netskope

Compliance Series

Using the Netskope Platform to Support Compliance with the

Australian Prudential Standard CPS 234 Information Security

TABLE OF CONTENTS

INTRODUCTION 3

NETSKOPE PRODUCTS OVERVIEW 5

HOW TO USE THIS GUIDE 17

NETSKOPE PRODUCTS 20

PRUDENTIAL STANDARD CPS 234 INFORMATION SECURITY 26

INTRODUCTION

The Australian Prudential Standard CPS 234 Information Security aims to ensure that Australian Prudential Regulation Authority (APRA) regulated entities establish and maintain robust information security measures to protect against incidents, including cyberattacks, by developing capabilities that address relevant vulnerabilities and threats. A key objective is to reduce the likelihood and impact of security incidents on the confidentiality, integrity, and availability of information assets, including those managed by third parties or related entities.

The Australian Prudential Standard applies to all APRA regulated entities, which include authorised deposit-taking institutions (ADIs), foreign ADIs, and non-operating holding companies (NOHCs) authorised under the Banking Act; general insurers, Category C insurers, authorised insurance NOHCs, and parent entities of Level 2 insurance groups under the Insurance Act; life companies, friendly societies, eligible foreign life insurance companies (EFLICs), and registered life NOHCs under the Life Insurance Act; private health insurers registered under the PHIPS Act; and RSE licensees under the SIS Act concerning their business operations.

The obligations for foreign ADIs, Category C insurers, and EFLICs apply only to their Australian branch operations. If an APRA-regulated entity is the Head of a group, it must comply with this Prudential Standard as an individual entity, ensure the requirements are applied throughout the group (including to non-APRA-regulated entities), and on a group-wide basis.

The key requirements of this Prudential Standard mandate that an APRA-regulated entity must clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies, and individuals. It must also maintain an information security capability that is proportionate to the size and threat level to its information assets, ensuring the continued sound operation of the entity. Additionally, the entity must implement controls to protect its information assets based on their criticality and sensitivity, conduct systematic testing and assurance of these controls' effectiveness, and notify APRA of any material information security incidents.

The official link for the standards is available here.

NETSKOPE PRODUCTS OVERVIEW

Netskope's products can be leveraged as a technical control to assist organisations in meeting the requirements of Australian Prudential Standard CPS 234, which focuses on information security, through several key features and capabilities:

Data Protection:

Data Loss Prevention (DLP): Netskope offers advanced DLP functionality that monitors and safeguards sensitive data, particularly in the cloud, helping organisations prevent unauthorised access, sharing, or transfer of critical information. This supports compliance with CPS 234's requirements to protect data from information security vulnerabilities and breaches.

Encryption and Tokenization: Netskope ensures that sensitive data is encrypted both in transit and at rest, reducing the risk of data breaches. This aligns with CPS 234's focus on maintaining appropriate controls over sensitive information to protect against potential cyber threats.

Visibility and Control:

Cloud Activity Monitoring: Netskope provides real-time visibility into cloud service usage and data movement, enabling organisations to maintain oversight of sensitive data and assist in compliance with CPS 234's requirement to monitor and manage information security risks effectively.

User and Entity Behavior Analytics (UEBA): By analysing user behaviour, Netskope detects anomalies and suspicious activity that may indicate security risks or breaches, helping organisations quickly address potential threats in accordance with CPS 234's incident detection and response guidelines, as well as residency policies, ensuring that sensitive data is stored and processed within specific regions, which can be critical for complying with APRA's expectations regarding data sovereignty and the handling of information assets.

Risk Management:

Risk Assessment: Netskope assesses the security posture of cloud services and applications, helping organisations identify and address risks that may affect their information assets.

Compliance Reporting: The platform offers detailed reports and audit trails, helping organisations demonstrate adherence to CPS 234. These reports facilitate regular security reviews, audits, and support responses to regulatory oversight.

Incident Response:

Threat Protection: Netskope provides protection against malware and other cyber threats, reducing the likelihood of incidents that could compromise sensitive information, a key aspect of CPS 234's focus on incident prevention.

Automated Incident Response: In case of a security incident, Netskope automates response actions, such as alerting relevant teams and restricting access to prevent further damage. This supports CPS 234's emphasis on prompt detection and rapid response to information security incidents.

Data Residency and Sovereignty:

Data Localization: Netskope enables organisations to enforce data residency policies, ensuring that sensitive data is stored and processed within specific regions, which can be critical for complying with APRA's expectations regarding data sovereignty and the handling of information assets.

By offering these capabilities, Netskope assists organisations in meeting the stringent requirements of CPS 234, strengthening their information security posture, mitigating risks, and ensuring the protection of critical data assets.

HOW TO USE THIS GUIDE

The Netskope platform consists of a suite of tools integrated into a unified Secure Access Service Edge (SASE) architecture. This SASE architecture's capabilities provide robust controls to support compliance with the Australian Prudential Standard CPS 234. The tools are designed to secure critical data, monitor security incidents, and alert stakeholders to any potential breaches or weaknesses in security controls, ensuring timely remediation.

The tables below outline key sections of CPS 234 and offer guidance on how Netskope's products can assist regulated entities in meeting their information security obligations and the ongoing management of security risks.

NETSKOPE PRODUCTS

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

Industry Terminology	Netskope Product Line/Abbreviation
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)
User Risk Metrics	User Confidence Index (UCI)

PRUDENTIAL STANDARD CPS 234 INFORMATION SECURITY

Requirements(s)	Netskope Response	Products
1 to 12 - Authority, Application, Interpretation, Adjustments, and Exclusions	Sections 1 to 12 set out the provisions related to Authority, Application, Interpretation, Adjustments and Exclusions, and Definitions. Netskope's products do not directly map to these sections.	
12 - Definitions	Section 12 provides key definitions of relevant terms. Netskope's products do not directly map to these sections.	
13 - Maintenance of Information security	Netskope provides comprehensive security solutions that can help an APRA-regulated entity's board ensure robust information security practices. By enforcing customizable cybersecurity and data privacy policies tailored to organizational risk and regulatory requirements, Netskope helps safeguard information assets. The Cloud Confidence Index (CCI) offers a risk assessment of SaaS applications, considering criteria like security policies, certifications, and legal concerns, aiding the board in evaluating potential threats to information security. Netskope's Cloud Access Security Broker (CASB) enhances visibility and control by monitoring and logging SaaS and IaaS activities, while applying real-time data loss prevention controls. This can help the board maintain oversight of activity-level security, ensuring alignment with organizational policies. Additionally, CASB aids in asset inventory and third-party risk management, crucial for a sound operational strategy. Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) provide continuous monitoring to prevent misconfigurations and ensure compliance with access management policies and industry standards. By preventing data exfiltration and integrating with Cloud Ticket Orchestrator for automated remediation, these tools improve the sound operation of the entity. Advanced Analytics further supports the board by offering insights into data flows and security trends, allowing tracking of access and threats to strengthen security postures.	• All products • CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • SSPM • Advanced Analytics • CTO
14 - Roles and Responsibilities	Section 14 sets out the roles and responsibilities with respect to implementing and maintaining information security for APRA-regulated entities. Netskope's products do not directly map to this section.	• CASB • NG-SWG • Public Cloud Security • DLP • CSPM • SSPM • CTO

Requirements(s)	Netskope Response	Products
15 - Information Security Capability	Netskope offers comprehensive network security solutions that ensure compliance with industry standards, assisting APRA-regulated entities in maintaining robust information security capabilities. The platform supports a defense-in-depth strategy, optimizing the independence and efficiency of security layers. Netskope's Cloud Confidence Index helps businesses evaluate SaaS risks, providing insights into vendor security practices and legal concerns. The Cloud Access Security Broker (CASB) enables detailed monitoring of SaaS and IaaS activities, applying real-time controls to prevent data loss and enhance policy compliance. In terms of asset management, Netskope facilitates the identification of managed and unmanaged apps, assessing their risk levels and criticality. Its Cloud and SaaS Security Posture Management tools continuously monitor for misconfigurations and automate remediation, aligning operations with regulatory requirements and organization policies. ZTNANext secures remote access with zero trust principles, integrating with identity providers to ensure encrypted data transmission and precise access controls. For entities addressing insider threats, Advanced User Entity and Behavior Analytics leverages machine learning for anomaly detection and risk assessment, while Device Intelligence employs AI to manage device access securely. Moreover, Netskope's Advanced Analytics offers data flow mapping and risk assessment, helping organizations manage threats and maintain sound operation by providing detailed insights into cloud app usage and security trends.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • SSPM • ZTNA Next • Advanced Analytics • Advanced UEBA • Device Intelligence • CTO

Requirements(s)	Netskope Response	Products
16 - Information Security Capability with Respect to Third Parties	Netskope provides comprehensive solutions for assessing and managing the security risks of SaaS and IaaS platforms, which can aid APRA-regulated entities in evaluating third-party information security capabilities. With its Cloud Confidence Index (CCI), Netskope scores SaaS applications, offering insights into the security posture of various vendors based on factors like security policies, certifications, and legal concerns. Its Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) tools continuously monitor critical IaaS and SaaS platforms. These tools help prevent misconfigurations and ensure compliance with organizational and regulatory standards, aiding in the safe management of information assets. They also integrate with Netskope's Cloud Ticket Orchestrator to automate alert generation and remediation. Moreover, SSPM's proactive alerting and customizable remediation instructions ensure swift response to potential security issues, and the ability to convert past misconfigurations into new security rules enhances overall security measures. These capabilities allow APRA-regulated entities to effectively assess and improve the information security capabilities of third-party vendors, helping to mitigate potential security incidents.	• CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • CTO • Threat Protection
17 - Information Security Capability with Respect to Vulnerabilities and Threats	Netskope provides comprehensive security solutions including its threat protection product capabilities designed to assist APRA-regulated entities maintain robust information security capabilities in the face of evolving threats and vulnerabilities. The company's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) tools continuously monitor IaaS and SaaS environments for misconfigurations, ensuring compliance with organizational and regulatory standards. These tools send alerts, automate remediation, and integrate with Netskope's Cloud Ticket Orchestrator to streamline response efforts, significantly reducing the risk of data breaches and misuse. Netskope's Device Intelligence uses AI/ML to identify, classify, and monitor all devices on a network, establishing behavioral baselines to detect anomalies and isolate risky devices, thereby aligning with zero trust principles. Its Advanced Analytics tool maps data flows, assesses cloud risk, and helps administrators track security trends, enhancing visibility and control over information assets. Further, Netskope's Cloud Risk Exchange and Cloud Threat Exchange components facilitate risk assessment and threat sharing, ensuring adaptive controls are enforced and allowing integration with third-party security tools. These capabilities support APRA-regulated entities in actively adapting their security posture to counter changing threats and vulnerabilities.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • SSPM • CRE • CTE • CTO • Threat Protection

Requirements(s)	Netskope Response	Products
18 - Policy Framework - Vulnerability Management	Netskope assists organizations in implementing a network security architecture that's aligned with industry-recognized cybersecurity and data privacy best practices. This includes a "defense-in-depth" strategy that minimizes interactions between security layers, allowing them to function independently. Properly customized and configured, the Netskope platform addresses risk to organizational operations, assets, individuals, and third parties. Netskope can enforce cybersecurity and data privacy policies defined by the organization. Policies can be customized, configured, and automated based on risk and regulatory requirements. Netskope additionally can assist communication and track acknowledgement of policies through implementation of pop-up banners/coaching pages across its products that can notify employees of potential policy infringements in line with organizational requirements. Netskope's products can assist in implementing security functions such as layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers. Netskope's CASB can assist with asset inventory, acquisition strategy, third-party risk management, and business continuity planning by identifying and inventorying managed and unmanaged apps and cloud services in the organization's IT ecosystem, and assessing their criticality based on usage and risk level. Netskope's ZTNA Next provides remote access to on-prem or cloud-hosted private apps from any device, anywhere. ZTNA Next integrates with NIST-compliant third-party identity providers to support secure authentication, uses end-to-end encryption to secure data in use and in motion, and applies granular controls to limit access and privileges based on zero trust principles. ZTNA Next logs all access attempts and can enforce organizational policies regarding failed login attempts. Overall, Netskope's suite of services helps entities comply with APRA requirements by strengthening their security posture and policy framework.	• All products • CASB • NG-SWG • SD-WAN • ZTNA Next • Threat Protection
19 - Policy Framework- Direction on Responsibilities	Section 19 requires an APRA-regulated entity's information security policy framework to provide direction on the responsibilities of all parties who have an obligation to maintain information security. Netskope's products do not directly map to this section.	

Requirements(s)	Netskope Response	Products
20 - Information Asset Identification and Classification	Netskope's Cloud Confidence Index (CCI) helps organizations assess the risk of SaaS applications by evaluating security policies, certifications, and legal concerns. It aids APRA-regulated entities in classifying information assets based on criticality and sensitivity. Netskope's Data Loss Prevention (DLP) engine provides comprehensive data security across web, cloud applications, and devices, safeguarding data in use, transit, or rest with machine learning-driven identification and classification. The context-aware policies enable real-time data protection by considering users, devices, apps, networks, and actions. This supports asset classification required by APRA, as DLP can obfuscate, encrypt, or block actions to protect sensitive information, ensuring that incidents don't compromise entity or customer interests. Additionally, Netskope's solutions incorporate Role-Based Access Control (RBAC) across its CASB, NG-SWG, and ZTNA Next services, advocating for the least-privilege principle, enhancing security, and facilitating compliance with APRA restrictions. DLP enforces RBAC to enable organizations to manage access during incident response, recover data integrity, and support continuous monitoring and forensic investigations. This suite of services provides tools to manage data classification, access control, and risk reduction for critical and sensitive information assets under APRA guidelines.	• CASB • NG-SWG • Cloud Confidence Index (CCI) • DLP • ZTNA Next
21 - Implementation of Security Controls	Netskope offers comprehensive cybersecurity solutions that align with APRA regulations by providing robust information security controls. Their Cloud Access Security Broker (CASB) and Next Generation Secure Web Gateway (NG-SWG) services support industry-recognized practices in cybersecurity and data privacy, enabling organizations to monitor, log, and control activities across SaaS, IaaS, and various network platforms. Netskope's Data Loss Prevention (DLP) engine uses machine learning to classify and protect sensitive data, ensuring compliance with organizational policies and regulatory requirements. It offers real-time protection and supports role-based access control, enforcing the least-privilege principle. Netskope's Cloud Security Posture Management and SaaS Security Posture Management continuously monitor for misconfigurations and facilitate automated remediation to minimize vulnerabilities and threats to information assets. These tools also assess the criticality and sensitivity of applications, aiding in business continuity planning and third-party risk management. Netskope's Device Intelligence and Cloud Threat Exchange enhance security by managing network-connected devices and sharing threat indicators in real time. This comprehensive approach ensures that security controls are timely and appropriate for the information assets' life-cycle stage and potential incident impacts, maintaining the integrity and confidentiality of critical data.	• All products • CASB • NG-SWG • Public Cloud Security • CSPM • DLP • SSPM • ZTNA Next • Device Intelligence • CTE • CTO

Requirements(s)	Netskope Response	Products
22 - Security Controls of Related Third Parties	Netskope offers comprehensive tools that can aid APRA-regulated entities in evaluating the information security controls of third-party providers. Its Cloud Confidence Index (CCI) assesses SaaS applications, helping organizations gauge the risks associated with different vendors' applications or services. Key evaluation criteria include the vendor's security policies, certifications, and privacy concerns. Netskope's CASB and NG-SWG, featuring a robust Data Loss Prevention (DLP) engine, ensure data security across various environments, using machine learning to safeguard sensitive information based on specific policies. DLP facilitates real-time data protection and supports role-based access, aiding in incident response and recovery. Through seamless integration with security information and event management (SIEM) tools, Netskope's CASB supports automated incident response, enhancing security oversight. Its Cloud Security Posture Management actively monitors IaaS platforms to prevent misconfigurations and potential data breaches, ensuring compliance with organizational and regulatory standards. Similarly, the SaaS Security Posture Management prevents SaaS misconfigurations while enabling automated remediation through integration with Cloud Ticket Orchestrator. These capabilities help APRA-regulated entities ensure that their third-party partners maintain robust information security controls, protecting valuable information assets effectively.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • DLP • SSPM • CTO
23 - Detecting and Responding to Information Security Incidents	Netskope offers robust mechanisms ideal for APRA-regulated entities to detect and respond to information security incidents promptly. Their products provide detailed insights and rich metadata for traffic across web, SaaS, IaaS, and public-facing custom apps, helping estimate the magnitude of a cyber incident, such as identifying impacted systems, users, data, and services. Netskope's Next Generation Secure Web Gateway (NG-SWG) integrates with NIST-compliant identity providers and extends SSO/MFA protections across managed and unmanaged apps. It decodes over 100 inline activities to detect anomalies and applies context-aware controls, such as stepped-up authentication or user notifications, for risky behaviors. NG-SWG's comprehensive logging and policy enforcement ensure detailed insights and user action non-repudiation, aiding incident response. Netskope's Cloud Log Shipper exports logs for integration with SIEM tools, enhancing incident analysis, while the Cloud Ticket Orchestrator automates response workflows, including role-based access control enforcement during incidents. Together, these features support APRA-regulated entities in establishing effective incident detection and swift response mechanisms, vital for regulatory compliance and maintaining security posture.	• All products • NG-SWG • Advanced Analytics • CLS • CTO

Requirements(s)	Netskope Response	Products
24 - Maintaining Plans to Respond to Information Security Incidnet	Section 24 requires an APRA-regulated entity's maintain incident response plans. Netskope's products do not directly map to this section.	
25 - Information Security Response Plans	Section 25 requires an APRA-regulated entity's maintain incident response plans. Netskope's products do not directly map to this section.	
26 - Annual Review and Test of Information Security Response Plans	Netskope offers comprehensive security solutions that can help APRA-regulated entities effectively review and test their information security response plans. Netskope's Cloud Access Security Broker (CASB) generates alerts and exports them to a security information and event management (SIEM) tool, facilitating automated incident response and recovery. This supports regular testing of response plans by providing real-time incident data and actions. Additionally, event logs from Netskope's tools can be used to perform lessons learned and generate progress reports, aiding in the evaluation of plan effectiveness. The Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) continuously monitor for misconfigurations and ensure compliance with organizational and regulatory standards. These tools send alerts and automate remediation, keeping security plans up to date and functional. By integrating with the Cloud Ticket Orchestrator, they streamline incident response workflows and automate service ticket generation. Netskope's Next Generation Secure Web Gateway (NG-SWG) applies granular policy controls and alerts on anomalous behavior, with detailed logging that assists in asserting non-repudiation. The Cloud Log Shipper exports logs to SIEM tools, supporting ongoing testing and refinement of security plans. Overall, Netskope's suite of tools provides robust support for maintaining effective and fit-for-purpose security response plans.	• CASB • NG-SWG • Public Cloud Security • CSPM • SSPM • CLS • CTO
27 - Testing Control Effectiveness	Section 27 requires an APRA-regulated entity to test effectiveness of its security controls. Netskope's products do not directly map to this section.	
28 - Testing Control Effectiveness of Related Third Parties	Section 28 requires an APRA-regulated entity to test effectiveness of its third-party security controls. Netskope's products do not directly map to this section.	
29 - Reporting to Board	Section 29 requires an APRA-regulated entity's obligations to identify and report information security control deficiencies that cannot be remediated in a timely manner. Netskope's products do not directly map to this section.	
30 - Method of Testing Control Effectiveness	Section 30 requires an APRA-regulated entity's obligations to ensure that testing is conducted by appropriately skilled and functionally independent specialists. Netskope's products do not directly map to this section.	

Requirements(s)	Netskope Response	Products
31 - Sufficiency of Testing Control Effectiveness	Section 31 requires an APRA-regulated entity's obligations to review the sufficiency of the testing program. Netskope's products do not directly map to this section.	
32 - Internal Audit	Netskope's solutions are valuable for APRA-regulated entities needing to ensure robust information security control assurance, especially in internal audits. Netskope's Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) continuously monitor mission-critical IaaS and SaaS platforms for misconfigurations against organizational policies and regulatory standards. This ensures that information security controls are appropriately designed and operating effectively, aligning with internal audit requirements. CSPM and SSPM automatically scan for potential issues, send alerts, and initiate remediation tasks, enhancing security control assurance through immediate corrective measures. Integration with Netskope's Cloud Ticket Orchestrator facilitates automated incident response and remediation, streamlining audits and compliance efforts. The CASB logs events, which are useful for incident analysis and generating reports like Progress and Action On Milestones, helping the internal audit review by providing clear evidence of security control performance. Additionally, the conversion of detected misconfigurations into new rules aids continuous improvement, strengthening the information security framework. Overall, Netskope's solutions support APRA-regulated entities by enhancing the design and operational efficacy of their information security controls, including third-party oversight, as required in audits.	• CASB • Public Cloud Security • CSPM • SSPM • CTO
33 - Provision of Skilled Personnel (Audit)	Netskope's solutions ensure robust information security control assurance, aligning with APRA's requirements for skilled personnel. The Cloud Access Security Broker (CASB) alerts and exports event data to security information and event management (SIEM) tools, facilitating automated incident response and enabling skilled personnel to perform detailed lessons learned analyses. Cloud Security Posture Management (CSPM) continuously monitors critical IaaS platforms to prevent misconfigurations and ensure compliance with access policies and regulatory standards. Its integration with Netskope's Cloud Ticket Orchestrator allows skilled teams to automate remediation, addressing potential threats swiftly. Regular scanning of cloud storage prevents data exfiltration, further supporting secure operations. On the SaaS front, Netskope's Security Posture Management prevents misconfigurations of mission-critical functions and provides actionable remediation instructions. Integrating SSPM with the Cloud Ticket Orchestrator further aids in automating responses to detected issues. By converting past discoveries into new security rules, Netskope enhances ongoing protection. Collectively, these capabilities allow an APRA-regulated entity to ensure that information security controls are consistently reviewed, updated, and assured by appropriately skilled personnel, meeting regulatory expectations.	• CASB • Public Cloud Security • CSPM • SSPM • CTO

Requirements(s)	Netskope Response	Products
34 - Internal Audit Functions	Section 34 requires an APRA-regulated entity's obligations related to internal audits functions. Netskope's products do not directly map to this section.	
35- Notifying Information Security Incident	Netskope's solutions can support APRA-regulated entities in managing information security incidents. Netskope's Cloud Confidence Index (CCI) offers an assessment framework for evaluating the security risks of SaaS applications, providing essential details on vendor security practices, audit capabilities, and legal considerations. Their Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) continuously monitor critical IaaS and SaaS environments to prevent misconfigurations and ensure compliance with organizational and regulatory standards. These systems detect and alert on any deviations that could lead to security incidents, thus helping entities maintain a secure posture. The integration with Netskope's Cloud Ticket Orchestrator allows for automated alert management and remediation, minimizing response time. Furthermore, SSPM's capability to guide the remediation of misconfigurations and convert prior issues into preventive rules can enhance an entity's proactive security measures. By optimizing these tools, APRA-regulated entities can rapidly detect and address incidents, ensuring timely notification to APRA within the mandated 72-hour window, thus safeguarding stakeholder interests and fulfilling regulatory requirements effectively.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • SSPM • CTO

Requirements(s)	Netskope Response	Products
36 - Notifying Information Security Incident	Netskope offers comprehensive security solutions that could assist APRA-regulated entities in identifying and addressing information security control weaknesses. Its Cloud Confidence Index (CCI) scores SaaS applications based on various risk criteria, including security policies, certifications, and privacy concerns, providing organizations with essential insight into potential risks. Netskope's Cloud Security Posture Management and SaaS Security Posture Management provide continuous monitoring for mission-critical IaaS and SaaS platforms, respectively. They prevent misconfigurations by ensuring adherence to organizational and regulatory standards. These systems also help prevent data exfiltration and automatically generate remediation actions through their integration with Netskope's Cloud Ticket Orchestrator. Importantly, they offer alerts with detailed remediation steps and can convert previous misconfigurations into new security rules. This proactive approach aids organizations in quickly identifying, reporting, and mitigating security issues, potentially preventing situations where they cannot remediate a material information security weakness in a timely manner. Thus, employing Netskope's solutions could help ensure compliance with APRA's notification requirements by swiftly discovering and addressing security control weaknesses before they become unmanageable.	• CASB • NG-SWG • Public Cloud Security • CSPM • Cloud Confidence Index (CCI) • SSPM • CTO

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.