

National Institute of Standards and  
Technology Cybersecurity Framework  
(NIST CSF) 2.0

# Aligning the Netskope Platform to NIST CSF 2.0



## TABLE OF CONTENTS

---

|                              |   |
|------------------------------|---|
| <u>INTRODUCTION</u>          | 3 |
| <u>THE FRAMEWORK CORE</u>    | 3 |
| <u>PROFILES AND TIERS</u>    | 4 |
| <u>HOW TO USE THIS GUIDE</u> | 4 |

## INTRODUCTION

---

The National Institute for Standards and Technology's Cyber Security Framework (NIST CSF) integrates industry standards and best practices to help organizations manage their cybersecurity risks. Since the publication of NIST CSF 1.1 in 2014, it has become the de facto standard, providing a common language to staff at all levels of an organization - and to partners at all points in the supply chain - to develop a shared understanding of their cybersecurity strengths and weaknesses.

NIST CSF 2.0 retains the same basic structure as its predecessor. It consists of a Framework Core composed of Functions that define broad strategic goals, such as Identifying the IT assets an organization must secure, and Responding appropriately to security incidents. These Functions are further divided into Categories and Subcategories of increasing granularity to which specific tools and controls can be mapped.

NIST CSF also retains the concepts of Profiles and Tiers. An enterprise's Organizational Profile consists of its Current Profile and its Target Profile. The Current Profile is descriptive, depicting the enterprise's current capabilities with respect to the strategic goals outlined in the Framework Core. Its Target Profile is aspirational, reflecting the level of cybersecurity maturity the enterprise wishes to attain. The level of cybersecurity maturity is captured in the concept of Tiers, where Tier 1 represents the lowest level of maturity, and Tier 4 the highest.

Like its predecessor, NIST CSF 2.0 does not consist of a one-size-fits-all checklist of tools and controls. It does not envision that every enterprise will have the same Target Profile, nor that every enterprise need aspire to Tier 4 in every category or subcategory of the Framework Core. Rather, an enterprise's Target Profile will be determined by strategic considerations including the enterprise's size, complexity, risk profile, industry, and regulatory environment, among other things.

## THE FRAMEWORK CORE

---

The most significant innovation in the NIST CSF 2.0 is the addition of a sixth Function - Govern - to the Framework Core. The Govern Function precedes but also informs all the other Functions. They are defined as follows:

**Govern (GV):** The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

**Identify (ID):** The organization's current cybersecurity risks are understood.

**Protect (PR):** Safeguards to manage the organization's cybersecurity risks are used.

**Detect (DE):** Possible cybersecurity attacks and compromises are found and analyzed.

**Respond (RS):** Actions regarding a detected cybersecurity incident are taken.

**Recover (RC):** Assets and operations affected by a cybersecurity incident are restored.

Each of these Functions consists of several categories and subcategories, defined in the mapping guide below.

## PROFILES AND TIERS

---

The other major change since NIST CSF 1.1 is the addition of the concept of Community Profiles. NIST defines a Community Profile as “a baseline of CSF outcomes that is created and published to address shared interests and goals among a number of organizations. A Community Profile is typically developed for a particular sector, subsector, technology, threat type, or other use case. An organization can use a Community Profile as the basis for its own Target Profile.”

Enterprises can also use CSF Tiers to assess their own Current Profiles and design their Target Profiles. The Tiers can be summarized as follows:

**Tier 1:** Partial Cybersecurity posture is ad hoc and reactive, with limited organizational awareness of cyber risk and poorly established or nonexistent processes for evaluating cyber risk or communicating information about cyber risk throughout the organization.

**Tier 2:** Risk Informed Cybersecurity strategy is approved by management and informed by business requirements, known threats, and risk tolerance. However, that strategy may not be communicated throughout the organization, and the organization may lack formal processes for assessing cyber risk - including in its supply chains - or for sharing information about cyber risks.

**Tier 3:** Repeatable Cybersecurity strategy is established as organizational policy, and processes and procedures are defined, implemented, reviewed, and updated on a regular basis. Information about cyber risk is effectively communicated throughout the organization, and appropriate personnel are assigned to roles necessary to monitor and respond to cyber threats.

**Tier 4:** Adaptive Cybersecurity strategy is consciously woven into the organization’s overall business strategy, and general awareness of the organization’s past and present cyber threat landscape results in cyber risk management becoming part of the organizational culture. Information about cyber risks and threats is shared effectively throughout the organization and with appropriate stakeholders. The organization’s cybersecurity policies and practices are continuously evolving, using real-time or near real-time information to inform supply chain management.

While NIST recommends that every enterprise aspire at least to Tier 2 across the Framework Core, whether to attain Tiers 3 or 4 depends on each enterprise’s unique combination of needs, capabilities, and risk tolerances.

## HOW TO USE THIS GUIDE

---

The Netskope Platform doesn’t just come into play once you’ve already settled on a Target Profile for your enterprise. On the contrary, it can help you understand your Current Profile so that you can then design and achieve the best Target Profile for your organization.

The table below breaks out each Function into its constituent Categories and Subcategories, and maps specific Netskope products to each Subcategory. The Functions are color-coded using the same scheme employed by NIST (yellow for Govern, blue for Identify, purple for Protect, orange for Detect, red for Respond, and green for Recover). The Netskope Reference describes how the Netskope Platform

addresses the corresponding Subcategory, and is accompanied by a list of specific products that map most directly to the Subcategory's requirements.

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                                 |

| Industry terminology                        | Netskope Product Line/Abbreviation                                                                                                                                                    |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Software-Defined Wide Area Network (SD-WAN) | Borderless SD-WAN<br>Secure SD-WAN<br>Endpoint SD-WAN<br>Wireless SD-WAN<br>IoT Intelligent Access                                                                                    |
| Threat/Risk Sharing                         | Secure Cloud Exchange <ul style="list-style-type: none"> <li>• Cloud Threat Exchange (CTE)</li> <li>• Cloud Risk Exchange (CRE)</li> <li>• Cloud Ticket Orchestrator (CTO)</li> </ul> |
| 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)                                                                                                                                                           |

| Function           | Category                                                                                                                                                                                                                                                    | Subcategory                                                                                                                                                                    | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                       | Products       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <b>GOVERN (GV)</b> | <b>Organizational Context (GV.OC):</b><br>The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood. | <b>GV.OC-01:</b><br>The organizational mission is understood and informs cybersecurity risk management.                                                                        | The Netskope platform can enforce cybersecurity policies defined by the organization.<br><br>Policies can be configured or automated based on levels of cybersecurity risks and include allowing, blocking and/or coaching activities.<br><br>For example, user notifications can pop up in real time when a user violates a policy. This ensures the user is educated on organizational policy in real time and may prevent an incident from occurring. | • All products |
|                    |                                                                                                                                                                                                                                                             | <b>GV.OC-02:</b><br>Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered. | The Netskope platform offers pop-up banners/coaching pages across its product that can notify internal stakeholders/employees of policy infringements in line with organizational requirements.<br><br>Netskope products offer reporting on employee high-risk activities in relation to activities, threats, and Data Loss Prevention (DLP) engines.                                                                                                    | • All products |

| Function           | Category                                                                                                                                                                                                                                                    | Subcategory                                                                                                                                                                   | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                              | Products                                                                                |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <b>GOVERN (GV)</b> | <b>Organizational Context (GV.OC):</b><br>The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization’s cybersecurity risk management decisions are understood. | <b>GV.OC-03:</b><br>Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed. | Netskope Security Posture Management (CSPM & SSPM) solutions are available for public cloud services and SaaS applications, giving visibility and control over cloud service security settings to manage according to legal, regulatory, and company policy requirements.<br><br>Netskope’s Cloud Confidence Index (CCI) also provides a risk-based score for SaaS applications, incorporating assessments based on privacy policies and regulatory compliance. | <ul style="list-style-type: none"> <li>• CSPM</li> <li>• SSPM</li> <li>• CCI</li> </ul> |
|                    |                                                                                                                                                                                                                                                             | <b>GV.OC-04:</b><br>Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated.     | Netskope products can provide external stakeholders secure access to organizations systems including both cloud and on-prem applications and services.                                                                                                                                                                                                                                                                                                          | <ul style="list-style-type: none"> <li>• ZTNA Next</li> </ul>                           |
|                    |                                                                                                                                                                                                                                                             | <b>GV.OC-05:</b><br>Outcomes, capabilities, and services that the organization depends on are understood and communicated.                                                    | The Netskope platform offers controls to identify and protect information assets and services including assets across web and cloud applications and/or cloud infrastructure along with devices. These controls can be used to create an inventory of information assets across sanctioned or unsanctioned services.                                                                                                                                            | <ul style="list-style-type: none"> <li>• All products</li> </ul>                        |
|                    | <b>Risk Management Strategy (GV.RM):</b><br>The organization’s priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.                              | <b>GV.RM-01:</b><br>Risk management objectives are established and agreed to by organizational stakeholders.                                                                  | Netskope products do not directly map to this subcategory. However, once objectives are established, the Netskope platform can apply controls to ensure risks are mitigated and controls are enforced.<br><br>The Netskope platform offers numerous risk dashboards that can be used to measure risk across web and cloud services.                                                                                                                             | <ul style="list-style-type: none"> <li>• All products</li> </ul>                        |

| Function           | Category                                                                                                                                                                                                                       | Subcategory                                                                                                                                                         | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Products                                                                                         |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| <b>GOVERN (GV)</b> | <b>Risk Management Strategy (GV.RM):</b><br>The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions. | <b>GV.RM-02:</b><br>Risk appetite and risk tolerance statements are established, communicated, and maintained.                                                      | <p>Netskope's Cloud Confidence Index (CCI) provides a risk-based score to over 85,000 cloud applications.</p> <p>Organizations can adjust the default score of an app by emphasizing or de-emphasizing risk elements that are more or less important to the organization, such as the need to comply with specific regulatory regimes like GDPR.</p> <p>In addition, Netskope can ensure a User Confidence Index (UCI) score is available to ensure risk is measured and controlled in relation to high-risk user activity.</p>                                                                                                                                                                 | <ul style="list-style-type: none"> <li>• CCI</li> <li>• UCI</li> </ul>                           |
|                    |                                                                                                                                                                                                                                | <b>GV.RM-03:</b><br>Cybersecurity risk management activities and outcomes are included in enterprise risk management processes.                                     | The Netskope platform offers a ticketing system to escalate high risk information security events and can store forensic data in forensic tools or repositories defined by customers to support enterprise risk management processes.                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <ul style="list-style-type: none"> <li>• All products</li> <li>• CTO</li> </ul>                  |
|                    |                                                                                                                                                                                                                                | <b>GV.RM-04:</b><br>Strategic direction that describes appropriate risk response options is established and communicated.                                           | <p>The Netskope platform offers pop-up banners/coaching pages across its product that can notify internal stakeholders/employees of policy infringements in line with organizational requirements.</p> <p>Netskope offers reporting on employee high-risk activities in relation to activities, threats, and Data Loss Prevention (DLP) engines.</p>                                                                                                                                                                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>• All products</li> </ul>                                 |
|                    |                                                                                                                                                                                                                                | <b>GV.RM-05:</b><br>Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties. | <p>Netskope products offer a ticketing system to escalate high risk information security events along with reporting capabilities to present reports and dashboards.</p> <p>Netskope Cloud Threat Exchange (CTE) and Cloud Risk Exchange (CRE) 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.</p> <p>Netskope's Cloud Confidence Index (CCI) discovers 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.</p> | <ul style="list-style-type: none"> <li>• Cloud Exchange</li> <li>• CCI</li> <li>• CTO</li> </ul> |



| Function           | Category                                                                                                                                                                                                                          | Subcategory                                                                                                                                                                       | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Products                                                                                                                                              |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>GOVERN (GV)</b> | <b>Risk Management Strategy (GV.RM):</b><br>The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.    | <b>GV.RM-06:</b><br>A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated.                       | <p>Netskope products identify and categorize managed and unmanaged apps and cloud services in the organization's IT environment.</p> <p>Netskope's Cloud Confidence Index (CCI) provides a risk-based score to each app based on numerous factors, including recently disclosed vulnerabilities and exploits.</p> <p>Advanced Analytics also has available cybersecurity risk dashboards that can be used to calculate, prioritize and report on risks to stakeholders.</p>                                                                                                                                                                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>• CCI</li> <li>• CASB</li> <li>• Advanced Analytics</li> </ul>                                                 |
|                    |                                                                                                                                                                                                                                   | <b>GV.RM-07:</b><br>Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions.                           | <p>Netskope products can help identify positive risks in both UEBA, Threat Protection, DLP and Advanced Analytics.</p> <p>Netskope's machine learning (ML) capabilities can identify good behavior and positive examples of activity and learn to identify future traits helping to understand new risks</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <ul style="list-style-type: none"> <li>• UEBA</li> <li>• Threat Protection</li> <li>• DLP</li> <li>• SkopeAI</li> <li>• Advanced Analytics</li> </ul> |
|                    | <b>Roles, Responsibilities, and Authorities (GV.RR):</b><br>Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated. | <b>GV.RR-01:</b><br>Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving. | <p>The Netskope platform can enforce cybersecurity policies defined by the organization.</p> <p>Policies can be configured or automated based on levels of cybersecurity risks and including allowing, blocking and/or coaching activities.</p> <p>For example, user notifications can pop up in real time when a user violates a policy. This ensures the user is educated on organizational policy in real time and prevents the incident from occurring.</p> <p>There is a high degree of flexibility in this mechanism, as Netskope provides the ability to warn users before a potential violation occurs, block them entirely from carrying out the action, or take more proactive steps such as real-time coaching, suggesting safer alternatives, or requesting a business justification for the activity.</p> | <ul style="list-style-type: none"> <li>• All products</li> </ul>                                                                                      |

| Function           | Category                                                                                                                                                                                                                          | Subcategory                                                                                                                                                                          | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Products                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>GOVERN (GV)</b> | <b>Roles, Responsibilities, and Authorities (GV.RR):</b><br>Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated. | <b>GV.RR-02:</b><br>Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.                       | The Netskope platform can enforce cybersecurity policies defined by the organization.<br><br>Netskope offers reporting on employee high-risk activities in relation to activities, threats, and Data Loss Prevention (DLP) engines.                                                                                                                                                                                                                                                          | <ul style="list-style-type: none"> <li>All products</li> </ul>                                                           |
|                    |                                                                                                                                                                                                                                   | <b>GV.RR-03:</b><br>Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.                                       | Netskope does not map to this subcategory.                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>N/A</li> </ul>                                                                    |
|                    |                                                                                                                                                                                                                                   | <b>GV.RR-04:</b><br>Cybersecurity is included in human resources practices.                                                                                                          | Netskope products can enforce additional controls for personnel who are deemed to be high-risk users, for example those who may be leaving an organization. This could include adding a user to a more restrictive set of controls when their risk profile increases.<br><br>Additionally, Netskope can help to ensure the HR platforms and services are accessed appropriately (i.e. by the appropriate personnel, activities are controlled, excessive permissions are not granted, etc.). | <ul style="list-style-type: none"> <li>NG-SWG</li> <li>CASB</li> <li>ZTNA Next</li> <li>Public Cloud Security</li> </ul> |
|                    | <b>Policy (GV.PO):</b><br>Organizational cybersecurity policy is established, communicated, and enforced.                                                                                                                         | <b>GV.PO-01:</b><br>Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced. | The Netskope platform can enforce cybersecurity policies defined by the organization.<br><br>Policies can be configured or automated based on levels of cybersecurity risks and including allowing, blocking and/or coaching activities.<br><br>For example, user notifications can pop up in real time when a user violates a policy. This ensures the user is educated on organizational policy in real time and prevents the incident from occurring.                                     | <ul style="list-style-type: none"> <li>All products</li> </ul>                                                           |

| Function           | Category                                                                                                                                                                                 | Subcategory                                                                                                                                                                                       | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                              | Products                                                                                     |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| <b>GOVERN (GV)</b> | <b>Policy (GV.PO):</b><br>Organizational cybersecurity policy is established, communicated, and enforced.                                                                                | <b>GV.PO-02:</b><br>Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission. | <p>The Netskope platform can enforce cybersecurity policies defined by the organization.</p> <p>Policies can be configured or automated based on levels of cybersecurity risks and including allowing, blocking and/or coaching activities.</p> <p>For example, user notifications can pop up in real time when a user violates a policy. This ensures the user is educated on organizational policy in real time and prevents the incident from occurring.</p> | <ul style="list-style-type: none"> <li>All products</li> </ul>                               |
|                    | <b>Oversight (GV.OV):</b><br>Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy. | <b>GV.OV-01:</b><br>Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction.                                                                     | Netskope does not map to this subcategory.                                                                                                                                                                                                                                                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>N/A</li> </ul>                                        |
|                    |                                                                                                                                                                                          | <b>GV.OV-02:</b><br>The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.                                              | Netskope Advanced Analytics has available cybersecurity risk dashboards that can be used to calculate, prioritize and report on risks to stakeholders.                                                                                                                                                                                                                                                                                                          | <ul style="list-style-type: none"> <li>Advanced Analytics</li> </ul>                         |
|                    |                                                                                                                                                                                          | <b>GV.OV-03:</b><br>Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed.                                                                    | <p>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.</p> <p>Both Netskope's Cloud &amp; Security Posture Management (CSPM/SSPM) continuously monitors SaaS apps and Public Cloud services to ensure adherence to updated policy configurations.</p>                                           | <ul style="list-style-type: none"> <li>Cloud Exchange</li> <li>CSPM</li> <li>SSPM</li> </ul> |

| Function           | Category                                                                                                                                                                                                 | Subcategory                                                                                                                                                                           | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Products                                                                                                 |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>GOVERN (GV)</b> | <b>Cybersecurity Supply Chain Risk Management (GV.SC):</b><br>Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders. | <b>GV.SC-01:</b><br>A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders. | Netskope products can be used to apply controls and baseline assessments required for and by suppliers in line with security requirements.<br><br>Netskope scores SaaS applications in its Cloud Confidence Index (CCI) and provides many important details that help organizations assess the risk of using each app or cloud service. Criteria include the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more.                                                                      | <ul style="list-style-type: none"> <li>CASB</li> <li>Public Cloud Security</li> <li>CCI</li> </ul>       |
|                    |                                                                                                                                                                                                          | <b>GV.SC-02:</b><br>Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.         | Netskope products score SaaS applications in its Cloud Confidence Index (CCI) and provide many important details that help organizations assess the risk of using each app or cloud service. Criteria include the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more.                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>CCI</li> </ul>                                                    |
|                    |                                                                                                                                                                                                          | <b>GV.SC-03:</b><br>Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.           | Netskope products can be used to apply controls and baseline assessments required for and by suppliers in line with security requirements.<br><br>Netskope can also audit web and cloud applications, and provide metadata to understand if suppliers are using underlying cloud infrastructure to support supply chain discovery.<br><br>Netskope also offers reverse proxy capabilities to protect cloud applications along with Netskope's Zero-Trust Network Access (ZTNA Next ) to manage suppliers' access to organizational assets. | <ul style="list-style-type: none"> <li>CASB</li> <li>Public Cloud Security</li> <li>ZTNA Next</li> </ul> |
|                    |                                                                                                                                                                                                          | <b>GV.SC-04:</b><br>Suppliers are known and prioritized by criticality..                                                                                                              | Netskope products discover cloud apps, including unmanaged apps, in use in the enterprise and can categorize them by usage and risk score.<br><br>This gives the organization a clearer picture of which apps are most critical to their day-to-day operations, as well as the risks of using any given app.                                                                                                                                                                                                                               | <ul style="list-style-type: none"> <li>CCI</li> <li>NG-SWG</li> <li>CASB</li> </ul>                      |

| Function           | Category                                                                                                                                                                                                 | Subcategory                                                                                                                                                                                                                 | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Products                                                                                                 |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>GOVERN (GV)</b> | <b>Cybersecurity Supply Chain Risk Management (GV.SC):</b><br>Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders. | <b>GV.SC-05:</b><br>Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties. | <p>Netskope products can be used to apply controls and baseline assessments required for and by suppliers in line with security requirements.</p> <p>Netskope CASB and Public Cloud Security can audit web and cloud applications, and provide metadata to understand if suppliers are using underlying cloud infrastructure to support supply chain discovery.</p> <p>Netskope also offers reverse proxy capabilities to protect cloud applications along with Netskope's Zero-Trust Network Access (ZTNA Next ) to manage suppliers' access to organizational assets.</p> | <ul style="list-style-type: none"> <li>CASB</li> <li>ZTNA Next</li> <li>Public Cloud Security</li> </ul> |
|                    |                                                                                                                                                                                                          | <b>GV.SC-06:</b><br>Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.                                                                       | <p>Netskope's Cloud Confidence Index (CCI) provides a risk-based score for over 85,000 applications, taking into consideration their enterprise readiness, auditability, privacy policies, and regulatory compliance.</p> <p>You can change the default score by giving more or less weight to criteria that are more or less important to your organization, and then compare apps side-by-side to determine which better meets your compliance needs.</p>                                                                                                                 | <ul style="list-style-type: none"> <li>CCI</li> </ul>                                                    |
|                    |                                                                                                                                                                                                          | <b>GV.SC-07:</b><br>The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship.   | <p>Netskope products score SaaS applications in its Cloud Confidence Index (CCI) and provide important details that help organizations assess the risk of using each app or cloud service. Criteria include the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more.</p>                                                                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>CCI</li> </ul>                                                    |
|                    |                                                                                                                                                                                                          | <b>GV.SC-08:</b><br>Relevant suppliers and other third parties are included in incident planning, response, and recovery activities.                                                                                        | <p>Netskope's CASB identifies and catalogs apps and cloud services in the organization's IT environment, and the Cloud Confidence Index (CCI) assigns each app a risk-based score. Together, these capabilities can help the organization identify critical cloud applications and service providers to ensure they are included in incident response planning.</p>                                                                                                                                                                                                         | <ul style="list-style-type: none"> <li>CASB</li> <li>CCI</li> </ul>                                      |

| Function           | Category                                                                                                                                                                                                 | Subcategory                                                                                                                                                                                                                 | Netskope Reference                                                                                                                                                                                                                                                                                                    | Products                                                 |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| <b>GOVERN (GV)</b> | <b>Cybersecurity Supply Chain Risk Management (GV.SC):</b><br>Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders. | <b>GV.SC-09:</b><br>Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle. | Netskope products score SaaS applications in its Cloud Confidence Index (CCI) and provide important details that help organizations assess the risk of using each app or cloud service. Criteria include the vendor's security policies and certifications, audit capabilities, legal and privacy concerns, and more. | <ul style="list-style-type: none"> <li>• CCI</li> </ul>  |
|                    |                                                                                                                                                                                                          | <b>GV.SC-10:</b><br>Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement.                                               | Netskope products can identify and catalog all managed and unmanaged apps and cloud services in the organization's IT ecosystem. This includes assessing activity and reporting on app usage allowing the organization to ensure certain services are off boarded.                                                    | <ul style="list-style-type: none"> <li>• CASB</li> </ul> |

| Function             | Category                                                                                                                                                                                                                                                                                                             | Subcategory                                                                                                    | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Products                                                                                                 |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>IDENTIFY (ID)</b> | <b>Asset Management (ID.AM):</b><br>Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | <b>ID.AM-01:</b><br>Inventories of hardware managed by the organization are maintained.                        | Netskope's Device Intelligence capability offers organizations the ability to produce an inventory of hardware on their network including IoT, OT and traditional devices.                                                                                                                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>• Device Intelligence</li> </ul>                                  |
|                      |                                                                                                                                                                                                                                                                                                                      | <b>ID.AM-02:</b><br>Inventories of software, services, and systems managed by the organization are maintained. | <p>Netskope products provide detailed reports and interactive dashboards that inventory, categorize, assign risk scores to, and show the usage of, more than 85,000 cloud applications in use within the enterprise including SaaS and Public Cloud services.</p> <p>Netskope can also identify, inventory, and enforce real-time control for unmanaged applications (i.e. end-user adopted SaaS applications that have not been officially onboarded by IT, also known as Shadow IT).</p> | <ul style="list-style-type: none"> <li>• CASB</li> <li>• Public Cloud Security</li> <li>• CCI</li> </ul> |

| Function             | Category                                                                                                                                                                                                                                                                                                             | Subcategory                                                                                                                                             | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Products                                                                                                                                                                          |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IDENTIFY (ID)</b> | <b>Asset Management (ID.AM):</b><br>Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | <b>ID.AM-03:</b><br>Representations of the organization's authorized network communication and internal and external network data flows are maintained. | <p>Netskope products are able to characterize SaaS, IaaS, and web usage across an entire enterprise including remote access connections to on-prem apps and services. This includes the monitoring of non-corporate devices accessing corporate SaaS applications and users accessing non-corporate SaaS applications from IT-managed devices.</p> <p>IT and Security teams are able to map communication and data flows to an exceptional degree of accuracy. Netskope will not only map where data is flowing, including for company and personal app instances, but also provide the necessary controls to contain data flows when unmanaged devices are being used and unmanaged services are being adopted by end users.</p> | <ul style="list-style-type: none"> <li>• NG-SWG</li> <li>• CASB</li> <li>• Public Cloud Security</li> <li>• ZTNA Next</li> <li>• DLP</li> <li>• Device Intelligence</li> </ul>    |
|                      |                                                                                                                                                                                                                                                                                                                      | <b>ID.AM-04:</b><br>Inventories of services provided by suppliers are maintained.                                                                       | <p>Netskope products provide detailed reports and interactive dashboards that inventory, categorize, assign risk scores to, and show the usage of, more than 85,000 cloud applications in use within the enterprise including SaaS and Public Cloud services.</p> <p>Netskope can also identify, inventory, and enforce real-time control for unmanaged applications (i.e. end-user adopted SaaS applications that have not been officially onboarded by IT, also known as Shadow IT).</p>                                                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• CASB</li> <li>• Public Cloud Security</li> <li>• CCI</li> </ul>                                                                          |
|                      |                                                                                                                                                                                                                                                                                                                      | <b>ID.AM-05:</b><br>Assets are prioritized based on classification, criticality, resources, and impact on the mission.                                  | <p>Netskope products can enforce conditional access policies to resources and assets based on user, location, service, activity, device type, operating system, and access method.</p> <p>In addition, Netskope can prioritize traffic, rate-limit bandwidth usage, and enforce access based on applications, devices, and user groups using Netskope Borderless SD-WAN.</p>                                                                                                                                                                                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>• NG-SWG</li> <li>• CASB</li> <li>• Public Cloud Security</li> <li>• ZTNA Next</li> <li>• Device Intelligence</li> <li>• SD-WAN</li> </ul> |

| Function             | Category                                                                                                                                                                                                                                                                                                             | Subcategory                                                                                                   | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Products                                                                                                                                                                |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IDENTIFY (ID)</b> | <b>Asset Management (ID.AM):</b><br>Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | <b>ID.AM-07:</b><br>Inventories of data and corresponding metadata for designated data types are maintained.  | <p>Netskope products offer controls to identify and protect information assets, including assets across web and cloud applications, cloud infrastructure, on-prem servers and endpoint devices. These controls can be used to create an inventory of information assets across managed and unmanaged devices using DLP discovery controls.</p> <p>Netskope offers controls to identify labeled classified data and metadata and can associate policies to protect this information. In addition, Netskope can apply controls around unclassified data and metadata based on its DLP engine, including fingerprinting and natural language processing.</p>                                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• NG-SWG</li> <li>• CASB</li> <li>• DLP</li> <li>• Public Cloud Security</li> <li>• Device Intelligence</li> </ul>               |
|                      |                                                                                                                                                                                                                                                                                                                      | <b>ID.AM-08:</b><br>Systems, hardware, software, services, and data are managed throughout their life cycles. | <p>Netskope products identify and catalog cloud apps and services in use by the organization.</p> <p>Additionally, Netskope's Public Cloud Security product enables organizations to develop and maintain a baseline configuration of their AWS, Azure, and GCP environments..</p> <p>Netskope CSPM can alert when cloud infrastructure deviates from the baseline, and can be configured to remediate any detected misconfigurations. Netskope SSPM provides the same functionality for managed SaaS applications.</p> <p>Netskope DLP can be used to identify data through discovery and identify last access date. This is helpful in identifying the lifecycle of data.</p> <p>Netskope Device Intelligence can also be leveraged to identify hardware (including IoT, OT and traditional devices) and manage devices and connectivity, useful for rogue or EOL devices.</p> | <ul style="list-style-type: none"> <li>• CASB</li> <li>• Public Cloud Security</li> <li>• DLP</li> <li>• CSPM</li> <li>• SSPM</li> <li>• Device Intelligence</li> </ul> |



| Function             | Category                                                                                                                                  | Subcategory                                                                                            | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Products                                                                                                                                                                   |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IDENTIFY (ID)</b> | <b>Risk Assessment (ID.RA):</b><br>The cybersecurity risk to the organization, assets, and individuals is understood by the organization. | <b>ID.RA-01:</b><br>Vulnerabilities in assets are identified, validated, and recorded.                 | <p>Netskope products can assist in identifying vulnerable OS and browsers for devices through NG-SWG and CASB including IoT, OT and traditional devices through Device Intelligence.</p> <p>In addition, vulnerabilities and misconfigurations can be discovered through scanning of cloud services, including public cloud (AWS, Azure, GCP) and SaaS using Public Cloud Security and CSPM and DSPM services.</p>                                                                                                                                                                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>• NG-SWG</li> <li>• CASB</li> <li>• Public Cloud Security</li> <li>• CSPM</li> <li>• DSPM</li> <li>• Device Intelligence</li> </ul> |
|                      |                                                                                                                                           | <b>ID.RA-02:</b><br>Cyber threat intelligence is received from information sharing forums and sources. | <p>Netskope Cloud Threat Exchange (CTE) integrates with threat intelligence from open source and commercial information-sharing forums to collect, analyze, and leverage intelligence on known malicious domains and IP addresses as part of the overall threat detection capability.</p> <p>Netskope Cloud Threat Exchange (CTE) also automatically shares IoCs between deployed defenses, including endpoints, SIEMs, SOAR, and IR systems.</p> <p>Netskope Threat Protection, part of NG-SWG, CASB, and other Netskope solutions, also includes multiple threat intelligence feeds. With Advanced Threat Protection, additional sandboxing capabilities are offered to analyze threats in binary form without need for a signature detection.</p> | <ul style="list-style-type: none"> <li>• Cloud Exchange</li> <li>• NG-SWG</li> <li>• CASB</li> <li>• Threat Protection</li> </ul>                                          |
|                      |                                                                                                                                           | <b>ID.RA-03:</b><br>Internal and external threats to the organization are identified and recorded.     | <p>Netskope products provide a User Confidence Index (UCI) and behavior-based analytics on user activities, which can help organizations identify internal threats including detecting data bulk uploads, downloads, and deletions, plus proximity, failed logins, shared credentials, rare events, risky countries, and data exfiltration between company and personal SaaS instances.</p> <p>Netskope Advanced Threat Protection can detect external malware/ ransomware from web and cloud services and can analyze to block in real time. Netskope provides detailed analysis of the malware type, which can help organizations understand the types of threats and threat actors impacting their organization.</p>                              | <ul style="list-style-type: none"> <li>• NG-SWG</li> <li>• CASB</li> <li>• Advanced Threat Protection</li> <li>• UCI</li> </ul>                                            |

| Function             | Category                                                                                                                                  | Subcategory                                                                                                                                          | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Products                                                                                                                                                                                                     |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IDENTIFY (ID)</b> | <b>Risk Assessment (ID.RA):</b><br>The cybersecurity risk to the organization, assets, and individuals is understood by the organization. | <b>ID.RA-04:</b><br>Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.                             | <p>Netskope products help identify what cloud services are in use within an enterprise, and more importantly how they are being used, including assessing the business impacts of data loss to cloud services and the probable impact if a cloud service itself is compromised.</p> <p>In addition, with Public Cloud Security and CSPM and SSPM, Netskope helps identify the likelihood of a threat exploiting a vulnerability or misconfiguration and includes the capability to remediate.</p> <p>Netskope provides the ability to quantify how much potentially sensitive data resides in cloud services beyond the corporate network perimeter. Netskope also provides the controls required to secure this data or assist the triage in relation to a data exfiltration event.</p> <p>Finally, Netskope ZTNA Next can assist in reducing the attack surface and therefore likelihood, by restricting lateral movement using zero trust principles to limit exposure.</p> | <ul style="list-style-type: none"> <li>• NG-SWG</li> <li>• CASB</li> <li>• Public Cloud Security</li> <li>• Threat Protection</li> <li>• CSPM</li> <li>• SSPM</li> <li>• ZTNA Next</li> <li>• CCI</li> </ul> |
|                      |                                                                                                                                           | <b>ID.RA-05:</b><br>Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization. | Risk information is generated using Netskope products and services and can be further integrated using Netskope Cloud Risk Exchange (CRE), which allows sharing of risk signals for individual users, devices, web and cloud services with other security solutions, assisting with the ability to prioritize risk.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>• All Products</li> </ul>                                                                                                                                             |
|                      |                                                                                                                                           | <b>ID.RA-06:</b><br>Risk responses are chosen, prioritized, planned, tracked, and communicated.                                                      | Risk information is generated using Netskope products and services and can be further integrated using Netskope Cloud Risk Exchange (CRE), which allows sharing of risk signals for individual users, devices, web and cloud services with other security solutions, assisting with the ability to prioritize risk.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>• All Products</li> </ul>                                                                                                                                             |
|                      |                                                                                                                                           | <b>ID.RA-07:</b><br>Changes and exceptions are managed, assessed for risk impact, recorded, and tracked.                                             | The Netskope platform can be integrated with change management solutions. Specific controls and baseline assessments can be completed for cloud infrastructure and cloud services tied to change management and business processes including the ability to add exceptions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <ul style="list-style-type: none"> <li>• All Products</li> </ul>                                                                                                                                             |

| Function             | Category                                                                                                                                                                  | Subcategory                                                                                                                                                        | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Products                                                                                                                                                                                           |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IDENTIFY (ID)</b> | <b>Risk Assessment (ID.RA):</b><br>The cybersecurity risk to the organization, assets, and individuals is understood by the organization.                                 | <b>ID.RA-08:</b><br>Processes for receiving, analyzing, and responding to vulnerability disclosures are established.                                               | Netskope Public Cloud Security and CSPM and SSPM helps identify a vulnerability or misconfiguration and includes the capability to remediate through approved processes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>Public Cloud Security</li> <li>CSPM</li> <li>SSPM</li> </ul>                                                                                                |
|                      |                                                                                                                                                                           | <b>ID.RA-09:</b><br>The authenticity and integrity of hardware and software are assessed prior to acquisition and use.                                             | Netskope Device Intelligence can assist with the authenticity and integrity of hardware. In addition, Netskope Cloud and SaaS Security Posture Management can be used to verify settings and configurations in cloud services and SaaS applications.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>CSPM</li> <li>SSPM</li> <li>Device Intelligence</li> </ul>                                                                                                  |
|                      |                                                                                                                                                                           | <b>ID.RA-10:</b><br>Critical suppliers are assessed prior to acquisition.                                                                                          | Netskope's Cloud Confidence Index (CCI) assigns cloud applications a risk-based score and provides many important details that help organizations assess the risk of using each app or cloud service. Criteria include the vendor's security policies and certifications, audit capabilities, and legal and privacy concerns, among others.                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <ul style="list-style-type: none"> <li>CCI</li> </ul>                                                                                                                                              |
|                      | <b>Improvement (ID.IM):</b><br>Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions. | <b>ID.IM-01:</b><br>Improvements are identified from evaluations.                                                                                                  | Netskope products can assess and evaluate new risks from cloud-based services during evaluation or PoC stage of procurement. Using Netskope Public Cloud Security and/or CSPM/SSPM or even CCI for cloud services, improvements can be recommended prior to procurement or go-live of new service. Ongoing, continuous security checks can be performed.                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>Public Cloud Security</li> <li>CSPM</li> <li>SSPM</li> <li>CCI</li> </ul>                                                                                   |
|                      |                                                                                                                                                                           | <b>ID.IM-02:</b><br>Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties. | <p>The Netskope platform can help organizations prepare for and get the most out of security tests and exercises. For example, Netskope can help organizations define the scope of tests and exercises by inventorying all unmanaged apps and devices in an ICT environment, and assigning risk-based scores.</p> <p>Netskope's Cloud Exchange can assist before and during security tests or exercises. The Cloud Threat Exchange and Cloud Risk Exchange can help identify risky users and assets, and provide up to the minute intel on various threats and vulnerabilities.</p> <p>Meanwhile, Netskope's Cloud Log Shipper (CLS) and Cloud Ticket Orchestrator (CTO) enable a comprehensive, bird's-eye view of any attack - real or simulated - and help streamline an organization's response.</p> | <ul style="list-style-type: none"> <li>NG-SWG</li> <li>CASB</li> <li>Public Cloud Security</li> <li>DLP</li> <li>Cloud Exchange</li> <li>RBI</li> <li>Cloud Firewall</li> <li>ZTNA Next</li> </ul> |

| Function             | Category                                                                                                                                                                  | Subcategory                                                                                                                                               | Netskope Reference                                                                                                                                                                                                                                                                                                                                               | Products                                                                                                         |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>IDENTIFY (ID)</b> | <b>Improvement (ID.IM):</b><br>Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions. | <b>ID.IM-03:</b><br>Improvements are identified from execution of operational processes, procedures, and activities..                                     | Netskope products can assess and evaluate new risks from cloud-based services during evaluation or PoC stage of procurement. Using Netskope Public Cloud Security and/or CSPM/SSPM or even CCI for cloud services, improvements can be recommended prior to procurement or go-live of new service. Ongoing, continuous security checks can also be performed.    | <ul style="list-style-type: none"> <li>Public Cloud Security</li> <li>CSPM</li> <li>SSPM</li> <li>CCI</li> </ul> |
|                      |                                                                                                                                                                           | <b>ID.IM-04:</b><br>Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved. | <p>The Netskope platform has built-in ticketing systems, log analysis, forensic reporting, and advanced analytics capabilities to help organizations respond in case of a security incident.</p> <p>Moreover, Netskope leverages machine learning and artificial intelligence to help identify new anomalies or security events based on previous incidents.</p> | <ul style="list-style-type: none"> <li>All Products</li> </ul>                                                   |

| Function            | Category                                                                                                                                                                                                                                        | Subcategory                                                                                                                  | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Products                                                                                                                                             |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PROTECT (PR)</b> | <b>Identity Management, Authentication, and Access Control (PR.AA):</b><br>Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access. | <b>PR.AA-01:</b><br>Identities and credentials for authorized users, services, and hardware are managed by the organization. | <p>Netskope NG-SWG, CASB and ZTNA Next provides auditing and verification of user identities and credentials.</p> <p>Netskope Public Cloud Security provides discovery of identities and credentials in public cloud services including AWS, Azure, GCP.</p> <p>Netskope’s Cloud Security Posture Management and SaaS Security Posture Management also provide security configuration, auditing, compliance, and company checks for user identities in cloud services and managed SaaS apps.</p> | <ul style="list-style-type: none"> <li>NG-SWG</li> <li>CASB</li> <li>Public Cloud Security</li> <li>ZTNA Next</li> <li>CSPM</li> <li>SSPM</li> </ul> |
|                     |                                                                                                                                                                                                                                                 | <b>PR.AA-02:</b><br>Identities are proofed and bound to credentials based on the context of interactions.                    | <p>Netskope NG-SWG, CASB and ZTNA Next provides detailed logging of all web, cloud and on-prem access activity by users, including inline app and cloud service API-level.</p> <p>This detailed activity level of logging and proxy transaction events will assist organizations in asserting non-repudiation for actions in their web, cloud and on-prem applications.</p>                                                                                                                      | <ul style="list-style-type: none"> <li>NG-SWG</li> <li>CASB</li> <li>Public Cloud Security</li> <li>ZTNA Next</li> </ul>                             |

| Function            | Category                                                                                                                                                                                                                                        | Subcategory                                                                    | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Products                                                                                                                                                                                      |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PROTECT (PR)</b> | <b>Identity Management, Authentication, and Access Control (PR.AA):</b><br>Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access. | <b>PR.AA-03:</b><br>Users, services, and hardware are authenticated.           | <p>Netskope products extend SSO/MFA across web, managed and unmanaged apps and cloud services, and can detect more than 100 inline actions within cloud services and SaaS applications, such as login, logout, view, browse, post, upload, delete, or download.</p> <p>When an action is detected, such as an upload of company data to a non-managed cloud service or application, Netskope can enforce a MFA step-up verification to confirm the activity is being performed by the actual user.</p> <p>Adaptive policy controls can also leverage Netskope’s Cloud Confidence Index (CCI) ratings for apps and Netskope’s User Confidence Index (UCI) risk scoring for the user to determine what is permitted.</p> <p>Device intelligence can also monitor IoT, OT and traditional devices for authentication.</p> | <ul style="list-style-type: none"> <li>• NG-SWG</li> <li>• CASB</li> <li>• Public Cloud Security</li> <li>• ZTNA Next</li> <li>• CCI</li> <li>• UCI</li> <li>• Device Intelligence</li> </ul> |
|                     |                                                                                                                                                                                                                                                 | <b>PR.AA-04:</b><br>Identity assertions are protected, conveyed, and verified. | <p>The Netskope platform integrates with third party identity providers like Okta, Ping, Google, Microsoft to manage secure and secret authentication, including support for SAML, SSO, and MFA.</p> <p>Authentication activities are logged in transaction log data with the Netskope platform to validate additional identity assertions.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• All Products</li> </ul>                                                                                                                              |

| Function     | Category                                                                                                                                                                                                                                        | Subcategory                                                                                                                                                                                                    | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Products                                                                                                                                                                                        |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PROTECT (PR) | <b>Identity Management, Authentication, and Access Control (PR.AA):</b><br>Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access. | <b>PR.AA-05:</b><br>Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties. | <p>Netskope products provide granular and adaptive policy controls with the ability to allow or block specific activities within an application, ensuring that access control permissions are not granted excessively and adhere to the principle of least privilege.</p> <p>When access to a cloud service or cloud application is granted, administrators can differentiate between personal, third-party, and corporate-owned instances of the same managed app and adjust policy controls accordingly.</p> <p>Activity controls can be implemented for both corporate-owned devices for web, SaaS, Shadow IT, and IaaS/PaaS, as well as personal devices accessing corporate-managed apps and cloud services.</p> <p>Netskope Zero Trust Network Access (ZTNA) ensures that remote users only have access to the private applications that are provisioned via policy through an outbound connection, without the need for full network access and inbound access rules.</p> | <ul style="list-style-type: none"> <li>• ZTNA Next</li> <li>• CASB</li> <li>• NG-SWG</li> <li>• Public Cloud Security</li> <li>• CSPM</li> <li>• SSPM</li> <li>• Device Intelligence</li> </ul> |
|              |                                                                                                                                                                                                                                                 | <b>PR.AA-06:</b><br>Physical access to assets is managed, monitored, and enforced commensurate with risk.                                                                                                      | Netskope does not map to this subcategory however logging can be used alongside CCTV and physical security controls to validate activity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• N/A</li> </ul>                                                                                                                                         |
|              | <b>Awareness and Training (PR.AT):</b><br>The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks.                                                       | <b>PR.AT-01:</b><br>Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.                                | <p>Netskope products can provide real-time user coaching when performing actions in Web or Cloud services. Netskope can coach users on data loss risks, including providing users the option to proceed with the action, cancel the action, or provide a business justification. These controls can be applied to managed and unmanaged apps and websites, so business processes can continue.</p> <p>Netskope can also redirect users to third party solutions for just-in-time training, reflecting the combination of the attempted activity and the users' perceived danger level to the company.</p>                                                                                                                                                                                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• NG-SWG</li> <li>• CASB</li> <li>• ZTNA Next</li> </ul>                                                                                                 |

| Function            | Category                                                                                                                                                                                  | Subcategory                                                                                                                                                                                             | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Products                                                                                                                                                         |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PROTECT (PR)</b> | <b>Awareness and Training (PR.AT):</b><br>The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks. | <b>PR.AT-02:</b><br>Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind. | <p>Netskope products can provide real-time user coaching when performing actions in Web or Cloud services. Netskope can coach users on data loss risks, including providing users the option to proceed with the action, cancel the action, or provide a business justification. These controls can be applied to managed and unmanaged apps and websites, so business processes can continue.</p> <p>For specialized roles, such as system administrators, Netskope also provides support for alerting on misconfigurations and vulnerabilities with recommendations on how to remediate using Public Cloud Security and CSPM/SSPM products. .</p>                                                                                    | <ul style="list-style-type: none"> <li>• NG-SWG</li> <li>• CASB</li> <li>• Public Cloud Security</li> <li>• CSPM</li> <li>• SSPM</li> <li>• ZTNA Next</li> </ul> |
|                     | <b>Data Security (PR.DS):</b><br>Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.            | <b>PR.DS-01:</b><br>The confidentiality, integrity, and availability of data-at-rest are protected.                                                                                                     | <p>Netskope products provide data-at-rest scanning and protection capabilities for IT-managed SaaS and IaaS applications and endpoint devices. This includes the ability to perform data loss prevention scans, which can alert on DLP violations and take corrective action.</p> <p>Netskope products can be configured to automatically revoke sharing permissions or encrypt a file, for example if a file containing sensitive information is being shared excessively.</p>                                                                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• CASB</li> <li>• DLP</li> <li>• Public Cloud Security</li> </ul>                                                         |
|                     |                                                                                                                                                                                           | <b>PR.DS-02:</b><br>The confidentiality, integrity, and availability of data-in-transit are protected.                                                                                                  | <p>Netskope products provide the ability to enforce real-time controls on data-in-transit across all SaaS, IaaS, and web usage within the enterprise, including widely adopted Shadow IT apps and cloud services and endpoint devices.</p> <p>Netskope cloud-hosted, enterprise-grade data loss prevention capabilities ensure that data is protected in transit anywhere in the enterprise, including when flowing to and from remote users.</p> <p>Netskope's DLP engine is fully integrated into the entire cloud platform, ensuring that both data-at-rest and data-in-transit are protected by the same set of policies and workflows. This ensures that policy is easy to implement and the DLP program is easy to maintain.</p> | <ul style="list-style-type: none"> <li>• CASB</li> <li>• DLP</li> <li>• Public Cloud Security</li> </ul>                                                         |

| Function            | Category                                                                                                                                                                                                                                                                                  | Subcategory                                                                                        | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Products                                                                                                                                                       |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PROTECT (PR)</b> | <b>Data Security (PR.DS):</b><br>Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.                                                                                                            | <b>PR.DS-10:</b><br>The confidentiality, integrity, and availability of data-in-use are protected. | <p>Netskope products are constructed specifically to address key gaps existing in traditional security stacks. With the continuous adoption of SaaS apps and cloud services for data hosting and storage, Netskope is also able to enforce real-time protections on data-in-motion to unsanctioned, user-adopted Shadow IT applications.</p> <p>Netskope provides this capability for thousands of cloud-hosted SaaS applications and cloud services. Netskope leverages a global-scale, cloud-native security platform to implement security controls in the cloud for any user, device, or location.</p> <p>In addition, Netskope's endpoint DLP provides monitoring and protection for endpoint data in use, including device control for USB storage devices.</p>                                                                                                                                                                | <ul style="list-style-type: none"> <li>CASB</li> <li>DLP</li> <li>Public Cloud Security</li> </ul>                                                             |
|                     |                                                                                                                                                                                                                                                                                           | <b>PR.DS-11:</b><br>Backups of data are created, protected, maintained, and tested.                | <p>Netskope products can discover information assets across cloud applications and endpoint devices and can identify data duplication from backups.</p> <p>In addition, Netskope offers legal hold capabilities that allow for the preservation of data in a forensic repository for legal requirements.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <ul style="list-style-type: none"> <li>NG-SWG</li> <li>CASB</li> <li>DLP</li> <li>Public Cloud Security</li> </ul>                                             |
|                     | <b>Platform Security (PR.PS):</b><br>The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability. | <b>PR.PS-01:</b><br>Configuration management practices are established and applied.                | <p>Netskope Cloud Security Posture Management enables organizations to develop and maintain a baseline configuration of their AWS, Azure, and GCP environments. CSPM provides assessments pursuant to common security and regulatory frameworks, such as CIS, PCI, NIST, and HIPAA and can alert when cloud infrastructure deviates from the baseline, and can be configured to remediate any detected misconfigurations.</p> <p>Netskope SaaS Security Posture Management provides the same functionality for managed SaaS applications.</p> <p>Netskope NG-SWG provides inline IaaS/PaaS user traffic analysis for more than 250 AWS services and more than 9000 APIs, plus similar inline functionality for GCP and Azure environments.</p> <p>Netskope Device Intelligence identifies rogue devices on networks including IoT, OT and traditional devices and can assist in identifying misconfigured or vulnerable systems.</p> | <ul style="list-style-type: none"> <li>Public Cloud Security</li> <li>CSPM</li> <li>SSPM</li> <li>NG-SWG</li> <li>CASB</li> <li>Device Intelligence</li> </ul> |



| Function            | Category                                                                                                                                                                                                                                                                                  | Subcategory                                                                                 | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Products                                                                                                                                                                               |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PROTECT (PR)</b> | <b>Platform Security (PR.PS):</b><br>The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability. | <b>PR.PS-02:</b><br>Software is maintained, replaced, and removed commensurate with risk.   | <p>Netskope's Cloud Confidence Index (CCI) provides a risk-based score to over 85,000 cloud applications.</p> <p>Organizations can adjust the default score of an app by emphasizing or de-emphasizing risk elements that are more or less important to the organization, such as the need to comply with specific regulatory regimes like GDPR.</p> <p>Netskope CCI can be used in conjunction with Public Cloud Security, CSPM, SSPM and DLP to maintain a record of cloud based services (both public cloud and SaaS) and Device Intelligence for on-prem devices and can identify risks associated with each service and report with Advanced Analytics to further rationalize use of key software services..</p> | <ul style="list-style-type: none"> <li>Public Cloud Security</li> <li>CCI</li> <li>CSPM</li> <li>SSPM</li> <li>DLP</li> <li>Device Intelligence</li> <li>Advanced Analytics</li> </ul> |
|                     |                                                                                                                                                                                                                                                                                           | <b>PR.PS-03:</b><br>Hardware is maintained, replaced, and removed commensurate with risk.   | Netskope Device Intelligence identifies rogue devices on networks including IoT, OT and traditional devices and can assist in identifying misconfigured or vulnerable systems or systems that are EOL.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>Device Intelligence</li> </ul>                                                                                                                  |
|                     |                                                                                                                                                                                                                                                                                           | <b>PR.PS-04:</b><br>Log records are generated and made available for continuous monitoring. | <p>The Netskope platform generates transaction log data across web, cloud, on-prem and device summarizing activity and reporting on this activity continuously.</p> <p>Furthermore, policy violations and other alerts are logged and workflows are implemented into the console to ensure records can be reviewed efficiently.</p> <p>Activity logs and alerts can be exported to other platforms (such as SIEM and SOAR platforms) with the Cloud Log Shipper tool, or used to automatically create service tickets with Netskope's Cloud Ticket Orchestrator (CTO) tool. Proxy transaction events can be streamed to cloud storage or SIEMs in near real-time.</p>                                                 | <ul style="list-style-type: none"> <li>All Products</li> </ul>                                                                                                                         |

| Function            | Category                                                                                                                                                                                                                                                                                  | Subcategory                                                                                                                                                  | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Products                                                                                                                                                                                         |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PROTECT (PR)</b> | <b>Platform Security (PR.PS):</b><br>The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability. | <b>PR.PS-05:</b><br>Installation and execution of unauthorized software are prevented.                                                                       | <p>Netskope NG-SWG Advanced Threat Protection provides anti-malware detection, bare-metal and cloud sandboxing, and ML-based detection to detect and prevent malicious code being executed. It also provides pre-execution analysis and heuristics for more than 3,500 file format families for Windows, Mac OS, Linux, iOS, Android, firmware, Flash, PDF, and other document types.</p> <p>Netskope API-based IaaS Storage Scan can scan cloud storage buckets and blogs to detect unauthorized changes to cloud storage data, including detecting if legitimate software has been replaced with malware.</p> <p>Netskope's Remote Browser Isolation ensures no malicious code is executed in an organization's environment. RBI works by executing web server code in cloud storage containers, and reproducing the resulting web page as an interactive pixel-rendered image. RBI ensures no executable code makes it from a web server to an end-user's system, essentially creating an "air gap," ensuring complete safety for viewing web pages browsed through RBI.</p> | <ul style="list-style-type: none"> <li>• NG-SWG</li> <li>• CASB</li> <li>• Public Cloud Security</li> <li>• CSPM</li> <li>• SSPM</li> <li>• Advanced Threat Protection</li> <li>• RBI</li> </ul> |
|                     |                                                                                                                                                                                                                                                                                           | <b>PR.PS-06:</b><br>Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle. | <p>Netskope products can be used to manage access to apps and services used during SDLC, such as GitHub and Public Cloud. With instance awareness, services can also be managed to separate development, test, and production environments.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>• NG-SWG</li> <li>• CASB</li> <li>• Public Cloud Security</li> <li>• ZTNA Next</li> <li>• Cloud Firewall</li> </ul>                                       |

| Function            | Category                                                                                                                                                                                                                       | Subcategory                                                                                                         | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Products                                                                                                                                                          |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PROTECT (PR)</b> | <b>Technology Infrastructure Resilience (PR.IR):</b><br>Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience. | <b>PR.IR-01:</b><br>Networks and environments are protected from unauthorized logical access and usage.             | <p>Netskope Zero Trust Network Access (ZTNA Next) protects private networks through a Zero Trust model. This ensures that remote users access only the applications they have been provisioned and do not gain remote access to the internal network (such as occurs with a VPN).</p> <p>Netskope NG-SWG advanced Threat Protection provides real-time malware detection and IPS capabilities for organizational web traffic, incorporating threat intelligence to detect malicious web traffic traversing an organization's network.</p> <p>Netskope's Cloud Firewall (CFW) provides firewall policies for egress traffic across ports and protocols for users and offices.</p> <p>Netskope's Borderless SD-WAN provides site-to-site connectivity including options to segment networks and environments and manage logical access.</p> | <ul style="list-style-type: none"> <li>• ZTNA Next</li> <li>• NG-SWG</li> <li>• Advanced Threat Protection</li> <li>• Cloud Firewall</li> <li>• SD-WAN</li> </ul> |
|                     |                                                                                                                                                                                                                                | <b>PR.IR-02:</b><br>The organization's technology assets are protected from environmental threats.                  | Netskope does not map to this subcategory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>• N/A</li> </ul>                                                                                                           |
|                     |                                                                                                                                                                                                                                | <b>PR.IR-03:</b><br>Mechanisms are implemented to achieve resilience requirements in normal and adverse situations. | Netskope products support resilience requirements in both normal and adverse conditions including the ability to both scale up and scale down on demand. Netskope supports a 99.999% SLA on availability.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>• All Products</li> <li>• SD-WAN</li> </ul>                                                                                |
|                     |                                                                                                                                                                                                                                | <b>PR.IR-04:</b><br>Adequate resource capacity to ensure availability is maintained.                                | <p>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 including ability to both scale up and scale down on demand. Netskope supports a 99.999% SLA on availability.</p> <p>In addition, Netskope Borderless SD-WAN offers hot standby at remote sites to help achieve resilience requirements at remote locations.</p>                                                                                                                                                                                                                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>• All Products</li> <li>• SD-WAN</li> </ul>                                                                                |

| Function           | Category                                                                                                                                         | Subcategory                                                                                                   | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Products                                                       |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| <b>DETECT (DE)</b> | <b>Continuous Monitoring (DE.CM):</b><br>Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events. | <b>DE.CM-01:</b><br>Networks and network services are monitored to find potentially adverse events.           | <p>The Netskope platform can assist monitoring for adverse events across the ecosystem of networks, public cloud, SaaS and devices.</p> <p>Events are created across a suite of products and can be assessed by either Proactive Digital Experience Monitoring or Cloud Firewall, or SD-WAN depending on the event and traffic profile. The same approach is taken for web, cloud and on-prem apps and services.</p> <p>Advanced analytics can also be used to assess trends and assist in identifying potential adverse events and anomalies.</p> <p>Cloud Exchange can be leveraged to extend and share event data across the ecosystem of network and security tools.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>All Products</li> </ul> |
|                    |                                                                                                                                                  | <b>DE.CM-02:</b><br>The physical environment is monitored to find potentially adverse events.                 | Netskope does not map to this subcategory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <ul style="list-style-type: none"> <li>N/A</li> </ul>          |
|                    |                                                                                                                                                  | <b>DE.CM-03:</b><br>Personnel activity and technology usage are monitored to find potentially adverse events. | <p>The Netskope platform provides a significant amount of visibility to administrators whilst supporting privacy-by-design.</p> <p>Netskope products can be configured to secure activity to Web, SaaS, IaaS, and egress traffic from on-network and remote users, but also secures app and cloud service activity to the extent that specific user actions (such as share, edit, delete, upload, download, etc.) within cloud apps are recorded. Netskope's unique ability to decode inline unpublished API calls and JSON streams to secure user activity in real time across apps and cloud services, including by instance (i.e. company vs. personal).</p> <p>Threat protection and Data protection (DLP) components are also used to identify activities that may be malicious such as intentionally downloading malicious code or attempting to exfiltrate data. In addition, configuration of public cloud and SaaS services can also be monitored to assist in identifying accidental or intentional misconfigurations.</p> <p>Cloud Exchange can be leveraged to extend and share activity data across an ecosystem of network and security tools.</p> | <ul style="list-style-type: none"> <li>All Products</li> </ul> |

| Function           | Category                                                                                                                                                                                        | Subcategory                                                                                                                                 | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Products                                                                                                                                                                                        |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DETECT (DE)</b> | <b>Continuous Monitoring (DE.CM):</b><br>Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events.                                                | <b>DE.CM-06:</b><br>External service provider activities and services are monitored to find potentially adverse events.                     | <p>Netskope Zero Trust Network Access (ZTNA) can monitor external service provider access to internal resources.</p> <p>Netskope products can also monitor activity from Public Cloud and SaaS provider activity logs via API integration, and inline end-user activity for both managed and unmanaged services by identifying user actions (e.g. edit, share, delete, upload, reboot, etc.) via forward proxy.</p> <p>Reverse proxy capabilities even allow for inline enforcement on non-corporate devices accessing corporate SaaS applications.</p>                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• ZTNA</li> <li>• Public Cloud Security</li> <li>• CASB</li> </ul>                                                                                       |
|                    |                                                                                                                                                                                                 | <b>DE.CM-09:</b><br>Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events. | <p>Netskope products can assist in monitoring use of systems and networks and can be used to detect anomalous behavior with policies set to take action to prevent security incidents for both outbound and inbound network, system, and application traffic.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <ul style="list-style-type: none"> <li>• NG-SWG</li> <li>• CASB</li> <li>• Public Cloud Security</li> <li>• ZTNA Next</li> <li>• DLP</li> <li>• Advanced Analytics</li> <li>• SD-WAN</li> </ul> |
|                    | <b>Adverse Event Analysis (DE.AE):</b><br>Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents. | <b>DE.AE-02:</b><br>Potentially adverse events are analyzed to better understand associated activities.                                     | <p>Netskope products help with identifying adverse events by logging activity with a set of details in order to provide critical context to events that may be involved in an incident.</p> <p>This includes information such as the device the event occurred on, the user, the app or service being accessed, the activity (such as a share, upload, delete, etc.), the data and many other important criteria.</p> <p>With Netskope's Advanced Analytics, events can be analyzed against trends and baseline activity to understand unusual and adverse events.</p> <p>Cloud exchange can also be leveraged to share indicators and signals relating to other systems and tools to further identify anomalies and IOCs.</p> | <ul style="list-style-type: none"> <li>• SASE</li> <li>• Cloud Exchange</li> <li>• Advanced Analytics</li> </ul>                                                                                |

| Function           | Category                                                                                                                                                                                        | Subcategory                                                                                  | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Products                                                                                                                                                                      |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DETECT (DE)</b> | <b>Adverse Event Analysis (DE.AE):</b><br>Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents. | <b>DE.AE-03:</b><br>Information is correlated from multiple sources.                         | Netskope's open architecture and Cloud Exchange tool enables third-party integration with market-leading security services, including Splunk, CrowdStrike, QRadar, Rapid7, Exabeam, AWS, Google, Microsoft, Sumologic, LogRhythm and many more.<br><br>Customers can integrate their Netskope deployment with existing solutions within their environment to ensure that the detailed data generated by Netskope is collected and correlated.                                                                                                                                                                                                                                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>• SASE</li> <li>• Cloud Exchange</li> <li>• Advanced Analytics</li> </ul>                                                              |
|                    |                                                                                                                                                                                                 | <b>DE.AE-04:</b><br>The estimated impact and scope of adverse events are understood.         | <p>With Netskope products, security teams are able to map communication and data flows. This can help understand the impact of an incident if it occurs within an app utilized by the organization, whether managed or unmanaged, and whether the instance is corporate or personal.</p> <p>This is supported by Netskope's Threat protection and DLP capabilities to help organizations understand and estimate the likelihood and impact of an adverse event.</p> <p>Netskope Cloud Risk Exchange can also be used to leverage additional adverse events from other services to support the assessment of the impact of an event.</p> <p>In addition, Netskope's Proactive Digital Experience Management (P-DEM) provides visibility and actionable insights on network and cloud performance to ensure the best user and app experience.</p> | <ul style="list-style-type: none"> <li>• SASE</li> <li>• Threat Protection</li> <li>• DLP</li> <li>• Cloud Exchange</li> <li>• P-DEM</li> <li>• Advanced Analytics</li> </ul> |
|                    |                                                                                                                                                                                                 | <b>DE.AE-06:</b><br>Information on adverse events is provided to authorized staff and tools. | <p>Netskope products provide security and network teams with a high degree of visibility into user activity on the web, SaaS, and IaaS. This activity can be distributed through a variety of means, including high-level reports, advanced analytics, detailed event logs, and even exported using Netskope's Cloud Log Shipper or near-real time transaction event streaming to third party tools (e.g., SIEM, UBA, XDR or SOAR services).</p> <p>Netskope's Proactive Digital Experience Management (P-DEM) provides broader visibility on network and cloud performance, granular insights into user experience, traffic patterns, app usage, and even Netskope Client adoption.</p>                                                                                                                                                        | <ul style="list-style-type: none"> <li>• SASE</li> <li>• Threat Protection</li> <li>• DLP</li> <li>• Cloud Exchange</li> <li>• P-DEM</li> <li>• Advanced Analytics</li> </ul> |

| Function           | Category                                                                                                                                                                                        | Subcategory                                                                                                      | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Products                                                                                                                                                                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DETECT (DE)</b> | <b>Adverse Event Analysis (DE.AE):</b><br>Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents. | <b>DE.AE-07:</b><br>Cyber threat intelligence and other contextual information are integrated into the analysis. | Netskope products support creation and ingestion of Cyber Threat Intelligence (CTI) and can detect and block activity that is considered malicious. Netskope's predefined conditions, rules, and machine-learning technology including Advanced Threat Protection and DLP, assist in providing context to event information.<br><br>APIs are provided for sandboxing and retrospective hunting, and the various modules of Netskope's Cloud Exchange perform threat intel sharing, log export, risk score exchange, and workflow automation. Furthermore, MITRE ATT&CK analysis is incorporated into sandboxing reports. | <ul style="list-style-type: none"> <li>• NG-SWG</li> <li>• Threat Protection</li> <li>• Advanced Threat Protection</li> <li>• SkopeAI</li> <li>• DLP</li> <li>• Cloud Exchange</li> <li>• Public Cloud Security</li> <li>• Advanced Analytics</li> </ul> |
|                    |                                                                                                                                                                                                 | <b>DE.AE-08:</b><br>Incidents are declared when adverse events meet the defined incident criteria.               | Netskope products provide customizable alert thresholds for malware detection, unauthorized actions, DLP, malicious sites, and compromised credentials. Alert thresholds can be configured for anomaly detections, such as large file uploads, downloads, and deletions.                                                                                                                                                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>• All Products</li> </ul>                                                                                                                                                                                         |

| Function            | Category                                                                                          | Subcategory                                                                                                                          | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Products                                                                                                                                                            |
|---------------------|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RESPOND (RS)</b> | <b>Incident Management (RS.MA):</b><br>Responses to detected cybersecurity incidents are managed. | <b>RS.MA-01:</b><br>The incident response plan is executed in coordination with relevant third parties once an incident is declared. | <p>Netskope products can be configured to collate and report on events and generate alerts on a series of suspicious events.</p> <p>Netskope has built-in ticketing systems, log analysis, forensic reporting, and advanced analytics capabilities to help an organization in the event of a security incident.</p> <p>Netskope also offers Role-Based Access Control that supports role-based access based on an organization's RACI policy or similar requirements to support responsibilities and procedures in the event of a security incident. Multiple levels of access, including data obfuscation, can be used to protect incident data on a need-to-know basis.</p> <p>Netskope ZTNA Next also allows for third-parties to securely connect to environments for triage and also secure access to security incident reports.</p> | <ul style="list-style-type: none"> <li>• SASE</li> <li>• Advanced Analytics</li> <li>• Skope AI</li> <li>• Cloud Exchange</li> <li>• Device Intelligence</li> </ul> |

| Function            | Category                                                                                          | Subcategory                                                                                                                          | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Products                                                                                                                                                            |
|---------------------|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RESPOND (RS)</b> | <b>Incident Management (RS.MA):</b><br>Responses to detected cybersecurity incidents are managed. | <b>RS.MA-01:</b><br>The incident response plan is executed in coordination with relevant third parties once an incident is declared. | <p>Netskope products can be configured to collate and report on events and generate alerts on a series of suspicious events.</p> <p>Netskope has built-in ticketing systems, log analysis, forensic reporting, and advanced analytics capabilities to help an organization in the event of a security incident.</p> <p>Netskope also offers Role-Based Access Control that supports role-based access based on an organization's RACI policy or similar requirements to support responsibilities and procedures in the event of a security incident. Multiple levels of access, including data obfuscation, can be used to protect incident data on a need-to-know basis.</p> <p>Netskope ZTNA Next also allows for third-parties to securely connect to environments for triage and also secure access to security incident reports.</p> | <ul style="list-style-type: none"> <li>• SASE</li> <li>• Advanced Analytics</li> <li>• Skope AI</li> <li>• Cloud Exchange</li> <li>• Device Intelligence</li> </ul> |
|                     |                                                                                                   | <b>RS.MA-02:</b><br>Incident reports are triaged and validated.                                                                      | <p>Netskope products can help with incident report creation providing context to improve triage response times and mitigation through reporting and Advanced Analytics.</p> <p>Netskope products can integrate with the customer's SIEM via near real-time transaction event streaming, Cloud Log Shipper, and SOAR tools with Netskope's Cloud Ticket Orchestrator (CTO), which can generate alerts or tickets based on incident notifications from Netskope. Reports can be directly generated on notification from SIEM and SOAR systems and investigated via the Netskope console.</p>                                                                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>• SASE</li> <li>• Advanced Analytics</li> <li>• Cloud Exchange</li> </ul>                                                    |
|                     |                                                                                                   | <b>RS.MA-03:</b><br>Incidents are categorized and prioritized.                                                                       | <p>Netskope incident severity can be set by the organization, in accordance with existing severity and incident categorization criteria. This enables organizations to have consistent categorization across tools and response plans.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>• SASE</li> <li>• Advanced Analytics</li> <li>• Cloud Exchange</li> </ul>                                                    |
|                     |                                                                                                   | <b>RS.MA-04:</b><br>Incidents are escalated or elevated as needed.                                                                   | <p>Netskope Cloud Ticket Orchestrator (CTO) enables the automatic creation of tickets in IT Service Management solutions and collaboration systems from events.</p> <p>Netskope's Advanced Analytics can be used to relevant incident response</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• SASE</li> <li>• Cloud Exchange</li> <li>• Advanced Analytics</li> </ul>                                                    |



| Function            | Category                                                                                                                             | Subcategory                                                                                                                                   | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Products                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RESPOND (RS)</b> | <b>Incident Management (RS.MA):</b><br>Responses to detected cybersecurity incidents are managed.                                    | <b>RS.MA-05:</b><br>The criteria for initiating incident recovery are applied.                                                                | Netskope Cloud Ticket Orchestrator (CTO) allows customers to map customer alerts, events, and log data into whatever format is required to facilitate automated workflows in ServiceNow, Jira, and PagerDuty, or notifications in Slack, Teams, Email, etc.<br><br>Initiating incident recovery is supported across the Netskope SASE service stack including SSE and SD-WAN services enabling organizations to recover quickly without the need to replace hardware or services impacted by incident.                                          | <ul style="list-style-type: none"> <li>• SASE</li> <li>• Cloud Exchange</li> <li>• Advanced Analytics</li> </ul>                                                                                                                                                                                                                                                                                                                             |
|                     |                                                                                                                                      | <b>Incident Analysis (RS.AN):</b><br>Investigations are conducted to ensure effective response and support forensics and recovery activities. | <b>RS.AN-03:</b><br>Analysis is performed to establish what has taken place during an incident and the root cause of the incident.                                                                                                                                                                                                                                                                                                                                                                                                              | Netskope products capture and display key data points that are critical for forensic investigations. This includes activity-level detail for traffic analyzed for web, cloud, network and device access.<br><br>Netskope products can also provide the file-content details of DLP violations so that forensics can be performed on policy violations and to determine root cause of incident both from an insider or external threat actor. |
|                     | <b>RS.AN-06:</b><br>Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved. |                                                                                                                                               | Netskope products record activity performed during incident investigation.<br><br>Furthermore, Netskope offers controls to meet certain legal and compliance requirements including ensuring integrity of logs and accurate timestamps etc for forensic reporting.<br><br>Netskope products also offer a legal hold capability to preserve data in a forensic repository. And Netskope's Data Loss Prevention engine can ensure all records related to a security incident and its investigation are preserved.                                 | <ul style="list-style-type: none"> <li>• SASE</li> <li>• Cloud Exchange</li> <li>• Advanced Analytics</li> </ul>                                                                                                                                                                                                                                                                                                                             |
|                     | <b>RS.AN-07:</b><br>Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved. |                                                                                                                                               | Netskope products allow customers to store forensic data in tools or repositories defined by the customer.<br><br>Furthermore, Netskope offers controls to meet certain legal and compliance requirements including ensuring integrity of logs and accurate timestamps etc for forensic reporting.<br><br>Netskope products also offer a legal hold capability to preserve data in a forensic repository. And Netskope's Data Loss Prevention engine can ensure all records related to a security incident and its investigation are preserved. | <ul style="list-style-type: none"> <li>• SASE</li> <li>• Cloud Exchange</li> <li>• Advanced Analytics</li> </ul>                                                                                                                                                                                                                                                                                                                             |

| Function            | Category                                                                                                                                                                                    | Subcategory                                                                                   | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Products                                                                                                                       |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>RESPOND (RS)</b> | <b>Incident Analysis (RS.AN):</b><br>Investigations are conducted to ensure effective response and support forensics and recovery activities                                                | <b>RS.MA-08:</b><br>An incident's magnitude is estimated and validated.                       | <p>Netskope products provide detailed insights and rich metadata for traffic across web, SaaS, IaaS, and public-facing custom apps and devices.</p> <p>This can significantly help in estimating the magnitude of a cyber incident, including identifying the number of systems, users, data and services impacted by the incident.</p> <p>Reporting on magnitude is possible using reporting and Advanced Analytics.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <ul style="list-style-type: none"> <li>• SASE</li> <li>• Cloud Exchange</li> <li>• Advanced Analytics</li> </ul>               |
|                     | <b>Incident Response Reporting and Communication (RS.CO):</b><br>Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies. | <b>RS.CO-02:</b><br>Internal and external stakeholders are notified of incidents.             | <p>Netskope products support the ability to notify stakeholders of incidents both internal and external.</p> <p>Netskope's threat protection and data protection controls can help identify if data has been compromised and make this information available as part of the follow-up incident response activity, i.e. to inform individuals if their personal data has been compromised.</p> <p>In addition, Netskope's Cloud Exchange allows customers to map customer alerts, events, and log data into whatever format is required to facilitate automated workflows in ServiceNow, Jira, and PagerDuty, or notifications in Slack, Teams, Email, etc.</p>                                                                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>• SASE</li> <li>• Cloud Exchange</li> <li>• DLP</li> <li>• Threat Protection</li> </ul> |
|                     |                                                                                                                                                                                             | <b>RS.CO-03:</b><br>Information is shared with designated internal and external stakeholders. | <p>Netskope products provide both detailed activity logs and high-level reports, so security teams are assured of having the information they need to effectively communicate critical information consistent with the organization's response plan.</p> <p>Using Netskope's ZTNA service, access to information related to an incident can also be shared with external stakeholders, such as third-party incident response teams.</p> <p>Further, Netskope Cloud Threat Exchange (CTE) enables bidirectional threat intelligence sharing. This can be integrated with both open- and closed-source intelligence feeds, ensuring that up-to-date threat intelligence is in the Netskope platform.</p> <p>Netskope Cloud Risk Exchange (CRE) enables the sharing of risk scores for users and devices, normalizing scores, and the ability to trigger actions with Netskope's Cloud Ticket Orchestrator (CTO).</p> | <ul style="list-style-type: none"> <li>• SASE</li> <li>• ZTNA Next</li> <li>• Cloud Exchange</li> </ul>                        |

| Function            | Category                                                                                                                   | Subcategory                                   | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Products                                                                                                                                                     |
|---------------------|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RESPOND (RS)</b> | <b>Incident Mitigation (RS.MI):</b><br>Activities are performed to prevent expansion of an event and mitigate its effects. | <b>RS.MI-01:</b><br>Incidents are contained.  | <p>Netskope inline policy controls ensure that additional restrictions can be enforced in the event of an incident. This could include a restrictive set of policies that can be immediately put in place to ensure particular applications, networks and/or services are not accessed or activities within particular applications are not performed.</p> <p>For example, a non-corporate instance of a SaaS application can be immediately blocked upon discovery of its use in an incident (while still allowing the corporate instance of the same app).</p> <p>Further, using Netskope ZTNA Next, remote access is restricted to apps and services only and ensures incidents are contained rather than allowing laterally movement and expansion which is common with legacy VPN remote access.</p> <p>Netskope Remote Browser Isolation (RBI) can also be used to contain web-based attacks and incidents within a remote browser that is completely isolated from the user's device..</p> | <ul style="list-style-type: none"> <li>• SASE</li> <li>• ZTNA Next</li> <li>• RBI</li> </ul>                                                                 |
|                     |                                                                                                                            | <b>RS.MI-02:</b><br>Incidents are eradicated. | <p>Netskope SASE with Advanced Threat Protection, Remote Browser Isolation, Cloud Firewall, and Client Traffic Exploit Prevention provides active mitigation against malware, high-risk websites, phishing, browser attacks, OS vulnerabilities, and firewall egress controls over all ports and protocols.</p> <p>Further, Netskope Zero Trust Network Access (ZTNA Next) can reduce incidents for organizational applications, protecting and mitigating remote access attacks which can arise from the use of traditional VPNs and compromised RDP, SSH, and legacy remote access solutions.</p>                                                                                                                                                                                                                                                                                                                                                                                               | <ul style="list-style-type: none"> <li>• SASE</li> <li>• Advanced Threat Protection</li> <li>• RBI</li> <li>• Cloud Firewall</li> <li>• ZTNA Next</li> </ul> |

| Function            | Category                                                                                                                                                                                 | Subcategory                                                                                                                                  | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Products                                                                                                                          |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>RECOVER (RC)</b> | <b>Incident Recovery Plan Execution (RC.RP):</b><br>Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents. | <b>RC.RP-01:</b><br>The recovery portion of the incident response plan is executed once initiated from the incident response process.        | The Netskope platform allows the organization to identify and prioritize critical services based on the intensity of their usage by the organization including devices, web and cloud services and remote access.<br><br>Restoration of remote access or restoration of critical services can be supported using Netskope including continuous assessments to ensure services are not further targeted.<br><br>Recovery support is however dependent on the incident in question.  | <ul style="list-style-type: none"> <li>All Products</li> </ul>                                                                    |
|                     |                                                                                                                                                                                          | <b>RC.RP-02:</b><br>Recovery actions are selected, scoped, prioritized, and performed.                                                       | The Netskope platform allows the organization to identify and prioritize critical services based on the intensity of their usage by the organization including devices, web and cloud services and remote access.<br><br>Restoration of remote access or restoration of critical services can be supported using Netskope including continuous assessments to ensure services are not further targeted.<br><br>Recovery support is however dependent on the incident in question.. | <ul style="list-style-type: none"> <li>All Products</li> </ul>                                                                    |
|                     |                                                                                                                                                                                          | <b>RC.RP-03:</b><br>The integrity of backups and other restoration assets is verified before using them for restoration.                     | Netskope's Data Loss Prevention (DLP) tool helps check the integrity of data, using machine learning to accurately and reliably identify, classify, and/or protect sensitive and critical data across an organization's IT ecosystem.<br><br>Furthermore, Netskope's Zero Trust Network Access (ZTNA Next), SD-WAN, and Cloud Firewall capabilities support network segmentation to ensure backups are stored in a secure environment.                                             | <ul style="list-style-type: none"> <li>DLP</li> <li>ZTNA Next</li> <li>SkopeAI</li> <li>SD-WAN</li> <li>Cloud Firewall</li> </ul> |
|                     |                                                                                                                                                                                          | <b>RC.RP-04:</b><br>Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms | The Netskope platform allows the organization to identify and prioritize critical services based on the intensity of their usage by the organization including devices, web and cloud services and remote access.<br><br>Restoration of remote access or restoration of critical services can be supported using Netskope including continuous assessments to ensure services are not further targeted.<br><br>Recovery support is however dependent on the incident in question.  | <ul style="list-style-type: none"> <li>All Products</li> </ul>                                                                    |

| Function            | Category                                                                                                                                                                                 | Subcategory                                                                                                                                                   | Netskope Reference                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Products                                                              |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| <b>RECOVER (RC)</b> | <b>Incident Recovery Plan Execution (RC.RP):</b><br>Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents. | <b>RC.RP-06:</b><br>The end of incident recovery is declared based on criteria, and incident-related documentation is completed.                              | Netskope does not map to this subcategory                                                                                                                                                                                                                                                                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>N/A</li> </ul>                 |
|                     |                                                                                                                                                                                          | <b>RC.CO-03:</b><br>Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders. | <p>The Netskope platform allows the organization to identify and prioritize critical services based on the intensity of their usage by the organization including devices, web and cloud services and remote access.</p> <p>Restoration of remote access or restoration of critical services can be supported using Netskope including continuous assessments to ensure services are not further targeted.</p> <p>Recovery support is however dependent on the incident in question.</p> | <ul style="list-style-type: none"> <li>All Products</li> </ul>        |
|                     |                                                                                                                                                                                          | <b>RC.CO-04:</b><br>Public updates on incident recovery are shared using approved methods and messaging.                                                      | <p>Netskope Data Loss Prevention tool helps ensure that only approved public updates related to incident recovery are released, using machine learning to accurately and reliably identify, classify, and protect sensitive and critical data across an organization.</p>                                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>NG-SWG</li> <li>DLP</li> </ul> |

---

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](https://www.netskope.com).

©2024 Netskope, Inc. All rights reserved. Netskope, NewEdge, SkopeAI, and the stylized “N” logo are registered trademarks of Netskope, Inc. Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks included are trademarks of their respective owners. 07/24 WP-745-1