netskope

EXECUTIVE OVERVIEW

# Netskope APRA Compliance Overview

## INTRODUCTION

Netskope has been actively engaged with Australian financial institutions to interpret and respond to the APRA Prudential Standard CPS 234. Netskope acknowledges the release of this standard reflects changes in the IT landscape, security and privacy concerns, and institutional involvement in contributing to the global open banking framework. All three have profound implications in the way data is utilized between institutions and their customers – with APRA seeking to ensure the prudential standard delivers guidance on implementing a security controls framework that complies with global regulatory standards and customer and community expectations.

In summary, CPS 234 delivers APRA's requirement to ensure both information and data are protected in a financial services context. Netskope's customers have expressed data as being the most important asset in their organization and the CPS 234 prudential standard aims to protect financial institutions from security beaches while maintaining the integrity of that data, from an IT perspective.

Netskope understands many financial institutions are also undergoing IT transformation whereby cloud plays a central part to that change. Cloud adoption implies there are avenues for data loss, or vulnerabilities that could lead to a cybersecurity attack. Netskope understands this has implications for both how IT and cloud are managed, and how incidents are reported to the institution's executives, and even APRA.

The prudential standard contains three components that directly relate to the capabilities provided by the Netskope platform.

They are;

1. Information asset identification and classification
2. Implementation of controls
3. Incident management.

## INFORMATION ASSET IDENTIFICATION AND CLASSIFICATION

The Netskope platform has been architected to facilitate the identification of data assets by type and sensitivity. Financial institutions are regulated to comply with payment and transactions standards such as PCI-DSS and therefore usually have data classification enabled as part of their information security policy.

These classification standards can be enforced in Netskope within the data loss prevention (DLP) engine, which has been architected to inspect key words and attributes within data and to act if that data violates classification standards. This may occur if a user has omitted entering in a classification within the data, or has attempted to transmit classified data that is not in accordance with organizational policy. Netskope's DLP engine is an industry leader in the CASB market and is used by the world's top financial institutions, including 25% of the Fortune 100 for this very purpose.

## IMPLEMENTATION OF CONTROLS

Netskope's control management platform, embedded within its DLP engine, allows it to block the transmission of information, or warn users they have violated a control or policy. Secondly, Netskope leverages most global control and compliance frameworks to enforce these controls. These include NIST 800-53 , ISO 27001, the Cloud Security Alliance's CCM (Cloud Controls Matrix), and industry specific controls such as APRA, as well as regional privacy regulations such as GDPR and Commonwealth of Australia - The Privacy Act 1988.

Netskope's customers have the ability to switch controls on or off, or even report to executives on control compliance or where controls remain open across the enterprise. Netskope's Cloud Risk Assessment even provides vulnerability analysis and management whereby customers obtain insight into where their organization is most exposed and the steps required to minimize exposure to risk.

## INCIDENT MANAGEMENT

Netskope's customers have advised that the incident management engine is one of the best features of the platform. In a single view, users can obtain forensic insight into incidents for DLP, behavior anomalies, compromised credentials, or malware attacks. This insight includes time stamps, IP address, location, user details, and location. From there, customers can quickly build a picture of the incident and react accordingly. Incident data can also be exported to either PDF or CSV file for reporting, if needed. Lastly, if needed, all of Netskope's customers have access to Incident Response playbooks which define the most ideal process for responding to incidents and how to manage them accordingly.

### 15. Maintain an IS capability commensurate with the size and extent of threats

A. Netskope provides a single unified SaaS security platform for the protection of all an organisation's sanctioned and unsanctioned SaaS, IaaS, PaaS, and Web services

B. Netskope is able to apply Shadow IT discovery tools to assist an organisation with understanding their cloud application usage landscape, along with what data is residing within that landscape.

C. Netskope is able to apply data loss prevention controls to an organisation information in transit to, in use by, and at rest in an organisation cloud applications, once the discovery is complete.

D. Netskope is able to detect and protect users from being attacked by detecting malicious payloads using inline and API driven advanced threat protection capabilities.

E. Netskope provides the ability to apply continuous compliance security assessments to Infrastructure as a Service implementations to ensure configuration is both hardened and compliant.

F. Netskope provides controls of access to malicious and categorised websites with its secure web gateway for complete end user HTTP/S protection.

### 16. Where information assets are managed by a related party or third party, the APRA-regulated entity must assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets.

A. Netskope's Shadow IT discovery feature provides organisations with the capability to find out what third-party cloud apps are being used by its end users.

B. Netskope cross references an organisation's discovered cloud application usage with the Netskope's Cloud Confidence Index (CCI). Netskope's CCI provides a full library of over 33000 Cloud Applications and their success in aligning with the Cloud Security Alliance's Cloud Controls Matrix, allowing an organisation to quickly assess the risk of the cloud applications and vendors. The CCI scoring mechanism assists in quickly identifying the most risky app usage. These risks can then be assessed as a priority through its current vendor due diligence program to either accept or implement blocking policies to mitigate risk.

C. Netskope's CCI tracks over 33,000 cloud services, each measured across 50+ criteria such as: product capabilities, legal, auditing and certifications, and SLAs. Netskope's CCI also includes additional parameters like data privacy, financial stability, and other attributes to provide a 360-degree view of a cloud service provider.

D. Netskope's IaaS Security Assessment allows organisations to continuously confirm security configurations and compliance of their private cloud infrastructure.

**17. An APRA-regulated entity must actively maintain its information security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment.**

A. Use of the Netskope discovery tools ensure there is a regular update of an organisation cloud application/asset/data usage

B. Use Netskope's IaaS Security Assessment tool ensures secure configurations are established and maintained from a single pane of glass on any IaaS products in use.

C. Use of Netskope's Secure Web Gateway tool blocks emerging web based threats access and downloads etc

D. Netskope cross references an organisation usernames and emails against the latest data breach reports to alert on end user credentials that have been compromised.

E. Netskope integrates with third-party endpoint anti-malware providers to maintain sophisticated updates on the latest malware threats

## POLICY FRAMEWORK

**18. An APRA-regulated entity must maintain an information security policy framework commensurate with its exposures to vulnerabilities and threats.**

A. It is recommended for APRA-regulated adopt a globally recognised information security framework such as ISO 27001, implementing the required controls from ISO 27002.

**19. An APRA-regulated entity's information security policy framework must provide direction on the responsibilities of all parties who have an obligation to maintain information security.**

A. It is recommended for APRA-regulated adopt a globally recognised information security framework such as ISO 27001 implementing the required controls from ISO 27002.

## INFORMATION ASSET IDENTIFICATION AND CLASSIFICATION

**20. An APRA-regulated entity must classify its information assets, including those managed by related parties and third-parties, by criticality and sensitivity. This classification must reflect the degree to which an information security incident affecting an information asset has the potential to affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers.**

A. Netskope API Integration can be used in combination with Netskope DLP policies to enforce defined classification and policies of data traversing to or contained within 3rd party infrastructure. Netskope can scan the files at rest within an organisation's sanctioned cloud application infrastructure looking for specified data identifiers that align with data that would be part of the organisation's classification strategy.

B. Once detected, these files can either automatically be assigned a classification tag as part of the organisation's classification solution or manually modified by a member of the security operations team.

C. Once a classification strategy has been established, DLP policies and controls can be implemented in order to protect data assets according to their classification, to protect classified data moving to any unsanctioned instance in the organisation's cloud application landscape.

## IMPLEMENTATION OF CONTROLS

**21. An APRA-regulated entity must have information security controls to protect its information assets, including those managed by related parties and third parties, that are implemented in a timely manner and that are commensurate with: (a) vulnerabilities and threats to the information assets; (b) the criticality and sensitivity of the information assets; (c) the stage at which the information assets are within their life-cycle; and (d) the potential consequences of an information security incident.**

A. Netskope provides a robust set of capabilities around policy violations, dependent on the context of the specific application, user and action/activity, as well as the deployment mode (data in motion "inline" or data at rest "API/introspection"). These include actions such as alert, bypass, coach, block, notify (user, owner, administrator, others), encrypt/decrypt, legal hold, quarantine, etc.

B. For example, on an inline policy to take action when a user uploads PCI data to a risky app, Netskope has the ability  to perform the following actions:
   - a. Alert
   - b. Allow
   - c. Block
   - d. Notify User
   - e. Idle Timeout
   - f. Quarantine
   - g. Encrypt
   - h. Bypass

C. As another example, on an  API Protection policy to inspect external (public) sharing of a specific type of document  — both historically and on an ongoing basis — Netskope offers the ability to perform the following actions:
   - a. Alert
   - b. Encrypt
   - c. Restrict Access to the following
     - i. Owner
     - ii. Internal User
     - iii. Whitelisted Domains
     - iv. Blacklisted Domains
     - v. Whitelisted User Profiles
     - vi. Blacklisted User Profiles
     - vii. Remove Public Links
   - d. Delete
   - e. Quarantine via Specific Profile (file is replaced by a tombstone)
   - f. Legal Hold via Specific Profile
   - g. Restrict Sharing to view
   - h. Disable Print and Download
   - i. Apply an RMS template (in case of O365 when AIP is present).

D. Netskope can be configured so that each of an organisation’s DLP rules be triggered at different severity levels and can also be configured to take action in policies based on specific severity. Admins can block specific actions like upload and share, alert for incident management purposes, quarantine files with sensitive data, encrypt files, and put the files in legal hold for review. These actions can be taken based on the severity of the incident. The solution supports four levels of severity - Low, Medium, High, and Critical. The severity level is based on violation counts that are configured on a rule by rule basis.

E. Netskope's incident management dashboard will enable an organisation’s to visualize your overall cloud data loss risk, understand DLP incidents in detail, and make informed policy decisions. Within the incident management dashboard, you will have visibility to incident status and access to very granular detail on every incident – user, severity, activity, application, source, destination, DLP policy, forensics. You will also have access to workflows to escalate an incident to your compliance officer, tag incidents, and write notes. You can also take action to create exceptions, undo policy action, mark false as false positive and notify respective parties.

F. Netskope offers integration with  anti-malware engines through native and 3rd party provider engines to deliver a single consolidated malware alert mechanism for inline and files at rest within an organisation’s cloud application landscape.

### 22. Where an APRA-regulated entity’s information assets are managed by a related party or third party, the APRA-regulated entity must evaluate the design of that party’s information security controls that protects the information assets of the APRA-regulated entity.

A. Netskope’s Shadow IT discovery feature provides an organisation with the capability to discover what third-party cloud applications are being used thereby enabling the organisation to be able to evaluate and implement protection measures around the use of informational assets processed by the cloud application.

B. Netskope cross references an organisation’s discovered cloud application usage with the Netskope’s Cloud Confidence Index (CCI). Netskope’s CCI provides a full library of Cloud Applications and their success in aligning with the Cloud Security Alliance’s Cloud Controls Matrix. Using a Netskope Algorithm all cloud applications are given a risk score from 1 to 100 allowing an organisation to quickly assess the risk of the cloud applications and vendors.

C. Controls can be put in place to protect any data being uploaded or downloaded from any risky cloud applications based on their alignment with the cloud application’s risk score so  an organisation can protect their information assets from risky third-party.

## INCIDENT MANAGEMENT

### 23. An APRA-regulated entity must have robust mechanisms in place to detect and respond to information security incidents in a timely manner.

A. Netskope's incident management dashboard will enable an organisation to visualize their overall cloud data loss risk, understand DLP incidents in detail, and make informed policy decisions. Within the incident management dashboard, you will have visibility to incident status and access to very granular detail on every incident – user, severity, activity, application, source, destination, DLP policy, forensics. You will also have access to workflows to escalate an incident to your compliance officer, tag incidents, and write notes. An organisation can also take action to create exceptions, undo policy action, mark false as false positive, and notify respective parties.

**24. An APRA-regulated entity must maintain plans to respond to information security incidents that the entity considers could plausibly occur (information security response plans).**

A. Netskope's incident management is able to correlate the DLP policies severity with the cloud application's CCI Risk score, to determine the correct level of action or response from an organisation.

**25. An APRA-regulated entity's information security response plans must include the mechanisms in place for: (a) managing all relevant stages of an incident, from detection to post-incident review; and(b) escalation and reporting of information security incidents to the Board, other governing bodies and individuals responsible for information security incident management and oversight, as appropriate.**

A. Netskope's incident management dashboard, you will have visibility to incident status and access to very granular detail on every incident – user, severity, activity, application, source, destination, DLP policy, forensics. Incident workflows make it easy to review alignment with an organisation security response plans at relevant stages of detection and escalations to your compliance officer, with incident tagging, and notes available, all collected through audit logs.

B. Netskope Alerts and incident management information can also be integrated via RestAPI or emails to third-party SIEM or Incident Response Solutions.

C. Netskope reporting can provide trending information to determine the volumes of DLP alerts over time to ensure the Netskope solution continues to provide value, return on investment and is fit-for-purpose.

**26. An APRA-regulated entity must annually review and test its information security response plans to ensure they remain effective and fit-for-purpose.**

A. Netskope alerts and incident management information can also be integrated via RestAPI or emails to third-party SIEM or Incident Response Solutions.

B. Netskope reporting can provide trending information to determine the volumes of DLP Alerts over time to ensure the Netskope solution continues to provide value, return on investment and is fit-for-purpose.

## TESTING CONTROL EFFECTIVENESS

**27. An APRA-regulated entity must test the effectiveness of its information security controls through a systematic testing program. The nature and frequency of the systematic testing must be commensurate with: (a) the rate at which the vulnerabilities and threats change; (b) the criticality and sensitivity of the information asset; (c) the consequences of an information security incident; (d) the risks associated with exposure to environments where the APRA regulated entity is unable to enforce its information security policies; 11 and (e) the materiality and frequency of change to information assets.**

A. Netskope's simple integration via APIs allowed effective testing of uploading samples of sensitive data into an organisation's sanctioned applications, with Netskope detecting the sensitive files, and their permissions, and all the necessary information was provided to an organisation's Incident Response team.

B. Netskope's inline forward and reverse proxy capabilities can be effectively tested by uploading samples of sensitive data to unsanctioned instances of an organisation's cloud applications landscape, and all the necessary information was provided to an organisation's Incident Response team.

C. Netskope discovery tools allows the business to detect changes of use, new cloud applications that start to trend and whose usage becomes more popular within an organisation.

D. Netskope forward proxy is able to control the use or new cloud applications that start to trend and whose usage becomes more popular within an organisation.

### 28. Where an APRA-regulated entity's information assets are managed by a related party or a third party, and the APRA-regulated entity is reliant on that party's information security control testing, the APRA-regulated entity must assess whether the nature and frequency of testing of controls in respect of those information assets is commensurate with paragraphs 27(a) to 27(e) of this Prudential Standard.

A. Netskope's simple integration via APIs allowed effective testing of uploading samples of sensitive data into an organisation's sanctioned applications, with Netskope detecting the sensitive files, and their permissions, and all the necessary information was provided to an organisation's incident response team.

B. Netskope's inline forward and reverse proxy capabilities can be  effectively tested by uploading samples of sensitive data to unsanctioned instances of an organisation's cloud applications landscape, and all the necessary information was provided to an organisation's incident response team.

C. Netskope discovery tools allows the business to detect changes of use, new cloud applications that start to trend and whose usage becomes more popular within an organisation.

D. Netskope forward proxy is able to control the use or new cloud applications that start to trend and whose usage becomes more popular within an organisation.

### 29  An APRA-regulated entity must escalate and report to the board or senior management any testing results that identify information security control deficiencies that cannot be remediated in a timely manner.

A. Netskope provides a registry of cloud services which includes a risk assessment of each service, named the Netskope Cloud Confidence Index (CCI). The CCI assesses an app's "enterprise readiness" based on objective criteria and then assigns it an overall score. Netskope's CCI tracks over 30,000 cloud services, each measured across 50+ criteria such as: product capabilities, legal, auditing and certifications, and SLAs. Netskope's CCI also includes additional parameters like data privacy, financial stability, and other attributes to provide a 360-degree view of a cloud service provider.

B. Based on these factors, an algorithm is applied to determine an overall enterprise-readiness index score — each app is given a score between 0-100. The score gives you an at-a-glance assessment of whether an app is ready for your enterprise, or if you'll need to limit access and permissions to the app based on its risk level. Moreover, you can incorporate the CCI into your cloud app policies within the Netskope Security Cloud Platform – such as to restrict certain activities within the app or limit device types that are allowed to access the app – in order to declare an app suitable for your organization.

C. Netskope is able to distinguish user activities and data flows across a categorized set of enterprise cloud apps (HR, marketing, finance, software development, CRM, etc.). This allows you to have a meaningful conversation with your line of business owners (such as a head of HR using SuccessFactors or a GM of a business unit using Salesforce) or enforce an effective policy (such as "Alert me when someone from support downloads content from any CRM app" or "Block people who are not in the AD group 'HR Directors' from downloading data from any HR app").

D. Queryable executive dashboard. Netskope's query language allows you to very quickly drill into your dashboard and ask key questions like: "Show me all of the apps in these 5 business-critical categories that are SAML-enabled" (if you want to quickly identify the top apps to pull into your SSO framework), or "Show me all of the CRM apps that enable sharing" (if you want to understand from which apps your Customer Support organization may be sharing proprietary content), or "Show me all uploads of more than 5 MB by one of our process engineers to any software development app" (if you want to identify potentially non-compliant upload of sensitive process or design documents).

### 34. An APRA-regulated entity's internal audit function must assess the information security control assurance provided by a related party or third party where: (a) an information security incident affecting the information assets has the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; and (b) internal audit intends to rely on the information security control assurance provided by the related party or third party

A. Netskope provides a registry of cloud services which includes a risk assessment of each service, named the Netskope Cloud Confidence Index (CCI). The CCI assesses an app's "enterprise readiness" based on objective criteria and then assigns it an overall score. Netskope's CCI tracks over 30,000 cloud services, each measured across 50+ criteria such as: product capabilities, legal, auditing and certifications, and SLAs. Netskope's CCI also includes additional parameters like data privacy, financial stability, and other attributes to provide a 360-degree view of a cloud service provider.

B. Based on these factors, an algorithm is applied to determine an overall enterprise-readiness index score — each app is given a score between 0-100. The score gives you an at-a-glance assessment of whether an app is ready for your enterprise, or if you'll need to limit access and permissions to the app based on its risk level. Moreover, you can incorporate the CCI into your cloud app policies within the Netskope Security Cloud Platform – such as to restrict certain activities within the app or limit device types that are allowed to access the app – in order to declare an app suitable for your organization.

C. APRA-regulated entities can also modify the weightings of these metrics based on your specific business requirements to ensure relevant benchmarking, as well as compare multiple cloud apps side-by-side for further evaluation. Further, APRA-regulated entities can associate "tags" to identify apps as sanctioned, unsanctioned, used by specific departments, etc. and then apply policies and/or reporting based on these tags.

D. Netskope also assesses the GDPR- readiness of the cloud services and provides a GDPR readiness widget to help you easily identify and report on apps that are not GDPR compliant.

E. The CCI is updated monthly with app update frequency, depending on the popularity of these apps among our customers. Netskope customers can also send feedback regarding the apps directly to us via the service portal (CCI crowdsourcing). A historical overview of each app's CCI trend and the reason why the score has changed in the past is also available.

**35. An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 72 hours, after becoming aware of an information security incident that: (a) materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers; or (b) has been notified to other regulators, either in Australia or other jurisdictions.**

A. Netskope's Incident dashboard enables a customer to visualize your overall cloud data loss risk, as well as drill into DLP incident details, in order to make informed policy decisions. Within the dashboard, you will see a preview of the file, and the violating content will be highlighted for easy identification. The dashboard can also provide very granular detail on every incident – user, severity, activity, application, source, destination, DLP policy, and forensics.

In addition to visibility of an incident, Netskope's Incident dashboard provides workflows to escalate the incident to your compliance officer, tag incidents, and write notes regarding the incident — allowing administrators to use one dashboard to open, investigate, and resolve cloud incidents.

Key features of Netskope incident management capabilities include:

a. Closed-Loop Workflows: Administrative 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 notify users or protect (i.e. encrypt, restrict, etc.) sensitive data.

b. Detailed Forensics: Detailed forensic and audit trails give security analysts a comprehensive view of each incident, including the specific policy violated, actions taken and a view of any sensitive data in complete context. This forensics view also includes a range of additional information including the user, device, location, app and app instance, and more, giving the analyst complete context to make a well-informed decision.

c. Incident Histories: Event-by-event incident history interlaces all activities for a given incident. This includes all 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 on, confirm and report on a successful resolution.

d. Customizable Role-Based Access Control: Netskope has greatly expanded predefined administrator and analyst roles, and also added fine-grained ability to define custom roles by both administrative functions and organizational scope, including by group, location, app/app instance and more.

**36. An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 10 business days, after it becomes aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner.**

A. Netskope's Incident dashboard enables a customer to visualize your overall cloud data loss risk, as well as drill into DLP incident details, in order to make informed policy decisions. Within the dashboard, you will see a preview of the file, and the violating content will be highlighted for easy identification. The dashboard can also provide very granular detail on every incident – user, severity, activity, application, source, destination, DLP policy, and forensics.

In addition to visibility of an incident, Netskope's incident dashboard provides workflows to escalate the incident to your compliance officer, tag incidents, and write notes regarding the incident — allowing administrators to use one dashboard to open, investigate, and resolve cloud incidents.

Key features of Netskope incident management capabilities include:

a. Closed-Loop Workflows: Administrative 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 notify users or protect (i.e. encrypt, restrict, etc.) sensitive data.

b. Detailed Forensics: Detailed forensic and audit trails give security analysts a comprehensive view of each incident, including the specific policy violated, actions taken and a view of any sensitive data in complete context. This forensics view also includes a range of additional information including the user, device, location, app and app instance, and more, giving the analyst complete context to make a well-informed decision.

c. Incident Histories: Event-by-event incident history interlaces all activities for a given incident. This includes all 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 on, confirm and report on a successful resolution.

d. Customizable Role-Based Access Control: Netskope has greatly expanded predefined administrator and analyst roles, and also added fine-grained ability to define custom roles by both administrative functions and organizational scope, including by group, location, app/app instance, and more.