT infrastructure and minimize risk to digital assets. It must demonstrate the entity's mature awareness of its cyber risk profile and tolerance levels, and how its cybersecurity strategy aligns with and supports its overall business strategy. It must be audited on a regular basis, and entities must establish processes for remediating any deficiencies revealed by such audits..	Netskope can be implemented to protect ICT assets including devices, servers and other infrastructure including both on-prem and cloudbased services. Netskope supports reporting and advanced analytics to align to organization's risk management frameworks including details on ICTrelated incidents and ICT third-party cloud service providers Netskope's Security Posture Management (*SPM) tools help to enforce many Risk Management Frameworks along with Netskope Cloud Exchange (CE) which allows organizations to integrate both Netskope and third party cybersecurity tools, giving a more holistic, consistent picture of security posture.	All products

Article	Requirements	Netskope Control	Netskope products
7	**Risk Management Framework** Formulate a risk management framework - tailored to each entity's business needs, size, and complexity - to address cyber risks quickly, efficiently, and comprehensively.	The Netskope NewEdge platform is a reliable platform with 99.999% SLA uptime. Encompassing 100+ full compute data centers across the globe with highavailability and industry-leading SLAs on performance throughput, the platform can handle traffic for organizations during peak times and can scale up quickly in the event of an increase in demand..	All products
8	**Identification**		
8.1	Identify, classify, and document all ITrelated business functions, information assets supporting those functions, and ICT system configurations and interconnections with internal and external ICT systems. Review and update on at least an annual basis.	Netskope offers controls to identify and classify information assets based on policies or requirements. It also uses an intelligent DLP engine to apply controls to any unclassified information. Netskope also provides detailed reports and interactive dashboards that identify, categorize, and assign risk scores to the thousands of applications that may be in use in an ICT ecosystem. In particular, Netskope's NG-SWG and CASB products can detect and catalog any external, unmanaged SaaS apps with an unmatched degree of accuracy.	• NG-SWG • CASB • Public Cloud Security • ZTNA Next • DLP • Device Intelligence
8.2	Continuously identify all sources of ICT risk - but especially those relevant to the financial sector - and assess cyber threats and vulnerabilities relevant to ICT-related business functions and information assets. Review relevant cyber risk scenarios on at least an annual basis.	Netskope Cloud Threat Exchange and Cloud Risk Exchange (both part of the Cloud Exchange platform) can keep an organization up to date with respect to particular cyber threats (including IoCs, malicious URLs, and malicious file hashes), and overall risk scores for users, devices, and apps in an ICT ecosystem. Netskope's Cloud Confidence Index discovers any cloud apps being used in an ecosystem and assigns a risk-based score to each based on many criteria, including recently disclosed vulnerabilities and exploits.	• CTE/CRE • CCI

Article	Requirements	Netskope Control	Netskope products
8.3	Entities with more than 10 employees must perform risk assessments upon any major change to their ICT network or infrastructure, or to the processes or procedures affecting their function, supporting processes, or information assets.	Netskope's Cloud Confidence Index (CCI) can help perform a risk assessment before adopting a new app, or when setting policies after an app has been adopted. Using CCI's interactive feature, organizations can adjust the risk impact of adopting a new app based on a specific level of tolerance for certain kinds of risks. Netskope's Security Posture Management (*SPM) tools help to enforce many Risk Management Frameworks along with Netskope Cloud Exchange (CE) which allows organizations to integrate both Netskope and third party cyber security tools, giving a more holistic, consistent picture of security posture. Advanced Analytics can be used to identify the outcome of any changes to ICT network or infrastructure and can be used to feed into a risk assessment for triage and trend analysis.	• NG-SWG • CASB • Public Cloud Security • ZTNA Next • DLP • Device Intelligence
8.4	Identify all information assets and ICT assets and map configuration of ICT assets and links and interdependencies between ICT assets.	The Netskope platform can discover managed and unmanaged devices in a network including the ability to characterize SaaS, IaaS, and web usage across an entire enterprise, including monitoring non-corporate devices accessing corporate SaaS applications and users accessing non-corporate SaaS applications from corporate devices. With Netskope in place, the security team can map communication and data flows for personal and corporate app instances, and enforce controls to contain data flows when unmanaged devices are being used or unmanaged services are being adopted by end users.	• NG-SWG • CASB • Public Cloud Security • ZTNA Next • DLP • Device Intelligence

Article	Requirements	Netskope Control	Netskope products
8.5	Identify and document all processes dependent on third party ICT vendors, and all interconnections with third party ICT vendors.	Netskope products can identify, categorize, and assign risk scores to thousands of apps in use in an ICT ecosystem. For example, the Cloud Confidence Index (CCI) assesses the risks associated with a given vendor's app or cloud service, based on criteria like the vendor's security policies and certifications, and its audit capabilities.	• Public Cloud Security • ZTNA Next • CCI • Device Intelligence
8.6	Entities shall maintain relevant inventories and update them periodically and every time any major change occurs.	Netskope can help maintain an inventory of systems and services for both cloud services (SaaS, PaaS, IaaS) along with an inventory of devices including IoT services.	• CASB • Device Intelligence
8.7	Conduct risk assessments on all legacy ICT systems at least once per year, and always before connecting new technologies, applications, or systems.	Netskope products can identify, categorize, and assign risk scores to thousands of apps in use in an ICT ecosystem. For example, the Cloud Confidence Index (CCI) assesses the risks associated with a given vendor's app or cloud service, based on criteria like the vendor's security policies and certifications, and its audit capabilities.	• CSPM • SSPM • CCI
9	**Protection and Prevention**		
9.1	Continuously monitor and control functioning of ICT systems and tools. Deploy appropriate security tools, policies, and procedures.	Many Netskope tools can be used to protect systems and networks, and identify anomalous behavior, malware and policy violations. As an example, Netskope's NG-SWG uses threat protection and data protection along with behavior-based analytics to identify both external and internal threats. For example, Netskope's Cloud Security Posture Management and SaaS Security Posture Management continuously monitor cloud services.	All products

Article	Requirements	Netskope Control	Netskope products
9.2	Design, procure, and implement ICT security strategies, policies, procedures, protocols, and tools specifically to (1) ensure the resilience, continuity, and availability of ICT systems, and (2) maintain high standards of security, confidentiality, and integrity of data at rest or in motion.	Netskope's NewEdge private cloud network implements a high-availability cloud-based architecture allowing operations to continue in the event of a failure at any node. And Netskope's Borderless SD-WAN supports high availability/resilience allowing remote users to access critical SaaS applications by enabling failover to alternate connectivity links in the event of a blackout/brownout. Netskope's Public Cloud Security tools protect data at rest and in motion. These can be configured to perform data loss prevention scans, alert on policy violations, and take corrective actions such as revoking sharing permissions or encrypting a sensitive file. Netskope's DLP engine is fully integrated into the entire cloud platform, ensuring that both data-atrest and data-in-motion are protected by the same set of policies and workflows.	• NG-SWG • CASB • ZTNA Next • Public Cloud Security • DLP • Threat Protection
9.3	Adopt state-of-the-art technology to (1) guarantee security of data transfers, (2) minimize risk of data corruption/loss or unauthorized access, (3) prevent data leakage, and (4) ensure proper data handling and record-keeping.	Netskope offers transfer controls between web, cloud, and private applications, including source and destination controls that identify traffic and data flows between the client and the web, the client and cloud applications, and the client and private applications. Reporting on data flows, including cross-border data transfers, is available via Advanced Analytics. Netskope's DLP engine uses machine learning algorithms to identify and protect sensitive data at rest or in motion. It enforces access and transfer policies, streamlines the process for responding to policy violations, and uses strong AES-256 encryption to protect sensitive data.	• DLP • NG-SWG • CASB • Public Cloud Security • ZTNA Next • Advanced Analytics

Article	Requirements	Netskope Control	Netskope products
9.4	Include the following in the Risk Management Framework: 1. information security policy defining rules to protect the confidentiality, integrity, and availability of the entities' and its customers' ICT resources, data, and information assets. 2. risk-based network and infrastructure management using appropriate techniques, methods, and protocols, including automated mechanisms for isolating affected information assets in the event of a cyber attack. 3. policies that limit physical and virtual access to ICT system resources and data to what is required only for legitimate and approved functions and activities. 4. policies for strong authentication mechanisms based on relevant standards. 5. risk-based policies for ICT change management, including changes to software, hardware, firmware components, system or security changes, to ensure all changes to ICT systems are recorded, tested, assessed, and approved in a controlled manner. 6. appropriate and comprehensive policies for updates and patches. Entities shall design the network connection infrastructure in a way that allows it to be instantaneously severed or segmented in order to minimize and prevent contagion, especially for interconnected financial processes.	Netskope offers controls to identify and protect data and use of cloud applications, cloud infrastructure, or private applications and their associated information assets using Zero-Trust principles. Policies can be implemented to ensure acceptable use of assets based on requirements. Netskope ZTNA Next allows for access to applications and services directly using Zero Trust principles, assisting with segmentation and limiting the exposure of networks and possibility of lateral movement. Netskope NG-SWG with Advanced Threat Protection, Remote Browser Isolation, Cloud Firewall, and Intrusion Prevention System provide active mitigation against malware, high-risk websites, phishing, browser attacks, OS vulnerabilities, and firewall egress controls over ports and protocols. Netskope can ensure that access control permissions adhere to the principle of least privilege. Netskope can also be used to identify misconfigurations in access controls, bringing them into alignment with policies and industry standards. Netskope integrates with third-party identity providers to manage secure authentication. And the Netskope NGSWG extends SSO/MFA across managed and unmanaged apps andcloud services.	• NG-SWG • CASB • Public Cloud Security • ZTNA Next • DLP • CSPM • SSPM • Device Intelligence • RBI • Cloud Firewall

Article	Requirements	Netskope Control	Netskope products
10	**Detection**		
10.1	Detect anomalous activities, including performance issues and security incidents, and to identify all potential material single points of failure.	Netskope Behavior Analytics identifies baselines of user behavior for web, app, and cloud services via real-time inline and API out-of-band monitoring across its Security Service Edge products. These create User Confidence Index scores to identify insider threats, compromised accounts or devices, and data exfiltration. Proactive Digital Experience Monitoring can be used to identify performance issues and the cause. Netskope can also aggregate and alert on automated testing results from third-party systems if they are configured to send their results to Netskope. Netskope continuously improves detection processes by advancing its integration with security operation center processes and third party solutions. APIs are provided for sandboxing and retrospective hunting, and the Cloud Exchange modules share threat intel, export event logs, exchange risk scores, and automate workflows with orchestration and collaboration solutions.	• NG-SWG • P-DEM • Public Cloud Security • CSPM • SSPM • DLP • CASB • Cloud Exchange
10.2	Detection mechanisms must: 1. enable multiple layers of control, 1. define alert thresholds and criteria for triggering incident detection and response processes, and 1. put in place automatic alert mechanisms for relevant staff in charge of incident response.	Netskope's open architecture and Cloud Log Shipper tool enables thirdparty integration with market-leading security services and ticketing systems. Netskope can be integrated with existing solutions in an environment to ensure the detailed data generated by Netskope is collected and correlated and alerts created. Netskope provides detailed activity logs and high-level reports, allowing security teams to effectively communicate critical information consistent with incident response plans. Moreover, Netskope's Cloud Ticket Orchestrator enables the automatic creation of security tickets, instantly escalating events to responsible parties.	• NG-SWG • Cloud Exchange • CASB • Public Cloud Security • Private Access

Article	Requirements	Netskope Control	Netskope products
10.3	Devote sufficient resources and capabilities -commensurate with the entity's size, business, and risk profile - to monitor user activity, anomalous behavior, and security incidents.	Netskope automatically identifies a baseline of normal user behavior via real-time security of user activity. Anomaly alerts are generated when unusual activity occurs.	• NG-SWG • CASB • Public Cloud Security • ZTNA Next • Advanced Analytics • SkopeAI • P-DEM
11	**Response and Recovery**		
11.1	As part of the Risk Management Framework, establish a dedicated and comprehensive Business Continuity Policy. Test the policy on an annual basis, and after any substantive change to ICT systems.	Netskope can help support business continuity through implementation of a Secure Access Service Edge architecture. Designed with over 100+ data centers and 99.999% availability, Netskope's NewEdge platform supports high availability of services with no reliance on public cloud infrastructure.	• SASE
11.2	The Business Continuity Policy must establish procedures and mechanisms for: 1. ensuring continuity of critical functions, 2. quickly, appropriately, and effectively responding to and resolving security incidents in a way that limits damage and prioritizes resumption of activities and recovery actions, 3. immediately activating dedicated containment measures, processes, and technologies suited to each type of security incident, including damage controls, 4. estimating impacts, damages, and losses, and 5. initiating communication and crisis management actions to ensure updated information is transmitted to all relevant staff, stakeholders, and regulators.	Netskope Proactive Digital Experience Management provides visibility on network and cloud performance so degradation, failover, or critical status information is accessible in near real time. The Cloud Ticket Orchestrator allows the ability to map alerts, events, and log data into whatever format is required to facilitate automated workflows in ServiceNow, Jira, and Pager Duty, or notifications in Slack, Teams, email, etc.	• P-DEM • Cloud Exchange • NG-SWG • CASB • Public Cloud Security • Private Access • Advanced Analytics • Device Intelligence

Article	Requirements	Netskope Control	Netskope products
11.3	As part of the Risk Management Framework, implement an Incident Response and Recovery Plan. For entities with more than 10 employees, the Incident Response and Recovery Plan must be independently audited.	Defining the scope of an Incident Response and Recovery Plan requires awareness of all the devices and applications - whether managed or unmanaged - that power a business, and the critical data that flow between them. The Netskope platform offers adaptive, comprehensive, and granular visibility into an entire ICT ecosystem, enabling an accurate assessment of critical systems.	• Device Intelligence • NG-SWG • CASB • DLP
11.4	Put in place, maintain, and periodically test appropriate business continuity plans, especially with respect to critical or important functions outsourced or contracted through third party ICT vendors.	Each vendor's CCI score is calculated with reference to numerous criteria, including: certifications, data protection capabilities, auditability, access controls, disaster recovery and business continuity plans, and any known vulnerabilities or exploits.	• CCI
11.5	As part of the entity's business continuity plan, conduct a business impact analysis (BIA) of its exposure to severe business disruptions. The BIA must consider the criticality of identified and mapped business functions, support processes, third-party dependencies and information assets, and their interdependencies. ICT assets and services must be designed and used in full alignment with the BIA, in particular with regard to adequately ensuring the redundancy of all critical components.	Netskope's NewEdge private cloud network implements a high-availability cloud-based architecture allowing operations to continue in the event of a failure at any node. Netskope's Borderless SD-WAN supports high availability/resilience allowing remote users to access critical SaaS applications by enabling failover to alternate connectivity links in the event of an incident. The Netskope platform will assist in identifying critical information assets and services. Netskope's NG-SWG and CASB will help inventory and classify managed and unmanaged apps in an ICT ecosystem, including by volume and patterns of usage.	• SASE • SD-WAN • NG-SWG • CASB • CCI • CSPM • SSPM • DLP
11.8	Keep records of activities before and during any events that cause the Business Continuity Policy or Incident Response and Recovery Plan to be activated.	Netskope offers a ticketing system to escalate high risk information security events and can store forensic data in forensic tools or repositories defined by the customer. In addition, Netskope offers legal hold capabilities that allow for the preservation of data in a forensic repository for legal requirements.	All products

Article	Requirements	Netskope Control	Netskope products
12	**Backup Policies and Recovery Methods**		
12.1	The Risk Management Framework must include a backup policy and recovery methods designed to minimize downtime and disruptions. The backup policy must specify the scope of the data subject to backup and the minimum frequency of backups, based on the criticality and sensitivity of the data.	The Netskope platform can support a backup policy, particularly with a view to minimizing downtime, by discovering, monitoring, and protecting critical and sensitive data, whether at rest, in motion, or in use, and mapping how that data flows across the ICT ecosystem.	• DLP • CASB • Public Cloud Security • Advanced Analytics
12.2	Backup systems must begin processing without delay, except where such processing would jeopardize the security of the network or the integrity or confidentiality of the data.	Netskope's industry-leading Data Loss Prevention tool uses Machine Learning and AI to identify, classify, and protect sensitive and critical data across an ICT ecosystem, ensuring sensitive or critical data is not exposed accurately and reliably.	• DLP • Public Cloud Security • CASB
12.3	To prevent unauthorized access or data corruption, backups must be stored in a secure operating environment segregated from the entity's normal ICT systems.	Netskope supports segregation of networks using Zero Trust Network Access, SD-WAN, and Cloud Firewall capabilities.	• ZTNA Next • Cloud Firewall • SD-WAN
12.4	Maintain redundant ICT capacities equipped with resources, capabilities, and functionalities sufficient to meet business needs.	Netskope has implemented a highavailability cloud-based architecture that allows operations to continue in the event of a failure. Netskope's NewEdge private cloud network uses a global data center footprint to replicate systems and backup data between regional data centers for reliability and disaster recovery.	• SASE • NG-SWG • CASB • ZTNA Next

Article	Requirements	Netskope Control	Netskope products
12.6	Recovery time objectives must be determined in light of both agreed service levels and the overall impact on market efficiency.	Netskope can support recovery time objectives by identifying and classifying mission critical applications and data in the ICT environment, and incorporating those findings into an Incident Response and Recovery Plan.	• NG-SWG • CASB • DLP • Public Cloud Security • Advanced Analytics
12.7	During recovery, including when reconstructing data from external stakeholders, perform multiple checks and reconciliations to ensure data integrity and consistency between systems.	Netskope can discover information assets across cloud applications and can identify duplication of data from backups.	• CASB • Public Cloud Security • DLP
13	**Learning and evolving**		
13.1	Put in place capabilities and staff - commensurate with the entity's size, business, and risk profile - to gather information on vulnerabilities and cyber threats, incidents, and attacks, and analyze their likely impact on digital operational resilience.	The modules of Netskope's Cloud Exchange integrate cyber security tools with industry-leading threat intel platforms and risk engines to provide up-to-the-minute information on vulnerabilities, threats, incidents, and attacks.	• NG-SWG • Threat Protection • Cloud Exchange
13.2	Conduct incident reviews after significant disruptions to core activities, analyzing the causes of the disruption and identifying required improvements to ICT operations or the Business Continuity Policy. The incident review must evaluate the following controls: 1. promptness in responding to security alerts and determining the severity of their impact, 2. quality and speed in performing forensic analysis, 3. effectiveness of incident escalation within the organization, and 4. effectiveness of internal and external communication.	The Netskope platform can help improve the speed and effectiveness of incident response by collating and reporting on events and generating alerts based on suspicious activity. Analyzing baseline activity and data from previous incidents, Netskope uses Machine Learning and Artificial Intelligence to detect new security events and prompt immediate triage and response.	• NG-SWG • CASB • Public Cloud Security • ZTNA Next • DLP • Advanced Analytics • Device Intelligence

Article	Requirements	Netskope Control	Netskope products
13.3	On a continuous basis, incorporate the following into the Risk Management Framework: 1. lessons learned from operational resilience testing (see Articles 26 and 27) and real world incidents, including any challenges faced in activating the Business Continuity Policy or Incident Response and Recovery Plan, and 2. relevant information exchanged with counterparties and assessed during supervisory reviews. Findings produced as a result of this process must be reported to the entity's managing body on an annual basis.	By integrating data from various security tools, and generating relevant alerts and security tickets, Netskope's Cloud Exchange makes it easier to derive lessons learned and implement policy changes in response. Netskope's Security Posture Management continuously monitors SaaS apps and Public Cloud services to ensure adherence to updated policy configurations.	• Cloud Exchange • CSPM • SSPM
13.4	Monitor the effectiveness of the Risk Management Framework, especially with respect to operational resilience. Map the evolution of cyber risks over time, analyzing the frequency, types, magnitude, and evolution of cyber incidents - especially cyber attacks and their patterns - to accurately assess the level of cyber risk exposure and develop a mature cyber security posture.	Netskope's Cloud Threat Exchange and Cloud Risk Exchange integrate security tools with industry-leading threat intel platforms and risk engines, providing up-to-the-minute information on evolving threats. Netskope Advanced Analytics allows for trend analysis and assessment of frequency, type and evolution of incidents and assists with identifying new patterns and TTP.	• Cloud Exchange • Advanced Analytics
13.5	Senior ICT staff shall report at least yearly to the management body on the findings (see 13.3) and put forward recommendations.	Netskope Advanced Analytics allows for trend analysis and assessment of frequency, type and evolution of incidents and assists with identifying new patterns and anomalies. Advanced analytics included senior management reporting that can be used to identify new and emerging risks.	• Advanced Analytics

Article	Requirements	Netskope Control	Netskope products
13.6	Develop compulsory cyber security awareness programs and digital operational resilience training and incorporate into training schemes for all employees and senior management.	Netskope can reinforce regular awareness training through the use of real-time pop-up notifications whenever a user violates a policy. These pop-up notifications can be implemented flexibly, allowing the customer to warn users before a potential violation occurs, block them entirely from carrying out the action, or provide them with real-time coaching, including suggesting safer alternatives or requesting a justification for the action.	All products
13.7	Monitor technological developments with a view to understanding the impact of deploying such technologies on the entity's ICT security requirements and digital operational resilience. Keep up to date with the latest ICT risk management processes in order to effectively combat current or new forms of cyber attack.	Netskope's Cloud Confidence Index provides up-to-date risk assessments of over 85,000 apps and cloud services. Moreover, the interactive feature allows customized assessments of a given app or service before provisioning, by giving more or less weight to various dimensions of risk depending on an organization's specific needs or tolerances. Netskope's CSPM/SSPM product can help identify latest ICT security requirements for cloud systems and identify misconfigurations. Additionally, Netskope's Cloud Exchange includes Cloud Threat Exchange, an up-to-the-minute threat intelligence feed that can be integrated with other security tools.	• Cloud Exchange • CCI • CSPM • SSPM

Article	Requirements	Netskope Control	Netskope products
15	**Further harmonization of ICT riskmanagement tools, methods, processes and policies** The ESA shall develop common draft regulatory technical standards in consultation with ENISA including: a. ensuring the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the availability, authenticity, integrity and confidentiality of data, including cryptographic techniques, and guarantee an accurate and prompt data transmission without major disruptions and undue delays; b. develop further components of the controls of access management rights referred to in Article 9(4), point (c), and associated human resource policy specifying access rights, procedures for granting and revoking rights, monitoring anomalous behavior in relation to ICT risk through appropriate indicators, including for network use patterns, hours, IT activity and unknown devices; c. develop further the mechanisms specified in Article 10(1) enabling a prompt detection of anomalous activities and the criteria set out in Article 10(2) triggering ICTrelated incident detection and response processes;	Netskope supports alignment with existing standards and frameworks and includes the ability to future-proof to incorporate new technical standards when they are launched. This includes guidance from recognized standards bodies including NIST, CISA, ENISA and many more	All products

Article	Requirements	Netskope Control	Netskope products
16	**Simplified Risk Management Framework for Small and Non-interconnected Enterprises**	**Refer to Articles 5 through 15**	**Refer to Articles 5 through 15**
16.1	Certain small and non-interconnected investment firms, payment institutions, electronic money institutions, and other entities are exempted from the above articles. However, they must still: 1. have a documented ICT risk management framework that covers protection of physical components and infrastructure, and ensures quick, efficient, and comprehensive management of ICT risk; 2. continuously monitor the security and functioning of ICT systems; 3. minimize the impact of ICT risk through the appropriate deployment of sound, resilient, and updated ICT systems, protocols, and tools; 4. promptly identify and detect sources of ICT risk and swiftly handle ICT-related incidents; 5. identify key dependencies on third-party providers; 6. ensure continuity of critical and important functions through business continuity and response and recovery plans, including back-ups and restoration; 7. test these plans on a regular basis; 8. implement lessons learned from such tests, including incorporating those lessons	See above	See above
16.2	The risk management framework should be documented and reviewed on a regular basis, and upon the occurrence of a major ICT-related incident, with a view to continuously improving it by incorporating lessons learned.	See above	See above
16.3	The ESA shall develop common draft regulatory technical standards in consultation with ENISA.	See above	See above

PILLAR II – ICT-RELATED INCIDENT MANAGEMENT, CLASSIFICATION, AND REPORTING

Article	Requirements	Netskope Control	Netskope products
17	**Incident management**		
17.1	Establish and implement an incident management process for detecting, managing, and reporting cybersecurity incidents and put in place early warning indicators as alerts. The incident management process should: 1. establish procedures to identify, track, log, categorize, and classify incidents according to their priority and the severity and criticality of services impacted; 2. assign roles and responsibilities to be activated in different types of incidents and scenarios; 3. set out plans for communication with staff, external stakeholders, the media, and clients, and establish internal escalation procedures, including for handling IT-related customer complaints; 4. ensure major incidents are reported to relevant senior management, explaining their impact, response, and additional controls established as a result; 5. establish incident response procedures to mitigate impacts and ensure timely and secure resumption of business operations.	Netskope's NG-SWG provides customizable alert thresholds for many different kinds of security incidents. The Cloud Log Shipper exports raw event and alert log data and reformats it into a version that can be easily used by security responders. The Cloud Ticket Orchestrator extracts alert logs and associated data and generates appropriate tickets and notifications, streamlining incident response. Netskope's CASB Closed Loop Incident Management functionality facilitates end-to-end incident management from incident creation to resolution. Closed loop workflows help security teams manage incidents by assigning owners, escalating for review, adding tags and notations, and tracking to resolution. Flexible remediation workflows provide security analysts with options to take actions such as notifying users or protecting sensitive data. Detailed forensic and audit trails give security analysts a comprehensive view of each incident - including the user, device, location, app and app instance, specific policy violated, actions taken, and a view of any sensitive data in complete context - ensuring they have complete context to make well-informed decisions. Event-by-event incident history interlaces activities for a given incident, including relevant user activities, policy triggers, and actions taken by admins and analysts to manage and remediate the incident. With a detailed timeline for each incident, analysts and auditors can track progress, confirm, and report on a successful resolution. Expanding beyond predefined admin and analyst roles, Netskope's Role-Based Access Control adds a fine-grained ability to define custom roles by both administrative functions and organizational scope.	All products

Article	Requirements	Netskope Control	Netskope products
17.2	Establish appropriate processes to ensure a consistent and integrated monitoring, handling, and follow-up of incidents, making sure to identify and eradicate root causes to prevent their recurrence.	Netskope's platform includes an in-built ticketing system and reporting to identify the root cause of incidents. In addition, the platform integrates with other tools such as ticketing and SIEM solutions to support ongoing monitoring and forensics aligning to an organization's incident response processes	All products
18	**Incident classification** Classify incidents and determine their impact based on: 1. the number of users or financial counterparts affected, and whether the incident has caused reputational damage; 2. the duration of the incident, including service downtime; 3. the geographic scope of the incident, particularly if it affects more than two Member States; 4. the loss of confidentiality, integrity, or availability of data; 5. the severity of the impact on the entity's ICT systems; 6. the criticality of the services affected; and 7. the economic impact of the incident in both relative and absolute terms.	Netskope's platform includes detailed reporting and advanced analytics to support classification of incidents. Netskope's data protection (DLP) capabilities help identify the number of records impacted (include user or financial data) along with loss of confidentiality, integrity, availability of the data. Advanced analytics can assist with correlating events to identify duration of the incident and the geographic scope (including regions affected). This includes dashboards that may assist with calculating the economic cost of an incident.	All products
19	**Incident reporting**		
19.1	Report major incidents to the competent authority using the reporting template prescribed by that authority. The report must contain all information necessary for the competent authority to determine the significance of the incident and assess any cross-border impacts.	The Netskope platform includes built-in ticketing systems, log analysis, forensic reporting, and advanced analytic capabilities to help respond to a security incident. This includes the ability to identify and assess any cross-border impacts. Forensic data can be analyzed and reports created in multiple formats to support incident notification.	All products

Article	Requirements	Netskope Control	Netskope products
19.3	Notify users and clients, without undue delay, of any major incident that may impact their financial interests. As soon as possible, inform them of all measures that have been taken to mitigate the adverse effects of the incident.	The Netskope platform includes built-in ticketing systems, log analysis, forensic reporting, and advanced analytic capabilities to help respond to a security incident. This includes the ability to identify and assess any cross-border impacts. Forensic data can be analyzed and reports created in multiple formats to support incident notification.	All products
19.4	Timing of notifications: 1. initial report submitted before the end of the business day; 2. intermediate report submitted within one week, with relevant updates thereafter when available; 3. final report once root cause analysis has been completed and impact figures are available, but not later than one month from the submission of the initial report.	The Netskope platform includes built-in ticketing systems, log analysis, forensic reporting, and advanced analytic capabilities to help respond to a security incident. This includes the ability to identify and assess any cross-border impacts. Forensic data can be analyzed and reports created in multiple formats to support incident notification.	All products

PILLAR III – DIGITAL OPERATIONAL RESILIENCE TESTING

Article	Requirements	Netskope Control	Netskope products
24	**General requirements for the performance of digital operational resilience testing**		
24.1	As part of the Risk Management Framework, establish, maintain, and review a sound and comprehensive digital operational resilience testing program, commensurate with the entity's size, business, and risk profile.	The Netskope platform can help both define and harden the attack surface in advance of any digital operational resilience testing. Netskope is limited to devices, web and cloud services but as part of an integrated ecosystem, can support resilience testing including providing connectivity resilience to critical services.	See above
24.2	The digital operational resilience testing programme shall include a range of assessments, tests, methodologies, practices and tools in accordance with Article 25 & 26	The Netskope platform can assist with testing and verification of testing including identifying vulnerabilities and misconfigurations in cloud services, network and device security and scanning of devices and SaaS and IaaS services.	• NG-SWG • CASB • DLP • Public Cloud Security • Cloud Firewall

Article	Requirements	Netskope Control	Netskope products
24.3	Testing must follow a risk-based approach, taking into account the evolving landscape of cyber risks, risks specific to the entity itself, and the criticality of information assets and services impacted by those risks.	The Netskope platform will help identify critical information assets and services. Netskope's NG-SWG and CASB will inventory and classify all managed and unmanaged apps in an ICT ecosystem, including by volume and patterns of usage. The Cloud Confidence Index (CCI) will score those apps based on their risk profiles, including any vulnerabilities or exploits. Meanwhile, Netskope's DLP will discover and protect sensitive data in an ICT environment. Netskope's Cloud Exchange can assist before and during resilience testing. The Cloud Threat Exchange and Cloud Risk Exchange can help identify risky users and assets, and give up to the minute intel on various threats and vulnerabilities. Meanwhile, the Cloud Log Shipper and Cloud Ticket Orchestrator offer a comprehensive, bird's-eye view of any attack - real or simulated - and help streamline a response. Netskope NG-SWG with Advanced Threat Protection, Remote Browser Isolation and Cloud Firewall provide active mitigation against malware, risky websites, phishing, browser attacks, OS vulnerabilities, and firewall egress controls over ports and protocols. Netskope inline policy controls ensure additional restrictions can be enforced in the event of an incident, such as preventing users from accessing certain applications and performing certain actions.	• NG-SWG • CASB • DLP • Public Cloud Security • Cloud Firewall • Cloud Exchange • RBI • ZTNA Next
24.4	Testing must be done by independent parties, whether internal or external.	If testing is done internally, Netskope can help define scope by inventorying both managed and unmanaged apps and devices in an ICT environment, and assigning risk-based scores.	• NG-SWG • CASB • Public Cloud Security
24.5	Establish procedures and policies to prioritize, classify, and remedy all issues acknowledged throughout the performance of the tests. Establish internal validation methodologies to ascertain that all identified weaknesses, deficiencies, or gaps are fully addressed.	Netskope's Cloud Security Posture Management and SaaS Security Posture Management continuously monitor IaaS platforms and SaaS apps and can automatically remediate any misconfigurations aligned to policies or industry standards.	• CSPM • SSPM

Article	Requirements	Netskope Control	Netskope products
24.6	Critical ICT systems and applications must be tested at least once per year.	The Netskope platform can help define the scope of critical ICT systems and applications. The NG-SWG, CASB, and Cloud Confidence Index will advise which SaaS apps - including unmanaged apps - are critical to day-to-day operations, and assign them a risk profile to make mitigation easier. Netskope's Cloud Security Posture Management and SaaS Security Posture Management can also help identify where "configuration drift" is most likely to occur in IaaS platforms and SaaS apps	• NG-SWG • CASB • CCI • CSPM • SSPM
25	**Testing of ICT tools and systems** The digital operational resilience testing program must include a full range of appropriate tests, including: 1. vulnerability assessments and scans; 2. open source analyses; 3. network security assessments; 4. gap analyses; 5. physical security reviews; 6. questionnaires and scanning software solutions; 7. source code reviews where feasible; 8. table-top exercises; 9. compatibility testing; 10. performance testing; 11. end-to-end testing; or 12. penetration testing	The Netskope platform can assist with testing and verification of testing including identifying vulnerabilities and misconfigurations in cloud services, network and device security and scanning of devices and SaaS and IaaS services.	• NG-SWG • CASB • DLP • Public Cloud Security • Cloud Firewall

Article	Requirements	Netskope Control	Netskope products
26	**Advanced testing of tools, systems, and processes based on threat-led penetration testing (TLPT)**		
26.2	Threat-led penetration testing must at least cover the entity's critical functions and services, and be performed on live production systems supporting such functions. Third-party ICT vendors included in the remit of the penetration testing should also participate whenever feasible. Apply effective risk management controls to reduce risks to data, damage to assets, and disruption to critical services or operations during testing. Provide documentation of threat led penetration testing to the competent authorities.	Netskope's NG-SWG, CASB and Public Cloud Security tools can inventory all managed and unmanaged applications in an ICT environment, allowing organizations to assess the criticality of various services to business operations, as well as risk profiles.	• NG-SWG • CASB • Public Cloud Security • CCI • CSPM • SSPM
26.3	Ensure the participation of ICT-third party service providers in the TLPT and retain at all times full responsibility for ensuring compliance with the regulation	Netskope provides organizations with a list of ICT-third party cloud service providers in use including a composite score (CCI) of their security and privacy credentials. Details including recent breaches also affect the CCI score and organizations can report on any changes and maintain a form of responsibility and reporting for their cloud providers.	• NG-SWG • CASB • Public Cloud Security • CCI • CSPM • SSPM
27	**Requirements for testers** 2c.Ensure threat intelligence provider is external to the financial entity	To support internal testers, Netskopecan provide threat intelligence that is external to the financial entity including details of compromised accounts and new malware/ransomware signatures along with detection of signatureless malware. Additional threat indicators can be consumed and shared across the ecosystem.	• Threat Protection • Cloud Exchange

PILLAR IV – MANAGING OF ICT THIRD-PARTY RISK

Article	Requirements	Netskope Control	Netskope products
28	**General principles**		
28.1	Third party risk management shall be implemented in light of the principle of proportionality, taking into account: 1. the scale, complexity, and importance of IT-related dependencies; and 2. risks arising from contractual arrangements with third party ICT vendors, taking into account the criticality or importance of the service, process, or function, and the potential impact on the continuity and quality of financial services activities.	Netskope's NG-SWG and CASB can identify managed and unmanaged apps in an environment. The Cloud Confidence Index provides important details for assessing the risks associated with any given app or cloud service, including the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more.	• NG-SWG • CASB • Public Cloud Security • CCI
28.2	The Risk Management Framework shall include a strategy for mitigating third party risk that will: 1. define a holistic multi-vendor strategy showing key dependencies on third party service providers and explain the rationale behind the procurement mix of third party service providers; and 2. be reviewed on a regular basis, with a view to identifying risks created by outsourcing critical or important functions.	Netskope's platform can support a multivendor strategy by identifying all SaaS apps and IaaS platforms in use in an environment, and using Netskope's Cloud Confidence Index to quantify the overall organizational risk they pose. Additional regular reviews can be performed using security posture management tools to ensure cloud services are adequately and securely configured.	• CASB • Public Cloud Security • CSPM • SSPM

Article	Requirements	Netskope Control	Netskope products
28.3	Maintain and update a Register of Information containing all contractual arrangements with third party ICT vendors. Distinguish between contractual arrangements that cover critical or important functions and those that do not. Report annually to the competent authorities on the number of new arrangements for ICT services, the categories of the third party service providers, the type of contractual arrangements, and the services and functions being provided. Furnish the Register of Information, or specified sections thereof, to the competent authority upon request. Inform the competent authority of any planned contracting of critical or important functions, and when a function becomes critical or important.	Netskope's NG-SWG, CASB and Public Cloud Security service can be used to inventory and categorize tens of thousands of web and cloud apps, enabling the customer to cross-reference with its Register of Information to ensure accuracy of reporting. Integrations exist with GRC and inventory tools to automatically populate and maintain a register of information including what data is being stored/ processed and location of service (GeoIP) These tools can also be used to discover unmanaged apps (Shadow IT), and redundant services, permitting the consolidation of cloud services.	• NG-SWG • CASB • CCI • Public Cloud Security
28.4	Before entering into a contractual arrangement: 1. assess whether it covers a critical or important function; 2. determine whether supervisory conditions for contracting are met; 3. identify and assess all relevant risks in relation to the contractual arrangement, including the possibility that such arrangements may contribute to reinforcing the risk of dependency on a small number of critical third party providers. 4. perform due diligence to determine the suitability of the third party provider; and 5. identify and assess any potential conflicts of interest.	Netskope's platform can assist in performing due diligence and vendor assurance for cloud services across various categories, including cloud storage, HR, CRM, marketing, and more. This is through the Cloud Confidence Index (CCI). CASB, CCI and DLP can assist in identifying if critical data is being stored in what cloud service and what general terms are applied to protecting the data.	• CASB • CCI • Public Cloud Security

Article	Requirements	Netskope Control	Netskope products
28.5	Contractual arrangements with third party ICT vendors must comply with high, appropriate, and latest information security standards.	Netskope can help identify what security standards cloud service providers follow and include this information in reports aligned to each supplier. Alerting and reporting can also be enabled to ensure if a Third-Party ICT vendor fails to recertify to a certain standard, their CCI score is directly affected.	• CASB • CCI • Public Cloud Security
28.6	Using a risk-based approach, and adhering to commonly accepted audit standards, determine the frequency of audits of third party service providers, and the areas to be audited.	The Netskope platform helps identify all managed and unmanaged cloud apps and services in an ICT environment, including those supplied by third party vendors. Using Netskope's Cloud Confidence Index (CCI), organizations can determine the appropriate frequency of audits of third party vendors based on their risk profiles and criticality to the enterprise's day-to-day operations.	• NG-SWG • CASB • Public Cloud Security • CCI
28.7	Ensure that contractual arrangements with ICT service providers are terminated at least under the following circumstances: 1. breach by the third party provider of applicable laws, regulations, or contractual terms; 2. circumstances identified through monitoring of third party risk which are deemed capable of altering the performance of the functions provided through the arrangement, including material changes that affect the arrangement or the situation of the third party provider; 3. the third party provider's evident weaknesses in its overall cyber risk management, and in particular the way it ensures the security and integrity of confidential, personal, or otherwise sensitive data; and 4. where the competent authority can no longer effectively supervise the entity as a result of the contractual arrangement.	The Netskope platform helps identify all managed and unmanaged cloud apps and services in an ICT environment, including those supplied by third party vendors. Using Netskope's Cloud Confidence Index (CCI), organizations can determine the appropriate frequency of audits of third party vendors based on their risk profiles and criticality to the enterprise's day-to-day operations. Alerting and reporting can also be enabled to ensure if a Third-Party ICT vendor fails to recertify to a certain standard or suffers a breach, their CCI score is directly affected.	• NG-SWG • CASB • Public Cloud Security • CCI

Article	Requirements	Netskope Control	Netskope products
28.8	Put in place comprehensive and documented exit strategies taking into account risks that may emerge at the level of the third party provider. Ensure the ability to exit contractual arrangements with third party providers without disruption to business activities, limiting compliance with regulatory requirements, or detriment to the continuity and quality of business services. Identify alternative solutions and develop transition plans to remove the contracted functions and relevant data from the third party provider and transfer them to alternative providers or return them in-house.	The Netskope platform can help identify managed and unmanaged cloud apps and services in an ICT environment, including those supplied by third party vendors. Using Netskope's Cloud Confidence Index (CCI), organizations can measure certain attributes to support termination decisions and transition plans including: – Data ownership – Download data upon termination – Delete data upon cancellation	• NG-SWG • CASB • Public Cloud Security • CCI
29	**Preliminary assessment of concentration risk and further suboutsourcing arrangements**		
29.1	When identifying and assessing risk related to dependency on a small number of critical third party providers, take into account whether the conclusion of a contractual arrangement would lead to: 1. contracting with a third party provider which is not easily substitutable; or 2. having in place multiple contractual arrangements in relation to the provision of ICT services with the same third party provider or closely connected third party providers.	The Netskope platform can help identify managed and unmanaged cloud apps and services in an ICT environment, including those supplied by third party vendors. Using Netskope's Cloud Confidence Index (CCI), organizations can determine the appropriate frequency of audits of third party vendors based on their risk profiles and criticality to the enterprise's day-to-day operations.	• NG-SWG • CASB • Public Cloud Security

Article	Requirements	Netskope Control	Netskope products
29.2	Weigh the benefits and risks of any contractual arrangement with third party ICT providers that includes the possibility that the third party further sub-contracts a critical or important function to other third party providers. For third party ICT providers established in a third-country, consider that jurisdiction's respect for data protection, effective enforcement of the law, insolvency law provisions that would apply in the event of the third party's bankruptcy, and any constraints that may impede the recovery of the financial entity's data. Assess whether and how potentially long or complex chains of subcontracting may impact the ability to fully monitor the contracted functions, and consequently the ability of the competent authority to supervise the entity.	The Netskope platform can help identify managed and unmanaged cloud apps and services in an ICT environment, including those supplied by third party vendors. In addition, using certain metadata, it's also possible that certain attributes may help assist the identification of fourth party providers i.e. public cloud services. Using Netskope's Cloud Confidence Index (CCI), organizations can measure certain attributes to support termination decisions and transition plans including: – Data ownership – Download data upon termination – Delete data upon cancellation	• NG-SWG • CASB • Public Cloud Security
30	**Key contractual provisions**		
30.1	Clearly allocate and set out in a single writing all rights and obligations of the financial entity and the third party ICT service provider, including all service level agreements. Maintain the document on paper or in a downloadable or accessible format.	Netskope's standard Subscription Services Agreement complies with this requirement.	All products

Article	Requirements	Netskope Control	Netskope products
30.2	Include the following provisions in any contractual arrangement: 1. a clear and complete description of all functions and services to be provided by the third party provider, indicating whether sub-contracting of a critical or important function, or material parts thereof, is permitted, and under what conditions; 2. locations where the contracted or subcontracted functions and services are to be provided and where data is to be processed, including the storage location, and the requirement for the third party provider to notify the entity if it envisages changing such locations; 3. provisions on accessibility, availability, integrity, security and protection of personal data; 4. provisions on ensuring access, recovery, and return in an easily accessible format of personal and non-personal data processed by the financial entity in the case of insolvency, resolution, or discontinuation of the third party provider's business operations; 5. full service level descriptions, including updates and revisions thereof; 6. the obligation of the ICT thirdparty service provider to provide assistance in case of an ICT incident at no additional cost or at a cost that is determined exante; 7. the obligation of the ICT-third party service provider to fully cooperate with the competent authorities and resolution authorities of the financial entity, including persons appointed by them; 8. termination rights and related minimum notices period for the termination of the contract, in accordance with competent authorities' expectations; 9. the conditions for the participation of ICT third-party providers in the entity's ICT security awareness programs and digital operational resilience training;	Netskope's standard Subscription Services Agreement complies with these requirements.	All products

Article	Requirements	Netskope Control	Netskope products
30.3	In addition to the key provisions above, contractual arrangements for ICT services supporting critical or important functions must also include the following: 1. full service level descriptions, including updates and revisions thereof, and precise quantitative and qualitative performance targets within the agreed service levels to allow an effective monitoring by the financial entity and enable without undue delay appropriate corrective actions when agreed service levels are not met; 2. notice periods and reporting obligations of the ICT third-party service provider to the financial entity, including notification of any development which may have a material impact on the ICT third-party service provider's ability to effectively carry out critical or important functions in line with agreed service levels; 3. requirements for the ICT thirdparty service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies which adequately guarantee a secure provision of services by the financial entity in line with its regulatory framework; 4. The obligation of the ICT thirdparty provider to participate and fully cooperate in the financial entity's threat led penetration testing;	Netskope's standard Subscription Services Agreement complies with these requirements.	All products

Article	Requirements	Netskope Control	Netskope products
30.3 cont	5. the right to monitor on an ongoing basis the ICT third-party service provider's performance, which includes: i) rights of access, inspection and audit by the financial entity or by an appointed third-party, and the right to take copies of relevant documentation, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies; ii) the right to agree alternative assurance levels if other clients' rights are affected; iii) the commitment to fully cooperate during the onsite inspections performed by the financial entity and details on the scope, modalities and frequency of remote audits; 6. exit strategies, in particular the establishment of a mandatory adequate transition period: (i) during which the ICT third-party service provider will continue providing the respective functions or services with a view to reduce the risk of disruptions at the financial entity; (ii) which allows the financial entity to switch to another ICT thirdparty service provider or change to on-premises solutions consistent with the complexity of the provided service.		
30.4	Consider using standard contractual clauses developed for specific services.	Netskope's Data Processing Addendum (DPA) includes Standard Contractual Clauses to ensure GDPR-compliant data processing.	All products

PILLAR V – INFORMATION SHARING ARRANGEMENTS

Article	Requirements	Netskope Control	Netskope products
45	**Information-sharing arrangements on cyber threat information and intelligence**		
45.1	Permits the voluntary sharing of cyber threat information and intelligence among financial entities, including indicators of compromise, tactics, techniques, procedures, cyber security alerts, and configuration tools provided such sharing: 1. is for the purpose of enhancing the entities' digital operational resilience; 2. takes place within trusted communities; and 3. is implemented through information sharing agreements	With Netskope's Cloud Threat Exchange and Cloud Risk Exchange, security tools can be integrated with industry-leading threat intel platforms and risk engines, providing up-to-the-minute information to enhance security posture.	• Cloud Exchange

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.