April 2020

NIST Cybersecurity Framework & Google Cloud

Securing critical infrastructure and managing cybersecurity risks

Table of Contents

Disclaimer

This guide is for informational purposes only. Google does not intend the information or recommendations in this guide to constitute legal advice. Each customer is responsible for independently evaluating its own particular use of the services as appropriate to support its legal compliance obligations.

Intended Audience

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), is a voluntary framework that captures standards, guidelines, and best practices to manage cybersecurity-related risk. This document is for customers who are interested in implementing NIST CSF security best practices in Google Cloud Platform. The Cybersecurity Framework helps to promote the protection and resilience of critical infrastructure. This guide is intended for security officers, compliance officers, IT administrators, and other employees who are responsible for NIST CSF implementation and compliance on Google Cloud Platform. After reading this guide, you will understand how Google is able to support FedRAMP and NIST compliance, as well as understand which Google Cloud products, tools and services to enable to help meet NIST CSF standards and guidelines.

Introduction

In February 2013, Presidential Executive Order 13636 was issued for "Improving Critical Infrastructure Cybersecurity."

As defined by the U.S. Patriot Act of 2001, critical infrastructure includes "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

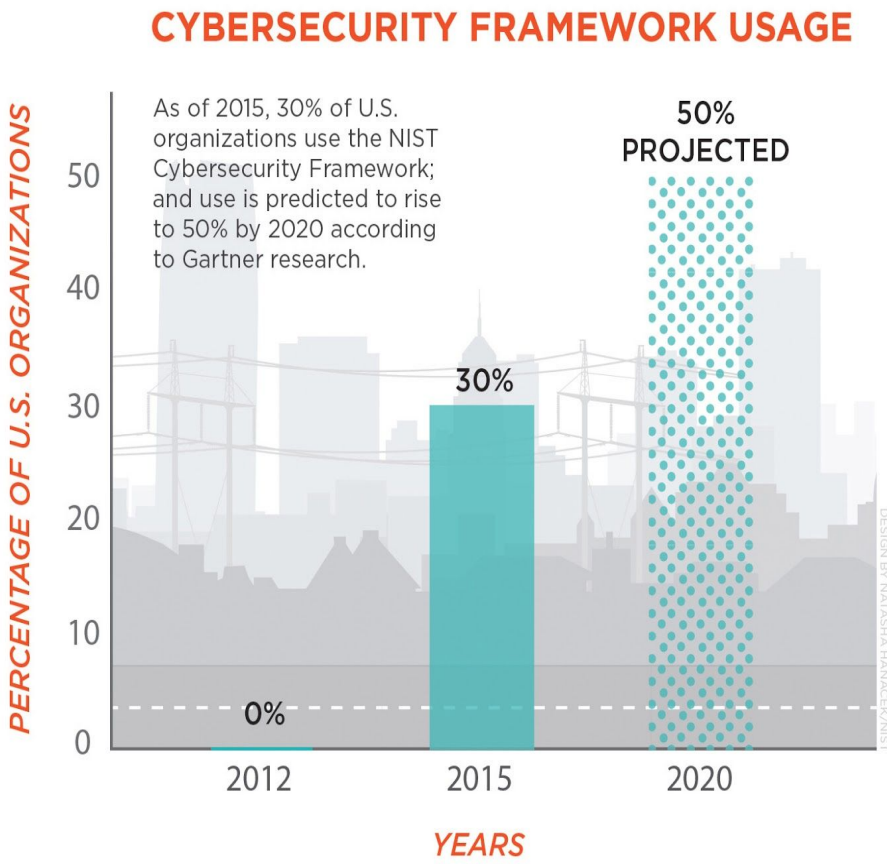
In response to this Executive Order, the Cybersecurity Enhancement Act of 2014 (CEA), identified the National Institute of Standards and Technology (NIST) as the leader in facilitating and supporting the development of cybersecurity risk frameworks. NIST would go on to formalize the Cybersecurity Framework (CSF) - a consistent, iterative approach for organizations to identify, assess, and manage cybersecurity risk.

By May 11, 2017, a Presidential Executive Order was passed requiring Government agencies to implement and enforce the NIST Cybersecurity Framework for all federal networks and critical infrastructure.

The NIST Cybersecurity Framework provides a common mechanism for organizations to:

01	02	03	04	05
Describe their current cybersecurity posture	**Describe their target state for cybersecurity**	**Identify and prioritize a continuous, repeatable process for reaching the target cybersecurity state**	**Assess progress toward the target state**	**Communicate cybersecurity risks to internal and external stakeholders**

As reported by Gartner, 30% of U.S. organizations leveraged the NIST Cybersecurity Framework by 2015, and it is projected that at least 50% will leverage the framework by 2020.



Despite fast-spreading adoption and provisioning of a common taxonomy for securely supporting technical innovation, decisions on how to implement the CSF are still left up to the organization. As quoted by NIST, "The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances." [1] [2]

To help both government and corporate organizations implement the NIST Cybersecurity Framework on Google Cloud, this whitepaper will identify Google Cloud products, services, tools, and offerings that align to each category of the NIST CSF. Organizations will subsequently be able to implement these capabilities on Google Cloud to improve, reinforce, and report on their security baseline, confidently building cybersecurity risk management and resilience into global systems.

[1] NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (source)
[2] Image: NIST Cybersecurity Framework Industry Impact (source)

NIST Cybersecurity Framework

Cybersecurity Framework: Functions

NIST generalizes cybersecurity activities into five core functions: ***Identify***, ***Protect***, ***Detect***, ***Respond***, and ***Recover***. These functions help guide organizations with mapping out the management of cybersecurity risks. Organizations should perform these functions concurrently, continuously, and regularly to establish an operational culture for dynamically addressing cybersecurity risks.

Identify	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. Functions include Asset Management, Governance, Business Environment, Risk Assessment, and Risk Management Strategy
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services. Functions include Identity & Access Management Control, Awareness & Training, Data Security, Maintenance, Protective Technologies, Information Protection Processes & Procedures.
Detect	Detect and implement appropriate activities to identify the occurrence of a cybersecurity event. Functions include Anomalies & Events, Security Continuous Monitoring, and Detection Processes
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. Functions include Response Planning, Communications, Analysis, Mitigation, and Improvements.
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impacted due to a cybersecurity incident. Functions include Recovery Planning, Improvements, and Communications.

Cybersecurity Framework: Categories

Each NIST CSF function spans across multiple categories, which outline the components of the function. These categories cover the cybersecurity risk management areas that should be implemented by organizations. When adopting new technology, including Google Cloud, organizations should leverage products and services that meet the requirements for each of the following categories:

I. IDENTIFY	
Unique Identifier	**Cybersecurity Framework Category**
ID.AM	*Asset Management*
ID.BE	*Business Environment*
ID.GV	*Governance*
ID.RA	*Risk Assessment*
ID.RM	*Risk Management Strategy*
ID.SC	*Supply Chain Risk Management*

II. PROTECT	
Unique Identifier	**Cybersecurity Framework Category**
PR.AC	*Identity and Access Control*
PR.AT	*Awareness and Training*
PR.DS	*Data Security*
PR.IP	*Information Protection Processes & Procedures*
PR.MA	*Maintenance*
PR.PT	*Protective Technology*

III. DETECT	
Unique Identifier	**Cybersecurity Framework Category**
DE.AE	*Anomalies and Events*
DE.CM	*Security Continuous Monitoring*
DE.DP	*Detection Processes*

IV. RESPOND	
Unique Identifier	**Cybersecurity Framework Category**
RS.RP	*Response Planning*
RS.CO	*Communications*
RS.AN	*Analysis*
RS.MI	*Mitigation*
RS.IM	*Improvements*

RECOVER	
Unique Identifier	**Cybersecurity Framework Category**
RC.RP	*Recovery Planning*
RC.IM	*Improvements*
RC.CO	*Communications*

Cybersecurity Framework: Subcategories

Further detailing cybersecurity implementation considerations, each category of the NIST CSF has subcategory items which define the risks that should be assessed for each topic. Selecting technologies and cloud service providers that can meet these subcategory needs is key to effectively leveraging the NIST CSF.

Each subcategory, along with corresponding Google Cloud products, methodologies and services that can help meet these requirements, will be outlined in the section: Implementing NIST CSF on Google Cloud.

Cybersecurity Framework: Implementation Tiers

Successful implementation of the NIST Cybersecurity Framework is dependent upon meeting the configuration requirements and security baseline that your organization defines as its target profile.

NIST outlines tiered implementation recommendations that will help organizations set the tone for how cybersecurity risk is managed across the organization. These tiers should influence how organizations prioritize assessments against their target profile, and help facilitate progress in addressing security gaps across ***Risk Management Programs***, ***Integrated Risk Management Programs***, and ***External Participation***.

RISK MANAGEMENT PROCESS

Tier 1: Partial	Organizational cybersecurity risk management practices aren't formalized. Risk is managed Ad-hoc and in a reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business & mission requirements.
Tier 2: Risk Informed	Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
Tier 3: Repeatable	The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
Tier 4: Adaptive	The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving, sophisticated threats

INTEGRATED RISK MANAGEMENT PROGRAM

Tier 1: Partial	Limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis. The organization may not have processes that enable cybersecurity information to be shared within the organization.
Tier 2: Risk Informed	There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or recurring.

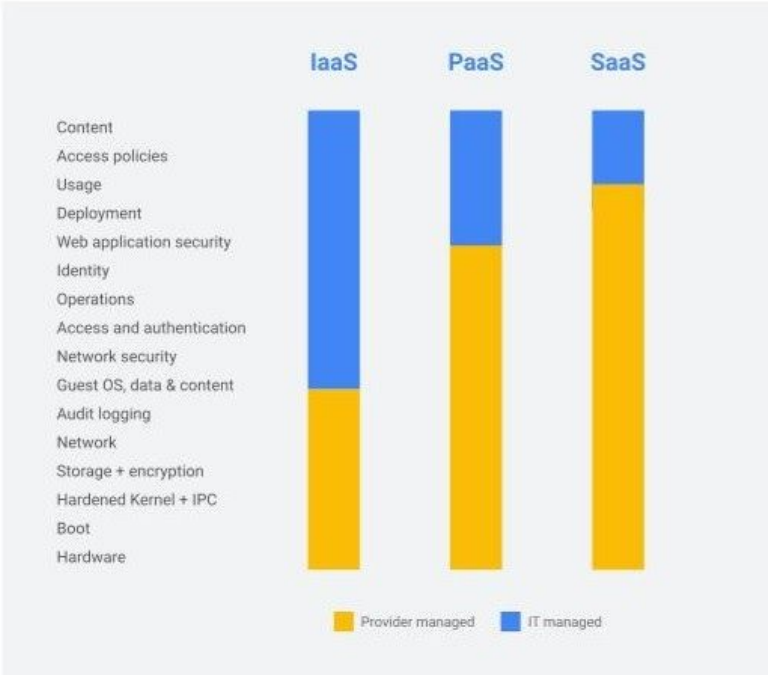
Tier 3: Repeatable	There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. Senior executives ensure consideration of cybersecurity through all lines of operation in the organization.
Tier 4: Adaptive	There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives are clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities and continuous awareness of activities on their systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.

EXTERNAL PARTICIPATION

Tier 1: Partial	The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses.
Tier 2: Risk Informed	The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others. Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses, but does not act consistently or formally upon those risks.
Tier 3: Repeatable	The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks. The organization collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities. The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, the organization usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring.
Tier 4: Adaptive	The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. The organization receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators. The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, the organization communicates proactively, using formal (e.g. agreements) and informal mechanisms to develop and maintain strong supply chain relationships.

Implementing NIST CSF on Google Cloud

The NIST CSF complements, but does not replace an organization's risk management process and cybersecurity program. And while cloud computing allows organizations to leverage a shared security model, data security is still the responsibility of the organization.



Committed to helping customers keep their data and critical infrastructure safe, Google equips organizations with a broad range of best practices, products, services, solutions and cloud capabilities to strengthen cybersecurity.

This section outlines each category and subcategories of the NIST Cybersecurity Framework. Corresponding to each NIST CSF category and subcategories, recommendations on how to meet and implement these requirements in Google Cloud are mapped accordingly. Organizations can leverage some or all of the suggested components to define, enforce, and manage cloud security and compliance.

Identify

ID.AM - Asset Management

The data, personnel, devices, systems, and facilities 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.

ID.AM-1: Physical devices and systems within the organization are inventoried

Cloud Identity
Google's Identity as a Service (IDaaS). Manage users, groups, devices, and applications across your organization.
https://cloud.google.com/identity/

Google Admin Console - Manage and add users, devices, data regions and security settings
https://gsuite.google.com/products/admin/

Cloud Resource Manager: Cloud Asset Inventory
Keeps a 5 week history of GCP asset metadata. Get an org-wide snapshot of your GCP resources and policies
https://cloud.google.com/resource-manager/docs/cloud-asset-inventory/overview

Forseti Security: Asset Inventory
Uses the Cloud Asset API to collect and store information about your GCP resources
https://forsetisecurity.org/docs/latest/configure/inventory/index.html

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

ID.AM-2: Software platforms and applications within the organization are inventoried

Cloud Resource Manager: Cloud Asset Inventory
Keeps a 5 week history of GCP asset metadata. Get an org-wide snapshot of your GCP resources and policies
https://cloud.google.com/resource-manager/docs/cloud-asset-inventory/overview

Forseti Security: Asset Inventory
Uses the Cloud Asset API to collect and store information about your GCP resources
https://forsetisecurity.org/docs/latest/configure/inventory/index.html

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

Cloud Private Catalog
Build out and manage a cloud catalog to manage your cloud resources and make them easily discoverable
https://cloud.google.com/private-catalog/

Cloud Data Catalog
Fully managed metadata discovery and management platform. Helps organizations quickly discover, manage, secure, and understand their data assets.
https://cloud.google.com/data-catalog/

ID.AM-3: Organizational communication and data flows are mapped

Cloud Resource Manager
Manage GCP resource hierarchy across your organization, folders, and projects
https://cloud.google.com/resource-manager/

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

ID.AM-4: External information systems are catalogued

Identity Platform
Add Google-grade identity and access management to your apps. Identity Platform is a customer identity and access management (CIAM) platform that helps organizations add identity and access management functionality to their applications.
https://cloud.google.com/identity-cp/

ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.

Cloud Resource Manager
Manage GCP resource hierarchy across your organization, folders, and projects
https://cloud.google.com/resource-manager/

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

Cloud Identity
Google's Identity as a Service (IDaaS). Manage users, groups, devices, and applications across your organization.
https://cloud.google.com/identity/

Google Admin Console
Manage and add users, devices, data regions and security settings
https://gsuite.google.com/products/admin

ID.BE - Business Environment

The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

ID.BE-1: The organization's role in the supply chain is identified and communicated

Google Cloud Adoption Framework
Determine your organization's cloud readiness and strategically map out your journey to the cloud
https://cloud.google.com/adoption-framework/

Professional Services: Transformation Advisory
Engage business leaders and users on innovating daily business processes with Google
https://services.google.com/fh/files/misc/transformation_advisory.pdf

Professional Services: Change Management Advisory
Engage with Google as your organization's strategic advisor in change management
https://services.google.com/fh/files/misc/change_management_advisory.pdf

ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated

Google Cloud Adoption Framework
Determine your organization's cloud readiness and strategically map out your journey to the cloud
https://cloud.google.com/adoption-framework/

Professional Services: Transformation Advisory
Engage business leaders and users on innovating daily business processes with Google
https://services.google.com/fh/files/misc/transformation_advisory.pdf

Professional Services: Change Management Advisory
Engage with Google as your organization's strategic advisor in change management
https://services.google.com/fh/files/misc/change_management_advisory.pdf

ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated

Google Cloud Adoption Framework
Determine your organization's cloud readiness and strategically map out your journey to the cloud
https://cloud.google.com/adoption-framework/

Professional Services: Transformation Advisory
Engage business leaders and users on innovating daily business processes with Google
https://services.google.com/fh/files/misc/transformation_advisory.pdf

Professional Services: Change Management Advisory
Engage with Google as your organization's strategic advisor in change management
https://services.google.com/fh/files/misc/change_management_advisory.pdf

ID.BE-4: Dependencies and critical functions for delivery of critical services are established

Google Cloud Services Overview
Overview of GCP's core computing & hosting, storage, database, networking, big data, and machine learning services
https://cloud.google.com/docs/overview/cloud-platform-services

GCP Products & Services
All of GCPs products and services
https://cloud.google.com/products/

ID.GV - Governance

The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

ID.GV-1: Organizational cybersecurity policy is established and communicated

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

Forseti Security
Systematically monitor your GCP resources, create and enforce rule-based security policies. Codify your security stance to maintain compliance and governance
https://forsetisecurity.org/about/

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

Identity Platform
Add Google-grade identity and access management to your apps. Identity Platform is a customer identity and access management (CIAM) platform that helps organizations add identity and access management functionality to their applications
https://cloud.google.com/identity-cp/

ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

Google's Security & Trust Center
Understand and leverage Google's ISO, SOC, PCI, HIPAA, FedRAMP, FIPS GDPR, and other compliance standards, regulations, and certifications
https://cloud.google.com/sec

ID.GV-4: Governance and risk management processes address cybersecurity risks

Professional Services: Cloud Discover Security
Engage with Google Consultants and Partners to understand your organization's security risks, key requirements, suggested security controls and Google's best practices
https://services.google.com/fh/files/misc/cloud_discover_security.pdf

Policy Intelligence
Smart access control for your GCP resources. Helps enterprises understand and manage their policies to reduce risk.
https://cloud.google.com/policy-intelligence/

ID.RA - Risk Assessment

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

ID.RA-1: Asset vulnerabilities are identified and documented

Cloud Security Scanner
Automatically scan App Engine applications for common vulnerabilities such as XXS, flash injection, mixed HTTP(S) content, outdated and insecure libraries
https://cloud.google.com/security-scanner/

Container Registry Vulnerability Scanner: Container Analysis
Scan container images stored in Container Registry for common vulnerabilities
https://cloud.google.com/container-registry/docs/container-analysis

Cloud Armor
Protect your infrastructure and web applications from Distributed Denial of Service (DDoS) attacks
https://cloud.google.com/armor/

Phishing Protection
Quickly report unsafe URLs to Google Safe Browsing and view status in Cloud Security Command Center
https://cloud.google.com/phishing-protection/

ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources

Forseti Security
Systematically monitor your GCP resources, create and enforce rule-based security policies. Codify your security stance to maintain compliance and governance
https://forsetisecurity.org/about/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

ID.RA-3: Threats, both internal and external, are identified and documented

G Suite Security Center
Actionable security insights for G Suite. Protect your organization with security analytics and best practice recommendations from Google. Get insights into external file sharing, visibility into spam and malware targeting users within your organization.
https://gsuite.google.com/products/admin/security-center/

Cloud Operations Suite
Store, search, analyze, monitor, and alert on log data and events in Google Cloud. Includes error reporting, production application profiling, application tracing, alerting, debugging, and 3rd party integrations
https://cloud.google.com/stackdriver/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

ID.RA-4: Potential business impacts and likelihoods are identified

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

G Suite Security Assessment
Google Consultants and Partners engage with organizations to improve the security posture of their Google Domain by assessing current configuration, security processes, and procedures
https://services.google.com/fh/files/misc/security_assessment.pdf

ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk

Forseti Security
Systematically monitor your GCP resources, create and enforce rule-based security policies. Codify your security stance to maintain compliance and governance
https://forsetisecurity.org/about/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

ID.RA-6: Risk responses are identified and prioritized

Forseti Security
Systematically monitor your GCP resources, create and enforce rule-based security policies. Codify your security stance to maintain compliance and governance
https://forsetisecurity.org/about/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

ID.RA - Risk Management

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders

Google Cloud Adoption Framework
Determine your organization's cloud readiness and strategically map out your journey to the cloud
https://cloud.google.com/adoption-framework/pdf

ID.RM-2: Organizational risk tolerance is determined and clearly expressed

Forseti Security
Systematically monitor your GCP resources, create and enforce rule-based security policies. Codify your security stance to maintain compliance and governance
https://forsetisecurity.org/about/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

Forseti Security
Systematically monitor your GCP resources, create and enforce rule-based security policies. Codify your security stance to maintain compliance and governance
https://forsetisecurity.org/about/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

G Suite Security Center
Actionable security insights for G Suite. Protect your organization with security analytics and best practice recommendations from Google. Get insights into external file sharing, visibility into spam and malware targeting users within your organization.
https://gsuite.google.com/products/admin/security-center/

Policy Intelligence
Smart access control for your GCP resources. Helps enterprises understand and manage their policies to reduce risk.
https://cloud.google.com/policy-intelligence/

ID.SC - Supply Chain Risk Management

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders

N/A - must be implemented by the organization.

ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process

Identity Platform
Add Google-grade identity and access management to your apps. Identity Platform is a customer identity and access management (CIAM) platform that helps organizations add identity and access management functionality to their applications
https://cloud.google.com/identity-cp/

ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.

N/A - must be implemented by the organization.

ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.

N/A - must be implemented by the organization.

ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers

N/A - must be implemented by the organization.

Protect

PR.AC - Identity Management Authentication and Access Control

Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, andaudited for authorized devices, users and processes

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

Cloud Identity
Google's Identity as a Service (IDaaS). Manage users, groups, devices, and applications across your organization. Also implements MFA and SSO
https://cloud.google.com/identity/

Google Admin Console
Manage and add users, devices, data regions and security settings
https://gsuite.google.com/products/admin/

PR.AC-2: Physical access to assets is managed and protected

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

VPC Service Controls
Define a security perimeter around specific GCP resources to help mitigate data exfiltration risks.
https://cloud.google.com/vpc-service-controls/

Cloud Identity Aware Proxy
Build an enterprise security model to control access to your applications and VMs. Verifying user identities and access request context to determine if users should be allowed access to resources.
https://cloud.google.com/iap/

Forseti Security
Systematically monitor your GCP resources, create and enforce rule-based security policies. Codify your security stance to maintain compliance and governance
https://forsetisecurity.org/about/

PR.AC-3: Remote access is managed

Cloud Identity Aware Proxy
Build an enterprise security model to control access to your applications and VMs. Verifying user identities and access request context to determine if users should be allowed access to resources.
https://cloud.google.com/iap/

Cloud VPN
Securely connect on-premise networks to GCP over IPSec
https://cloud.google.com/vpn/docs/concepts/overview

Context Aware Access
Manage access to apps and infrastructure based on a user's identity and context.
https://cloud.google.com/context-aware-access/

PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

Identity Platform
Add Google-grade identity and access management to your apps. Identity Platform is a customer identity and access management (CIAM) platform that helps organizations add identity and access management functionality to their applications
https://cloud.google.com/identity-cp/

PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)

Cloud VPC
Manage network functionality and segmentation of cloud resources. Leverage Cloud Router, Cloud VPN, Firewalls, Routes, VPC Flow Logs, Shared VPC and VPC peering for more granular network security
https://cloud.google.com/vpc/

Cloud Resource Manager
Manage and separate GCP resource hierarchy across your organization, folders, and projects
https://cloud.google.com/resource-manager/

PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions

Cloud Identity
Google's Identity as a Service (IDaaS). Manage users, groups, devices, and applications across your organization. Also implements MFA and SSO
https://cloud.google.com/identity/

Google Admin Console
Manage and add users, devices, data regions and security settings
https://gsuite.google.com/products/admin/

Identity Platform
Add Google-grade identity and access management to your apps. Identity Platform is a customer identity and access management (CIAM) platform that helps organizations add identity and access management functionality to their applications
https://cloud.google.com/identity-cp/

PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

Cloud Identity
Google's Identity as a Service (IDaaS). Manage users, groups, devices, and applications across your organization. Also implements MFA and SSO
https://cloud.google.com/identity/

Google Admin Console
Manage and add users, devices, data regions and security settings
https://gsuite.google.com/products/admin/

Identity Platform
Add Google-grade identity and access management to your apps. Identity Platform is a customer identity and access management (CIAM) platform that helps organizations add identity and access management functionality to their applications
https://cloud.google.com/identity-cp/

PR.AT - Awareness and Training

The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.

PR.AT-1: All users are informed and trained

Google Cloud Training
Leverage on-demand coursera courses, hands on qwiklabs, and Google or Partner-led classroom instruction to train your organization.
https://cloud.google.com/training/

PR.AT-2: Privileged users understand their roles and responsibilities

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

Cloud Identity
Google's Identity as a Service (IDaaS). Manage users, groups, devices, and applications across your organization. Also implements MFA and SSO
https://cloud.google.com/identity/

PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities

Identity Platform
Add Google-grade identity and access management to your apps. Identity Platform is a customer identity and access management (CIAM) platform that helps organizations add identity and access management functionality to their applications
https://cloud.google.com/identity-cp/

PR.AT-4: Senior executives understand their roles and responsibilities

Google Cloud Adoption Framework
Determine your organization's cloud readiness and strategically map out your journey to the cloud
https://cloud.google.com/adoption-framework/

Professional Services: Transformation Advisory
Engage business leaders and users on innovating daily business processes with Google
https://services.google.com/fh/files/misc/transformation_advisory.pdf

Professional Services: Change Management Advisory
Engage with Google as your organization's strategic advisor in change management
https://services.google.com/fh/files/misc/change_management_advisory.pdf

PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

Cloud Identity
Google's Identity as a Service (IDaaS). Manage users, groups, devices, and applications across your organization. Also implements MFA and SSO
https://cloud.google.com/identity/

PR.DS - Data Security

Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

PR.DS-1: Data-at-rest is protected

Google Encryption at Rest
All data in Google is encrypted at rest by default using envelope encryption
https://cloud.google.com/security/encryption-at-rest/

Cloud Key Management Service
Manage, generate, use, rotate, and destroy AES256, RSA 2048, RSA 3072, RSA 4096, EC P256, and EC P384 cryptographic keys on Google Cloud
https://cloud.google.com/kms/

Customer Supplied Encryption Keys (CSEKs)
In addition to Google's default encryption, supply your own AES256 encryption keys to encrypt GCP data
https://cloud.google.com/storage/docs/encryption/customer-supplied-keys

Cloud HSM
Protect your encryption keys in the cloud using a fully hosted, FIPS 140-2 Level 3 compliant hardware security model
https://cloud.google.com/hsm/

PR.DS-2: Data-in-transit is protected

Google Encryption in Transit
Data encrypted in transit automatically at Layer 7 and layer 3/4 in Google Cloud via TLS
https://cloud.google.com/security/encryption-in-transit/

PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition

Cloud Resource Manager
Manage and separate GCP resource hierarchy across your organization, folders, and projects
https://cloud.google.com/resource-manager/

Cloud Private Catalog
Build out and manage a cloud catalog to manage your cloud resources and make them easily discoverable
https://cloud.google.com/private-catalog/

Cloud Data Catalog
Fully managed metadata discovery and management platform. Helps organizations quickly discover, manage, secure, and understand their data assets.
https://cloud.google.com/data-catalog/

PR.DS-4: Adequate capacity to ensure availability is maintained

GCP Quotas
Set, enforce, and request quotas on resource usage to regulate how much of a particular GCP resource a project can use.
https://cloud.google.com/docs/quota

Autoscaling
Use GCE managed instance groups or managed compute services like Google App Engine to automatically scale capacity based on need or Cloud Monitoring metrics
https://cloud.google.com/compute/docs/autoscaler/

PR.DS-5: Protections against data leaks are implemented

Cloud Data Loss Prevention
Configure DLP to automatically discover, classify, and redact sensitive data in Google Cloud & G Suite
https://cloud.google.com/dlp/

Phishing Protection
Quickly report unsafe URLs to Google Safe Browsing and view status in Cloud Security Command Center
https://cloud.google.com/phishing-protection/

Access Approval API
Allows you to explicitly approve access to your data or configurations on GCP before it happens.
https://cloud.google.com/access-approval/docs/overview

VPC Service Controls
Define a security perimeter around specific GCP resources to help mitigate data exfiltration risks.
https://cloud.google.com/vpc-service-controls/

PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity

Titan Security Key
Prevent account hacks, phishing attacks, and enforce MFA/2SV using Titan Security Keys
https://cloud.google.com/titan-security-key/

Shielded VMs
Leverage hardened virtual machines on GCP that defend against rootkits, botkits, protect against remote attacks, privilege escalation, and malicious insiders
https://cloud.google.com/shielded-vm/

reCAPTCHA Enterprise
Protect your website from fraudulent activity, spam, and abuse.
https://cloud.google.com/recaptcha-enterprise/

Binary Authorization
Deploy-time security controls to ensure that only trusted container images are deployed on Kubernetes. Requires images to be signed by trusted authorities during development and enforces signature validation during deployment
https://cloud.google.com/binary-authorization/

PR.DS-7: The development and testing environment(s) are separate from the production environment

GKE Sandbox
provides additional isolation for multi-tenant workloads, helping to prevent container escapes, and increasing workload security.
https://cloud.google.com/kubernetes-engine/sandbox/

Cloud Resource Manager
Manage and separate GCP resource hierarchy across your organization, folders, and projects
https://cloud.google.com/resource-manager/

PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity

Titan Security Key
Prevent account hacks, phishing attacks, and enforce MFA/2SV using Titan Security Keys
https://cloud.google.com/titan-security-key/

Shielded VMs
Leverage hardened virtual machines on GCP that defend against rootkits, botkits, protect against remote attacks, privilege escalation, and malicious insiders
https://cloud.google.com/shielded-vm/

PR.IP - Information Protection Processes and Procedures

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

Forseti Security
Systematically monitor your GCP resources, create and enforce rule-based security policies. Codify your security stance to maintain compliance and governance
https://forsetisecurity.org/about/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

Policy Intelligence
Smart access control for your GCP resources. Helps enterprises understand and manage their policies to reduce risk.
https://cloud.google.com/policy-intelligence/

Cloud Deployment Manager
Create declarative templates that specify all resources needed for your cloud deployment. Establish a repeatable, template-driven deployment process
https://cloud.google.com/deployment-manager/

PR.IP-2: A System Development Life Cycle to manage systems is implemented

Cloud Deployment Manager
Create declarative templates that specify all resources needed for your cloud deployment. Establish a repeatable, template-driven deployment process
https://cloud.google.com/deployment-manager/

Binary Authorization
Deploy-time security controls to ensure that only trusted container images are deployed on Kubernetes. Requires images to be signed by trusted authorities during development and enforces signature validation during deployment
https://cloud.google.com/binary-authorization/

PR.IP-3: Configuration change control processes are in place

Access Approval API
Allows you to explicitly approve access to your data or configurations on GCP before it happens.
https://cloud.google.com/access-approval/docs/overview

Binary Authorization
Deploy-time security controls to ensure that only trusted container images are deployed on Kubernetes. Requires images to be signed by trusted authorities during development and enforces signature validation during deployment
https://cloud.google.com/binary-authorization/

PR.IP-4: Backups of information are conducted, maintained, and tested

Google Cloud Storage
Store, serve, backup and archive data with Multi-regional, Regional, Coldline, or Nearline storage buckets
https://cloud.google.com/storage/

PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met

N/A - must be implemented by the organization.

PR.IP-6: Data is destroyed according to policy

Google Cloud Data Deletion
Understand how data is fully deleted from Google Cloud over the course of 180 days via deletion requests, soft deletion, and backup expiration processes
https://cloud.google.com/security/deletion/

PR.IP-7: Protection processes are improved

Policy Intelligence
Smart access control for your GCP resources. Helps enterprises understand and manage their policies to reduce risk.
https://cloud.google.com/policy-intelligence/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

G Suite Security Assessment
Google Consultants and Partners engage with organizations to improve the security posture of their Google Domain by assessing current configuration, security processes, and procedures
https://services.google.com/fh/files/misc/security_assessment.pdf

PR.IP-8: Effectiveness of protection technologies is shared

Forseti Security
Systematically monitor your GCP resources, create and enforce rule-based security policies. Codify your security stance to maintain compliance and governance
https://forsetisecurity.org/about/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

Incident Response Management
Leverage IRM with Monitoring to identify, manage, investigate, and resolve incidents
https://cloud.google.com/incident-response/docs/

PR.IP-10: Response and recovery plans are tested

Incident Response Management
Leverage IRM with Monitoring to identify, manage, investigate, and resolve incidents
https://cloud.google.com/incident-response/docs/

Google Cloud Disaster Recovery Planning Guide
Build a disaster recovery architecture and plan for data and applications in Google Cloud
https://cloud.google.com/solutions/dr-scenarios-planning-guide

PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

Cloud Operations Suite
Store, search, analyze, monitor, and alert on log data and events in Google Cloud. Includes error reporting, production application profiling, application tracing, alerting, debugging, and 3rd party integrations
https://cloud.google.com/stackdriver/

PR.IP-12: A vulnerability management plan is developed and implemented

Forseti Security
Systematically monitor your GCP resources, create and enforce rule-based security policies. Codify your security stance to maintain compliance and governance
https://forsetisecurity.org/about/

Cloud Operations Suite
Store, search, analyze, monitor, and alert on log data and events in Google Cloud. Includes error reporting, production application profiling, application tracing, alerting, debugging, and 3rd party integrations
https://cloud.google.com/stackdriver/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

PR.MA - Maintenance

Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

Cloud Identity
Google's Identity as a Service (IDaaS). Manage users, groups, devices, and applications across your organization. Also implements MFA and SSO
https://cloud.google.com/identity/

Google Admin Console
Manage and add users, devices, data regions and security settings
https://gsuite.google.com/products/admin/

Cloud Operations Suite
Store, search, analyze, monitor, and alert on log data and events in Google Cloud. Includes error reporting, production application profiling, application tracing, alerting, debugging, and 3rd party integrations
https://cloud.google.com/stackdriver/

PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

Identity Platform
Add Google-grade identity and access management to your apps. Identity Platform is a customer identity and access management (CIAM) platform that helps organizations add identity and access management functionality to their applications
https://cloud.google.com/identity-cp/

Cloud Identity Aware Proxy
Build an enterprise security model to control access to your applications and VMs. Verifying user identities and access request context to determine if users should be allowed access to resources.
https://cloud.google.com/iap/

VPC Service Controls
Define a security perimeter around specific GCP resources to help mitigate data exfiltration risks.
https://cloud.google.com/vpc-service-controls/

Cloud VPC
Manage network functionality and segmentation of cloud resources. Leverage Cloud Router, Cloud VPN, Firewalls, Routes, VPC Flow Logs, Shared VPC and VPC peering for more granular network security
https://cloud.google.com/vpc/

Cloud Operations Suite
Store, search, analyze, monitor, and alert on log data and events in Google Cloud. Includes error reporting, production application profiling, application tracing, alerting, debugging, and 3rd party integrations
https://cloud.google.com/stackdriver/

PR.PT - Protective Technology

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

Cloud Operations Suite
Store, search, analyze, monitor, and alert on log data and events in Google Cloud. Includes error reporting, production application profiling, application tracing, alerting, debugging, and 3rd party integrations
https://cloud.google.com/stackdriver/

Forseti Security
Systematically monitor your GCP resources, create and enforce rule-based security policies. Codify your security stance to maintain compliance and governance
https://forsetisecurity.org/about/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

PR.PT-2: Removable media is protected and its use restricted according to policy

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

PR.PT-4: Communications and control networks are protected

Cloud VPC
Manage network functionality and segmentation of cloud resources. Leverage Cloud Router, Cloud VPN, Firewalls, Routes, VPC Flow Logs, Shared VPC and VPC peering for more granular network security
https://cloud.google.com/vpc/

VPC Service Controls
Define a security perimeter around specific GCP resources to help mitigate data exfiltration risks.
https://cloud.google.com/vpc-service-controls/

Cloud VPN
Securely connect on-premise networks to GCP over IPSec
https://cloud.google.com/vpn/docs/concepts/overview

Cloud Armor
Protect your infrastructure and web applications from Distributed Denial of Service (DDoS) attacks
https://cloud.google.com/armor/

PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations

Global, Regional, Zonal Resources
Build in high availability by leveraging global, zonal, and regional Google Cloud resources
https://cloud.google.com/compute/docs/regions-zones/global-regional-zonal-resources

Google Cloud Load Balancing
Implement global network autoscaling, HTTP(S), TCP, SSL, and Internal Load Balancing
https://cloud.google.com/load-balancing/

Cloud CDN
Deliver content across Google's global, low-latency network using cloud content delivery network
https://cloud.google.com/cdn/

Autoscaling
Use GCE managed instance groups or managed compute services like Google App Engine to automatically scale capacity based on need or Cloud Monitoring metrics
https://cloud.google.com/compute/docs/autoscaler/

Google Deployment Manager
Create and manage cloud resources with simple templates. Specify all the resources needed for your application in a declarative format, use templates to parameterize and reuse configurations.
https://cloud.google.com/deployment-manager/

Detect

DE.AE - Anomalies and Events

Anomalous activity is detected and the potential impact of events is understood.

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed

Cloud VPC
Manage network functionality and segmentation of cloud resources. Leverage Cloud Router, Cloud VPN, Firewalls, Routes, VPC Flow Logs, Shared VPC and VPC peering for more granular network security
https://cloud.google.com/vpc/

Traffic Director
Enterprise-ready traffic management for open service mesh.. Delivers configuration and traffic control intelligence to sidecar service proxies.
https://cloud.google.com/traffic-director/

VPC Service Controls
Define a security perimeter around specific GCP resources to help mitigate data exfiltration risks.
https://cloud.google.com/vpc-service-controls/

DE.AE-2: Detected events are analyzed to understand attack targets and methods

Cloud Armor
Protect your infrastructure and web applications from Distributed Denial of Service (DDoS) attacks
https://cloud.google.com/armor/

G Suite Phishing & Malware Protection
Advanced phishing and malware protection. Place emails in quarantine, protect against anomalous attachments, protect Google Groups from inbound email spoofing.
https://support.google.com/a/answer/7577854

Network Telemetry
Enable firewall logging, VPC flow logs, performance monitoring and metrics, and log exports to keep your networks and services secure
https://cloud.google.com/network-telemetry/

Incident Response Management
Leverage IRM with Monitoring to identify, manage, investigate, and resolve incidents.
https://cloud.google.com/incident-response/docs/

Cloud Operations Suite
Store, search, analyze, monitor, and alert on log data and events in Google Cloud. Includes error reporting, production application profiling, application tracing, alerting, debugging, and 3rd party integrations
https://cloud.google.com/stackdriver/

Cloud Security Scanner
Automatically scan App Engine, Compute Engine, and Kubernetes Engine applications for common vulnerabilities such as XXS, flash injection, mixed HTTP(S) content, outdated and insecure libraries
https://cloud.google.com/security-scanner/

Container Registry Vulnerability Scanner: Container Analysis
Scan container images stored in Container Registry for common vulnerabilities
https://cloud.google.com/container-registry/docs/container-analysis

DE.AE-3: Event data are collected and correlated from multiple sources and sensors

Cloud Operations Suite
Store, search, analyze, monitor, and alert on log data and events in Google Cloud. Includes error reporting, production application profiling, application tracing, alerting, debugging, and 3rd party integrations
https://cloud.google.com/stackdriver/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

G Suite Security Center
Actionable security insights for G Suite. Protect your organization with security analytics and best practice recommendations from Google. Get insights into external file sharing, visibility into spam and malware targeting users within your organization.
https://gsuite.google.com/products/admin/security-center/

DE.AE-4: Impact of events is determined

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

G Suite Security Center
Actionable security insights for G Suite. Protect your organization with security analytics and best practice recommendations from Google. Get insights into external file sharing, visibility into spam and malware targeting users within your organization.
https://gsuite.google.com/products/admin/security-center/

DE.AE-5: Incident alert thresholds are established

Incident Response Management
Leverage IRM with Monitoring to identify, manage, investigate, and resolve incidents
https://cloud.google.com/incident-response/docs/

Cloud Operations Suite
Store, search, analyze, monitor, and alert on log data and events in Google Cloud. Includes error reporting, production application profiling, application tracing, alerting, debugging, and 3rd party integrations
https://cloud.google.com/stackdriver/

DE.CM - Security Continuous Monitoring

The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

DE.CM-1: The network is monitored to detect potential cybersecurity events

Network Telemetry
Enable firewall logging, VPC flow logs, performance monitoring and metrics, and log exports to keep your networks and services secure
https://cloud.google.com/network-telemetry/

Cloud Armor
Protect your infrastructure and web applications from Distributed Denial of Service (DDoS) attacks
https://cloud.google.com/armor/

VPC Service Controls
Define a security perimeter around specific GCP resources to help mitigate data exfiltration risks.
https://cloud.google.com/vpc-service-controls/

Traffic Director
Enterprise-ready traffic management for open service mesh. Delivers configuration and traffic control intelligence to sidecar service proxies.
https://cloud.google.com/traffic-director/

DE.CM-2: The physical environment is monitored to detect potential cybersecurity events

Cloud Operations Suite
Store, search, analyze, monitor, and alert on log data and events in Google Cloud. Includes error reporting, production application profiling, application tracing, alerting, debugging, and 3rd party integrations
https://cloud.google.com/stackdriver/

G Suite Security Center
Actionable security insights for G Suite. Protect your organization with security analytics and best practice recommendations from Google. Get insights into external file sharing, visibility into spam and malware targeting users within your organization.
https://gsuite.google.com/products/admin/security-center/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events

Cloud Operations Suite
Store, search, analyze, monitor, and alert on log data and events in Google Cloud. Includes error reporting, production application profiling, application tracing, alerting, debugging, and 3rd party integrations
https://cloud.google.com/stackdriver/

DE.CM-4: Malicious code is detected

Cloud Security Scanner
Automatically scan App Engine, Compute Engine, and Kubernetes Engine applications for common vulnerabilities such as XXS, flash injection, mixed HTTP(S) content, outdated and insecure libraries
https://cloud.google.com/security-scanner/

Container Registry Vulnerability Scanner: Container Analysis
Scan container images stored in Container Registry for common vulnerabilities
https://cloud.google.com/container-registry/docs/container-analysis

DE.CM-5: Unauthorized mobile code is detected

Android Enterprise
provides multiple layers of security to prevent intrusions including built in Titan Security Keys, Google Play Protect, Management APIs, hardened OS platform, and dedicated hardware.
https://www.android.com/enterprise/security/
https://blog.google/technology/safety-security/your-android-phone-is-a-security-key/

Cloud Security Scanner
Automatically scan App Engine, Compute Engine, and Kubernetes Engine applications for common vulnerabilities such as XXS, flash injection, mixed HTTP(S) content, outdated and insecure libraries
https://cloud.google.com/security-scanner/

Container Registry Vulnerability Scanner: Container Analysis
Scan container images stored in Container Registry for common vulnerabilities
https://cloud.google.com/container-registry/docs/container-analysis

DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events

Cloud Operations Suite
Store, search, analyze, monitor, and alert on log data and events in Google Cloud. Includes error reporting, production application profiling, application tracing, alerting, debugging, and 3rd party integrations
https://cloud.google.com/stackdriver/

Identity Platform
Add Google-grade identity and access management to your apps. Identity Platform is a customer identity and access management (CIAM) platform that helps organizations add identity and access management functionality to their applications
https://cloud.google.com/identity-cp/

DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed

Cloud Operations Suite
Store, search, analyze, monitor, and alert on log data and events in Google Cloud. Includes error reporting, production application profiling, application tracing, alerting, debugging, and 3rd party integrations
https://cloud.google.com/stackdriver/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

Cloud Identity
Google's Identity as a Service (IDaaS). Manage users, groups, devices, and applications across your organization.
https://cloud.google.com/identity/

Google Admin Console
Manage and add users, devices, data regions and security settings
https://gsuite.google.com/products/admin/

Identity Platform
Add Google-grade identity and access management to your apps. Identity Platform is a customer identity and access management (CIAM) platform that helps organizations add identity and access management functionality to their applications
https://cloud.google.com/identity-cp/

DE.CM-8: Vulnerability scans are performed

Cloud Armor
Protect your infrastructure and web applications from Distributed Denial of Service (DDoS) attacks
https://cloud.google.com/armor/

Container Registry Vulnerability Scanner: Container Analysis
Scan container images stored in Container Registry for common vulnerabilities
https://cloud.google.com/container-registry/docs/container-analysis

Cloud Security Scanner
Automatically scan App Engine, Compute Engine, and Kubernetes Engine applications for common vulnerabilities such as XXS, flash injection, mixed HTTP(S) content, outdated and insecure libraries
https://cloud.google.com/security-scanner/

DE.DP - Detection Processes

Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

Cloud Identity
Google's Identity as a Service (IDaaS). Manage users, groups, devices, and applications across your organization.
https://cloud.google.com/identity/

Google Admin Console
Manage and add users, devices, data regions and security settings
https://gsuite.google.com/products/admin/

Identity Platform
Add Google-grade identity and access management to your apps. Identity Platform is a customer identity and access management (CIAM) platform that helps organizations add identity and access management functionality to their applications
https://cloud.google.com/identity-cp/

DE.DP-2: Detection activities comply with all applicable requirements

Cloud Operations Suite
Store, search, analyze, monitor, and alert on log data and events in Google Cloud. Includes error reporting, production application profiling, application tracing, alerting, debugging, and 3rd party integrations
https://cloud.google.com/stackdriver/

G Suite Security Center
Actionable security insights for G Suite. Protect your organization with security analytics and best practice recommendations from Google. Get insights into external file sharing, visibility into spam and malware targeting users within your organization.
https://gsuite.google.com/products/admin/security-center/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

DE.DP-3: Detection processes are tested

Google's Security & Trust Center
Understand and leverage Google's ISO, SOC, PCI, HIPAA, FedRAMP, FIPS GDPR, and other compliance standards, regulations, and certifications
https://cloud.google.com/sec

DE.DP-4: Event detection information is communicated

Event Threat Detection
Uncover security threats in Google Cloud Platform environments.
https://cloud.google.com/event-threat-detection/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

Cloud Pub/Sub
Stream analytics, events, notifications and messages
https://cloud.google.com/pubsub/

G Suite Security Center
Actionable security insights for G Suite. Protect your organization with security analytics and best practice recommendations from Google. Get insights into external file sharing, visibility into spam and malware targeting users within your organization.
https://gsuite.google.com/products/admin/security-center/

Cloud Functions
Event-driven serverless compute platform.
https://cloud.google.com/functions/

DE.DP-5: Detection processes are continuously improved

Policy Intelligence
Smart access control for your GCP resources. Helps enterprises understand and manage their policies to reduce risk.
https://cloud.google.com/policy-intelligence/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

Respond

RS.RP - Response Planning

Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

RS.RP-1: Response plan is executed during or after an incident

Incident Response Management
Leverage IRM with Monitoring to identify, manage, investigate, and resolve incidents
https://cloud.google.com/incident-response/docs/

G Suite Security Center
Actionable security insights for G Suite. Protect your organization with security analytics and best practice recommendations from Google. Get insights into external file sharing, visibility into spam and malware targeting users within your organization.
https://gsuite.google.com/products/admin/security-center/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

RS.CO - Communications

Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

RS.CO-1: Personnel know their roles and order of operations when a response is needed

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

Cloud Identity
Google's Identity as a Service (IDaaS). Manage users, groups, devices, and applications across your organization.
https://cloud.google.com/identity/

Google Admin Console
Manage and add users, devices, data regions and security settings
https://gsuite.google.com/products/admin/

Identity Platform
Add Google-grade identity and access management to your apps. Identity Platform is a customer identity and access management (CIAM) platform that helps organizations add identity and access management functionality to their applications
https://cloud.google.com/identity-cp/

RS.CO-2: Incidents are reported consistent with established criteria

Incident Response Management
Leverage IRM with Monitoring to identify, manage, investigate, and resolve incidents
https://cloud.google.com/incident-response/docs/

Cloud Operations Suite
Store, search, analyze, monitor, and alert on log data and events in Google Cloud. Includes error reporting, production application profiling, application tracing, alerting, debugging, and 3rd party integrations
https://cloud.google.com/stackdriver/

RS.CO-3: Information is shared consistent with response plans

Log Exports
Export logs to GCS for storage & archival, to BigQuery for analysis, or to external systems for broader integration and analysis
https://cloud.google.com/logging/docs/export/

RS.CO-4: Coordination with stakeholders occurs consistent with response plans

Incident Response Management
Leverage IRM with Monitoring to identify, manage, investigate, and resolve incidents
https://cloud.google.com/incident-response/docs/

RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

Identity Platform
Add Google-grade identity and access management to your apps. Identity Platform is a customer identity and access management (CIAM) platform that helps organizations add identity and access management functionality to their applications
https://cloud.google.com/identity-cp/

Incident Response Management
Leverage IRM with Monitoring to identify, manage, investigate, and resolve incidents
https://cloud.google.com/incident-response/docs/

Cloud Identity & Access Management
Maintain fine-grained control over who has access to what cloud resources. Define access roles & permissions while enforcing separation of duties and least privilege
https://cloud.google.com/iam/

RS.AN - Analysis

Analysis is conducted to ensure effective response and support recovery activities.

RS.AN-1: Notifications from detection systems are investigated

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/
G Suite Security Center
Actionable security insights for G Suite. Protect your organization with security analytics and best practice recommendations from Google. Get insights into external file sharing, visibility into spam and malware targeting users within your organization.
https://gsuite.google.com/products/admin/security-center/

Cloud Operations Suite
Store, search, analyze, monitor, and alert on log data and events in Google Cloud. Includes error reporting, production application profiling, application tracing, alerting, debugging, and 3rd party integrations
https://cloud.google.com/stackdriver/

RS.AN-2: The impact of the incident is understood

G Suite Security Center
Actionable security insights for G Suite. Protect your organization with security analytics and best practice recommendations from Google. Get insights into external file sharing, visibility into spam and malware targeting users within your organization.
https://gsuite.google.com/products/admin/security-center/

Incident Response Management
Leverage IRM with Monitoring to identify, manage, investigate, and resolve incidents
https://cloud.google.com/incident-response/docs/

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

RS.AN-3: Forensics are performed

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

Log Exports
Export logs to GCS for storage & archival, to BigQuery for analysis, or to external systems for broader integration and analysis
https://cloud.google.com/logging/docs/export/

BigQuery
Serverless, highly-scalable, and cost-effective cloud data warehouse with an in-memory BI Engine and machine learning built in. Analyze all your batch and streaming data.
https://cloud.google.com/bigquery/

RS.AN-4: Incidents are categorized consistent with response plans

Incident Response Management
Leverage IRM with Monitoring to identify, manage, investigate, and resolve incidents
https://cloud.google.com/incident-response/docs/

RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

G Suite Security Center
Actionable security insights for G Suite. Protect your organization with security analytics and best practice recommendations from Google. Get insights into external file sharing, visibility into spam and malware targeting users within your organization.
https://gsuite.google.com/products/admin/security-center/river/

Event Threat Detection
Uncover security threats in Google Cloud Platform environments.
https://cloud.google.com/event-threat-detection/

Forseti Security
Systematically monitor your GCP resources, create and enforce rule-based security policies. Codify your security stance to maintain compliance and governance
https://forsetisecurity.org/about/

RS.MI - Mitigation

Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident

RS.MI-1: Incidents are contained

Incident Response Management
Leverage IRM with Monitoring to identify, manage, investigate, and resolve incidents
https://cloud.google.com/incident-response/docs/

Event Threat Detection
Uncover security threats in Google Cloud Platform environments.
https://cloud.google.com/event-threat-detection/

RS.MI-2: Incidents are mitigated

Cloud Security Scanner
Automatically scan App Engine, Compute Engine, and Kubernetes Engine applications for common vulnerabilities such as XXS, flash injection, mixed HTTP(S) content, outdated and insecure libraries
https://cloud.google.com/security-scanner/

Cloud Armor
Protect your infrastructure and web applications from Distributed Denial of Service (DDoS) attacks
https://cloud.google.com/armor/

Container Registry Vulnerability Scanner: Container Analysis
Scan container images stored in Container Registry for common vulnerabilities
https://cloud.google.com/container-registry/docs/container-analysis

Phishing Protection
Quickly report unsafe URLs to Google Safe Browsing and view status in Cloud Security Command Center
https://cloud.google.com/phishing-protection/

RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

G Suite Security Center
Actionable security insights for G Suite. Protect your organization with security analytics and best practice recommendations from Google. Get insights into external file sharing, visibility into spam and malware targeting users within your organization.
https://gsuite.google.com/products/admin/security-center/

Cloud Security Scanner
Automatically scan App Engine, Compute Engine, and Kubernetes Engine applications for common vulnerabilities such as XXS, flash injection, mixed HTTP(S) content, outdated and insecure libraries
https://cloud.google.com/security-scanner/

Cloud Armor
Protect your infrastructure and web applications from Distributed Denial of Service (DDoS) attacks
https://cloud.google.com/armor/

Container Registry Vulnerability Scanner: Container Analysis
Scan container images stored in Container Registry for common vulnerabilities
https://cloud.google.com/container-registry/docs/container-analysis

Phishing Protection
Quickly report unsafe URLs to Google Safe Browsing and view status in Cloud Security Command Center
https://cloud.google.com/phishing-protection/

RS.IM - Improvements

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

RS.IM-1: Response plans incorporate lessons learned

Incident Response Management
Leverage IRM with Monitoring to identify, manage, investigate, and resolve incidents
https://cloud.google.com/incident-response/docs/

Event Threat Detection
Uncover security threats in Google Cloud Platform environments.
https://cloud.google.com/event-threat-detection/

RS.IM-2: Response strategies are updated

Cloud Security Command Center (CSCC)
Enhance your security posture with centralized asset discovery and inventory, sensitive data identification, app vulnerability detection, access control monitoring, anomaly detection, and input from 3rd party security tools with real-time notifications
https://cloud.google.com/security-command-center/

Forseti Security
Systematically monitor your GCP resources, create and enforce rule-based security policies. Codify your security stance to maintain compliance and governance
https://forsetisecurity.org/about/

G Suite Security Center
Actionable security insights for G Suite. Protect your organization with security analytics and best practice recommendations from Google. Get insights into external file sharing, visibility into spam and malware targeting users within your organization.
https://gsuite.google.com/products/admin/security-center/

Recover

RC.RP - Recovery Planning

Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

RC.RP-1: Recovery plan is executed during or after a cybersecurity incident

Google Cloud Disaster Recovery Planning Guide
Build a disaster recovery architecture and plan for data and applications in Google Cloud
https://cloud.google.com/solutions/dr-scenarios-planning-guide

Global, Regional, Zonal Resources
Build in high availability by leveraging global, zonal, and regional Google Cloud resources
https://cloud.google.com/compute/docs/regions-zones/global-regional-zonal-resources

Google Cloud Load Balancing
Implement global network autoscaling, HTTP(S), TCP, SSL, and Internal Load Balancing
https://cloud.google.com/load-balancing/

Cloud CDN
Deliver content across Google's global, low-latency network using cloud content delivery network
https://cloud.google.com/cdn/

Autoscaling
Use GCE managed instance groups or managed compute services like Google App Engine to automatically scale capacity based on need or Cloud Monitoring metrics
https://cloud.google.com/compute/docs/autoscaler/

Google Deployment Manager
Create and manage cloud resources with simple templates. Specify all the resources needed for your application in a declarative format, use templates to parameterize and reuse configurations.
https://cloud.google.com/deployment-manager/

Incident Response Management
Leverage IRM with Monitoring to identify, manage, investigate, and resolve incidents
https://cloud.google.com/incident-response/docs/

RC.IM - Improvements

Recovery planning and processes are improved by incorporating lessons learned into future activities.

RC.IM-1: Recovery plan is executed during or after a cybersecurity incident

Google Cloud Disaster Recovery Planning Guide
Build a disaster recovery architecture and plan for data and applications in Google Cloud
https://cloud.google.com/solutions/dr-scenarios-planning-guide

Global, Regional, Zonal Resources
Build in high availability by leveraging global, zonal, and regional Google Cloud resources
https://cloud.google.com/compute/docs/regions-zones/global-regional-zonal-resources

Google Cloud Load Balancing
Implement global network autoscaling, HTTP(S), TCP, SSL, and Internal Load Balancing
https://cloud.google.com/load-balancing/

Cloud CDN
Deliver content across Google's global, low-latency network using cloud content delivery network
https://cloud.google.com/cdn/

Autoscaling
Use GCE managed instance groups or managed compute services like Google App Engine to automatically scale capacity based on need or Cloud Monitoring metrics
https://cloud.google.com/compute/docs/autoscaler/

Incident Response Management
Leverage IRM with Monitoring to identify, manage, investigate, and resolve incidents
https://cloud.google.com/incident-response/docs/

Google Deployment Manager
Create and manage cloud resources with simple templates. Specify all the resources needed for your application in a declarative format, use templates to parameterize and reuse configurations.
https://cloud.google.com/deployment-manager/

RC.IM-2: Recovery strategies are updated

Google Cloud Disaster Recovery Planning Guide
Build a disaster recovery architecture and plan for data and applications in Google Cloud
https://cloud.google.com/solutions/dr-scenarios-planning-guide

Global, Regional, Zonal Resources
Build in high availability by leveraging global, zonal, and regional Google Cloud resources
https://cloud.google.com/compute/docs/regions-zones/global-regional-zonal-resources

Google Deployment Manager
Create and manage cloud resources with simple templates. Specify all the resources needed for your application in a declarative format, use templates to parameterize and reuse configurations.
https://cloud.google.com/deployment-manager/

Incident Response Management
Leverage IRM with Monitoring to identify, manage, investigate, and resolve incidents
https://cloud.google.com/incident-response/docs

RC.CO - Communications

Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

RC.CO-1: Public relations are managed

Contact Center AI
Combine the best of Google AI with your customer contact center software to improve customer experience and operational efficiency.
https://cloud.google.com/solutions/contact-center/

RC.CO-2: Reputation is repaired after an incident

N/A - must be implemented by the organization.

RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

Incident Response Management
Leverage IRM with Monitoring to identify, manage, investigate, and resolve incidents
https://cloud.google.com/incident-response/docs/

Contact Center AI
Combine the best of Google AI with your customer contact center software to improve customer experience and operational efficiency.
https://cloud.google.com/solutions/contact-center/

Google Cloud Status Dashboard
View the current status of GCP services and uptime
https://status.cloud.google.com/

Summary

The NIST Cybersecurity Framework consolidates industry standards and security best practices to help organizations manage their IT systems and critical infrastructure. Organizations that adopt Google Cloud and the Cybersecurity Framework will not only understand their cybersecurity risks, threats and vulnerabilities, but they will also understand the impacts of these factors and how to prevent and mitigate them.

With capabilities in place to track and maintain security measures and controls, the CSF and Google Cloud make it possible for organizations to gain meaningful insights into how security configurations affect organizational objectives and business outcomes. Under a shared responsibility model, companies can offload security components to be enforced by Google on trusted, validated and accredited cloud services infrastructure.

Secure by design, Google Cloud implements built in, layered security measures across a global network to protect user information, identities, applications and devices. Leveraging the robust set of security products and services made available to customers, organizations can protect critical assets while meeting compliance requirements for any industry, on Google Cloud.

Additional Resources

- NIST Cybersecurity Framework version 1.1 | Documentation
- NIST Cybersecurity Framework Industry Impacts | Article
- Google Cloud Security & Trust Center | Website
- Google Cloud Security Products | Website