NIST CSF 2.0 Function ➜ Category (Identifier)

GOVERN (GV)

Organizational Context GV.OC-02 / GV.OC-04

Summary:
Cloud-hosted client services and contractual uptime commitments are understood, so loss of availability triggers immediate escalation.

Implementation Examples:
GV.OC-02:

- **Ex1:** Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees)
- **Ex2:** Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., privacy expectations of customers, business expectations of partnerships, compliance expectations of regulators, ethics expectations of society)

GV.OC-04:

- **Ex1:** Establish criteria for determining the criticality of the organization's capabilities and services as viewed by internal and external stakeholders
- **Ex2:** Determine (e.g., from a business impact analysis) assets and business operations that are vital to achieving mission objectives and the potential impact of a loss (or partial loss) of such operations
- **Ex3:** Establish and communicate resilience objectives (e.g., recovery time objectives) for delivering critical capabilities and services in various operating states (e.g., under attack, during recovery, normal operation)

Risk Management Strategy GV.RM-01 / GV.RM-05 / GV.RM-06

Summary:
DDoS is on the enterprise risk register with a defined risk appetite; communication lines and a standard scoring method guide the response.

Implementation Examples:
GV.RM-01:

- **Ex1:** Update near-term and long-term cybersecurity risk management objectives as part of annual strategic planning and when major changes occur

- **Ex2:** Establish measurable objectives for cybersecurity risk management (e.g., manage the quality of user training, ensure adequate risk protection for industrial control systems)

- **Ex3:** Senior leaders agree about cybersecurity objectives and use them for measuring and managing risk and performance

GV.RM-05:

- **Ex1:** Determine how to update senior executives, directors, and management on the organization's cybersecurity posture at agreed-upon intervals

- **Ex2:** Identify how all departments across the organization — such as management, operations, internal auditors, legal, acquisition, physical security, and HR — will communicate with each other about cybersecurity risks

GV.RM-06:

- **Ex1:** Establish criteria for using a quantitative approach to cybersecurity risk analysis, and specify probability and exposure formulas

- **Ex2:** Create and use templates (e.g., a risk register) to document cybersecurity risk information (e.g., risk description, exposure, treatment, and ownership)

- **Ex3:** Establish criteria for risk prioritization at the appropriate levels within the enterprise

- **Ex4:** Use a consistent list of risk categories to support integrating, aggregating, and comparing cybersecurity risks

Roles, Responsibilities & Authorities GV.RR-02 / GV.RR-03

Summary:
An incident response team (IRT) with clear authority and budget was activated at 14:10.

Implementation Examples:
GV.RR-02:

- **Ex1:** Document risk management roles and responsibilities in policy

- **Ex2:** Document who is responsible and accountable for cybersecurity risk management activities and how those teams and individuals are to be consulted and informed

- **Ex3:** Include cybersecurity responsibilities and performance requirements in personnel descriptions

- **Ex4:** Document performance goals for personnel with cybersecurity risk management responsibilities, and periodically measure performance to identify areas for improvement

- **Ex5:** Clearly articulate cybersecurity responsibilities within operations, risk functions, and internal audit functions

GV.RR-03:

- **Ex1:** Conduct periodic management reviews to ensure that those given cybersecurity risk management responsibilities have the necessary authority
- **Ex2:** Identify resource allocation and investment in line with risk tolerance and response
- **Ex3:** Provide adequate and sufficient people, process, and technical resources to support the cybersecurity strategy

Policy GV.PO-01 / GV.PO-02

Summary:
Firewall-change and emergency-shutdown policies authorized rapid blocking of ICMP traffic and non-critical services.

Implementation Examples:
GV.PO-01:

- **Ex1:** Create, disseminate, and maintain an understandable, usable risk management policy with statements of management intent, expectations, and direction
- **Ex2:** Periodically review policy and supporting processes and procedures to ensure that they align with risk management strategy objectives and priorities, as well as the high-level direction of the cybersecurity policy
- **Ex3:** Require approval from senior management on policy
- **Ex4:** Communicate cybersecurity risk management policy and supporting processes and procedures across the organization
- **Ex5:** Require personnel to acknowledge receipt of policy when first hired, annually, and whenever policy is updated

GV.PO-02:

- **Ex1:** Update policy based on periodic reviews of cybersecurity risk management results to ensure that policy and supporting processes and procedures adequately maintain risk at an acceptable level
- **Ex2:** Provide a timeline for reviewing changes to the organization's risk environment (e.g., changes in risk or in the organization's mission objectives), and communicate recommended policy updates
- **Ex3:** Update policy to reflect changes in legal and regulatory requirements
- **Ex4:** Update policy to reflect changes in technology (e.g., adoption of artificial intelligence) and changes to the business (e.g., acquisition of a new business, new contract requirements)

Oversight GV.OV-01

Summary:
Post-incident, leadership reviews results to fine-tune the DDoS risk strategy.

Implementation Examples:

- **Ex1:** Measure how well the risk management strategy and risk results have helped leaders make decisions and achieve organizational objectives
- **Ex2:** Examine whether cybersecurity risk strategies that impede operations or innovation should be adjusted

Cyber-Supply-Chain Risk Management GV.SC-01 / GV.SC-05 / GV.SC-08

Summary:
ISP contracts and DDoS-scrubbing options are re-evaluated; providers will be included in future drills.

Implementation Examples:
GV.SC-01:

- **Ex1:** Establish a strategy that expresses the objectives of the cybersecurity supply chain risk management program
- **Ex2:** Develop the cybersecurity supply chain risk management program, including a plan (with milestones), policies, and procedures that guide implementation and improvement of the program, and share the policies and procedures with the organizational stakeholders
- **Ex3:** Develop and implement program processes based on the strategy, objectives, policies, and procedures that are agreed upon and performed by the organizational stakeholders
- **Ex4:** Establish a cross-organizational mechanism that ensures alignment between functions that contribute to cybersecurity supply chain risk management, such as cybersecurity, IT, operations, legal, human resources, and engineering

GV.SC-05:

- **Ex1:** Establish security requirements for suppliers, products, and services commensurate with their criticality level and potential impact if compromised
- **Ex2:** Include all cybersecurity and supply chain requirements that third parties must follow and how compliance with the requirements may be verified in default contractual language
- **Ex3:** Define the rules and protocols for information sharing between the organization and its suppliers and sub-tier suppliers in agreements
- **Ex4:** Manage risk by including security requirements in agreements based on their criticality and potential impact if compromised

- **Ex5:** Define security requirements in service-level agreements (SLAs) for monitoring suppliers for acceptable security performance throughout the supplier relationship lifecycle

GV.SC-08:

- **Ex1:** Define and use rules and protocols for reporting incident response and recovery activities and the status between the organization and its suppliers
- **Ex2:** Identify and document the roles and responsibilities of the organization and its suppliers for incident response
- **Ex3:** Include critical suppliers in incident response exercises and simulations
- **Ex4:** Define and coordinate crisis communication methods and protocols between the organization and its critical suppliers
- **Ex5:** Conduct collaborative lessons learned sessions with critical suppliers

IDENTIFY (ID)

Asset Management ID.AM-03 / ID.AM-05

Summary:
Up-to-date network-flow diagrams and a critical-asset list allowed the IRT to focus on edge routers and core services first.

Implementation Examples:
ID.AM-03:

- **Ex1:** Maintain baselines of communication and data flows within the organization's wired and wireless networks
- **Ex2:** Maintain baselines of communication and data flows between the organization and third parties
- **Ex3:** Maintain baselines of communication and data flows for the organization's infrastructure-as-a-service (IaaS) usage
- **Ex4:** Maintain documentation of expected network ports, protocols, and services that are typically used among authorized systems

ID.AM-05:

- **Ex1:** Define criteria for prioritizing each class of assets
- **Ex2:** Apply the prioritization criteria to assets
- **Ex3:** Track the asset priorities and update them periodically or when significant changes to the organization occur

Risk Assessment ID.RA-03 / ID.RA-04 / ID.RA-05

Summary:
Threat of volumetric ICMP floods and their business impact were pre-assessed, enabling swift prioritization of mitigation.

Implementation Examples:
ID.RA-03:

- **Ex1:** Use cyber threat intelligence to maintain awareness of the types of threat actors likely to target the organization and the TTPs they are likely to use
- **Ex2:** Perform threat hunting to look for signs of threat actors within the environment
- **Ex3:** Implement processes for identifying internal threat actors

ID.RA-04:

- **Ex1:** Business leaders and cybersecurity risk management practitioners work together to estimate the likelihood and impact of risk scenarios and record them in risk registers

- **Ex2:** Enumerate the potential business impacts of unauthorized access to the organization's communications, systems, and data processed in or by those systems

- **Ex3:** Account for the potential impacts of cascading failures for systems of systems

ID.RA-05:

- **Ex1:** Develop threat models to better understand risks to the data and identify appropriate risk responses

- **Ex2:** Prioritize cybersecurity resource allocations and investments based on estimated likelihoods and impacts

Improvement ID.IM-02 / ID.IM-04

Summary:
Scheduled DDoS exercises and IR-plan updates are added to the continuous-improvement backlog.

Implementation Examples:
ID.IM-02:

- **Ex1:** Identify improvements for future incident response activities based on findings from incident response assessments (e.g., tabletop exercises and simulations, tests, internal reviews, independent audits)

- **Ex2:** Identify improvements for future business continuity, disaster recovery, and incident response activities based on exercises performed in coordination with critical service providers and product suppliers

- **Ex3:** Involve internal stakeholders (e.g., senior executives, legal department, HR) in security tests and exercises as appropriate

- **Ex4:** Perform penetration testing to identify opportunities to improve the security posture of selected high-risk systems as approved by leadership

- **Ex5:** Exercise contingency plans for responding to and recovering from the discovery that products or services did not originate with the contracted supplier or partner or were altered before receipt

- **Ex6:** Collect and analyze performance metrics using security tools and services to inform improvements to the cybersecurity program

ID.IM-04:

- **Ex1:** Establish contingency plans (e.g., incident response, business continuity, disaster recovery) for responding to and recovering from adverse events that can

interfere with operations, expose confidential information, or otherwise endanger the organization's mission and viability

- **Ex2:** Include contact and communication information, processes for handling common scenarios, and criteria for prioritization, escalation, and elevation in all contingency plans
- **Ex3:** Create a vulnerability management plan to identify and assess all types of vulnerabilities and to prioritize, test, and implement risk responses
- **Ex4:** Communicate cybersecurity plans (including updates) to those responsible for carrying them out and to affected parties
- **Ex5:** Review and update all cybersecurity plans annually or when a need for significant improvements is identified

PROTECT (PR)

Identity & Access Control PR.AA-05

Summary:
Firewall ACLs enforce least-privilege ICMP access from trusted sources once services resume.

Implementation Examples:

- **Ex1:** Review logical and physical access privileges periodically and whenever someone changes roles or leaves the organization, and promptly rescind privileges that are no longer needed
- **Ex2:** Take attributes of the requester and the requested resource into account for authorization decisions (e.g., geolocation, day/time, requester endpoint's cyber health)
- **Ex3:** Restrict access and privileges to the minimum necessary (e.g., zero trust architecture)
- **Ex4:** Periodically review the privileges associated with critical business functions to confirm proper separation of duties

Awareness & Training PR.AT-01 / PR.AT-02

Summary:
"Lessons-learned" session and new staff training on DDoS recognition & playbooks are planned.

Implementation Examples:

PR.AT-01:

- **Ex1:** Provide basic cybersecurity awareness and training to employees, contractors, partners, suppliers, and all other users of the organization's non-public resources
- **Ex2:** Train users to recognize social engineering attempts and other common attacks, report attacks and suspicious activity, comply with acceptable use policies, and perform basic cyber hygiene tasks (e.g., patching software, choosing passwords, protecting credentials)
- **Ex3:** Explain the consequences of cybersecurity policy violations, both to individual users and the organization as a whole
- **Ex4:** Periodically assess or test users on their understanding of basic cybersecurity practices
- **Ex5:** Require annual refreshers to reinforce existing practices and introduce new practices

PR.AT-02:

- **Ex1:** Identify the specialized roles within the organization that require additional cybersecurity training, such as physical and cybersecurity personnel, finance personnel, senior leadership, and anyone with access to business-critical data
- **Ex2:** Provide role-based cybersecurity awareness and training to all those in specialized roles, including contractors, partners, suppliers, and other third parties
- **Ex3:** Periodically assess or test users on their understanding of cybersecurity practices for their specialized roles
- **Ex4:** Require annual refreshers to reinforce existing practices and introduce new practices

Platform Security PR.PS-01 / PR.PS-04 / PR.PS-05

Summary:
Edge-firewall rule changes (rate-limiting, ICMP drop) applied through approved configuration management and fully logged.

Implementation Examples:

PR.PS-01:

- **Ex1:** Establish, test, deploy, and maintain hardened baselines that enforce the organization's cybersecurity policies and provide only essential capabilities (i.e., principle of least functionality)
- **Ex2:** Review all default configuration settings that may potentially impact cybersecurity when installing or upgrading software
- **Ex3:** Monitor implemented software for deviations from approved baselines

PR.PS-04:

- **Ex1:** Configure all operating systems, applications, and services (including cloud-based services) to generate log records
- **Ex2:** Configure log generators to securely share their logs with the organization's logging infrastructure systems and services
- **Ex3:** Configure log generators to record the data needed by zero-trust architectures

PR.PS-05:

- **Ex1:** When risk warrants it, restrict software execution to permitted products only or deny the execution of prohibited and unauthorized software
- **Ex2:** Verify the source of new software and the software's integrity before installing it

- **Ex3:** Configure platforms to use only approved DNS services that block access to known malicious domains
- **Ex4:** Configure platforms to allow the installation of organization-approved software only

Technology Infrastructure Resilience PR.IR-01 / PR.IR-03 / PR.IR-04

Summary:
IDS/IPS tuning and capacity headroom ensure the network can absorb future volumetric bursts.

Implementation Examples:

PR.IR-01:

- **Ex1:** Logically segment organization networks and cloud-based platforms according to trust boundaries and platform types (e.g., IT, IoT, OT, mobile, guests), and permit required communications only between segments
- **Ex2:** Logically segment organization networks from external networks, and permit only necessary communications to enter the organization's networks from the external networks
- **Ex3:** Implement zero trust architectures to restrict network access to each resource to the minimum necessary
- **Ex4:** Check the cyber health of endpoints before allowing them to access and use production resources

PR.IR-03:

- **Ex1:** Avoid single points of failure in systems and infrastructure
- **Ex2:** Use load balancing to increase capacity and improve reliability
- **Ex3:** Use high-availability components like redundant storage and power supplies to improve system reliability

PR.IR-04:

- **Ex1:** Monitor usage of storage, power, compute, network bandwidth, and other resources
- **Ex2:** Forecast future needs, and scale resources accordingly

DETECT (DE)

Continuous Monitoring DE.CM-01 / DE.CM-09

Summary:
At 14:03 the SIEM flagged an inbound-traffic spike; routers and servers continued to feed telemetry during the event.

Implementation Examples:

DE.CM-01:

- **Ex1:** Monitor DNS, BGP, and other network services and protocols for adverse events
- **Ex2:** Monitor wired and wireless networks for connections from unauthorized endpoints
- **Ex3:** Monitor facilities for unauthorized or rogue wireless networks
- **Ex4:** Compare actual network flows against baselines to detect deviations
- **Ex5:** Monitor network communications to identify changes in security postures for zero trust purposes

DE.CM-09:

- **Ex1:** Monitor email, web, file sharing, collaboration services, and other common attack vectors to detect malware, phishing, data leaks and exfiltration, and other adverse events
- **Ex2:** Monitor authentication attempts to identify attacks against credentials and unauthorized credential reuse
- **Ex3:** Monitor software configurations for deviations from security baselines
- **Ex4:** Monitor hardware and software for signs of tampering
- **Ex5:** Use technologies with a presence on endpoints to detect cyber health issues (e.g., missing patches, malware infections, unauthorized software), and redirect the endpoints to a remediation environment before access is authorized

Adverse Event Analysis DE.AE-02 / DE.AE-03 / DE.AE-04 / DE.AE-08

Summary:
NetFlow, firewall, and IDS data were correlated; the event met incident criteria at 14:15 and was declared a DDoS.

Implementation Examples:

DE.AE-02:

- **Ex1:** Use security information and event management (SIEM) or other tools to continuously monitor log events for known malicious and suspicious activity
- **Ex2:** Utilize up-to-date cyber threat intelligence in log analysis tools to improve detection accuracy and characterize threat actors, their methods, and indicators of compromise
- **Ex3:** Regularly conduct manual reviews of log events for technologies that cannot be sufficiently monitored through automation
- **Ex4:** Use log analysis tools to generate reports on their findings

DE.AE-03:

- **Ex1:** Constantly transfer log data generated by other sources to a relatively small number of log servers
- **Ex2:** Use event correlation technology (e.g., SIEM) to collect information captured by multiple sources
- **Ex3:** Utilize cyber threat intelligence to help correlate events among log sources

DE.AE-04:

- **Ex1:** Use SIEMs or other tools to estimate impact and scope, and review and refine the estimates
- **Ex2:** A person creates their own estimates of impact and scope

DE.AE-08:

- **Ex1:** Apply incident criteria to known and assumed characteristics of activity in order to determine whether an incident should be declared
- **Ex2:** Take known false positives into account when applying incident criteria

RESPOND (RS)

Incident Management RS.MA-01 / RS.MA-03 / RS.MA-05

Summary:
The IR plan was executed; the event was categorized as “High-Severity Availability Incident”; criteria to start recovery (ICMP PPS < threshold) were defined.

Implementation Examples:

RS.MA-01:

- **Ex1:** Detection technologies automatically report confirmed incidents
- **Ex2:** Request incident response assistance from the organization’s incident response outsourcer
- **Ex3:** Designate an incident lead for each incident
- **Ex4:** Initiate execution of additional cybersecurity plans as needed to support incident response (e.g., business continuity and disaster recovery)

RS.MA-03:

- **Ex1:** Further review and categorize incidents based on the type of incident (e.g., data breach, ransomware, DDoS, account compromise)
- **Ex2:** Prioritize incidents based on their scope, likely impact, and time-critical nature
- **Ex3:** Select incident response strategies for active incidents by balancing the need to quickly recover from an incident with the need to observe the attacker or conduct a more thorough investigation

RS.MA-05:

- **Ex1:** Apply incident recovery criteria to known and assumed characteristics of the incident to determine whether incident recovery processes should be initiated
- **Ex2:** Take the possible operational disruption of incident recovery activities into account

Incident Analysis RS.AN-03 / RS.AN-06 / RS.AN-08

Summary:
Root-cause analysis traced disruption to spoofed ICMP floods; all actions and logs were preserved for forensics.

Implementation Examples:

RS.AN-03:

- **Ex1:** Determine the sequence of events that occurred during the incident and which assets and resources were involved in each event
- **Ex2:** Attempt to determine what vulnerabilities, threats, and threat actors were directly or indirectly involved in the incident
- **Ex3:** Analyze the incident to find the underlying, systemic root causes
- **Ex4:** Check any cyber deception technology for additional information on attacker behavior

RS.AN-06:

- **Ex1:** Require each incident responder and others (e.g., system administrators, cybersecurity engineers) who perform incident response tasks to record their actions and make the record immutable
- **Ex2:** Require the incident lead to document the incident in detail and be responsible for preserving the integrity of the documentation and the sources of all information being reported

RS.AN-08:

- **Ex1:** Review other potential targets of the incident to search for indicators of compromise and evidence of persistence
- **Ex2:** Automatically run tools on targets to look for indicators of compromise and evidence of persistence

Incident Response Reporting & Communication RS.CO-02 / RS.CO-03

Summary:
Upper management, the DPO, and (if required) law enforcement are notified per policy.

Implementation Examples:

RS.CO-02:

- **Ex1:** Follow the organization's breach notification procedures after discovering a data breach incident, including notifying affected customers
- **Ex2:** Notify business partners and customers of incidents in accordance with contractual requirements
- **Ex3:** Notify law enforcement agencies and regulatory bodies of incidents based on criteria in the incident response plan and management approval

RS.CO-03:

- **Ex1:** Securely share information consistent with response plans and information sharing agreements

- **Ex2:** Voluntarily share information about an attacker's observed TTPs, with all sensitive data removed, with an Information Sharing and Analysis Center (ISAC)
- **Ex3:** Notify HR when malicious insider activity occurs
- **Ex4:** Regularly update senior leadership on the status of major incidents
- **Ex5:** Follow the rules and protocols defined in contracts for incident information sharing between the organization and its suppliers
- **Ex6:** Coordinate crisis communication methods between the organization and its critical suppliers

Incident Mitigation RS.MI-01 / RS.MI-02

Summary:
Containment: Drop rules + shut down non-critical services.
Eradication: Rate-limit + source-verification rules to block residual attack traffic.

Implementation Examples:

RS.MI-01:

- **Ex1:** Cybersecurity technologies (e.g., antivirus software) and cybersecurity features of other technologies (e.g., operating systems, network infrastructure devices) automatically perform containment actions
- **Ex2:** Allow incident responders to manually select and perform containment actions
- **Ex3:** Allow a third party (e.g., internet service provider, managed security service provider) to perform containment actions on behalf of the organization
- **Ex4:** Automatically transfer compromised endpoints to a remediation virtual local area network (VLAN)

RS.MI-02:

- **Ex1:** Cybersecurity technologies and cybersecurity features of other technologies (e.g., operating systems, network infrastructure devices) automatically perform eradication actions
- **Ex2:** Allow incident responders to manually select and perform eradication actions
- **Ex3:** Allow a third party (e.g., managed security service provider) to perform eradication actions on behalf of the organization

RECOVER (RC)

Incident Recovery Plan Execution RC.RP-01 / RC.RP-02 / RC.RP-05 / RC.RP-06

Summary:
IRT restored email, DNS, and customer portals first; verified service health; declared recovery complete once ICMP volume normalized.

Implementation Examples:

RC.RP-01:

- **Ex1:** Begin recovery procedures during or after incident response processes
- **Ex2:** Make all individuals with recovery responsibilities aware of the plans for recovery and the authorizations required to implement each aspect of the plans

RC.RP-02:

- **Ex1:** Select recovery actions based on the criteria defined in the incident response plan and available resources
- **Ex2:** Change planned recovery actions based on a reassessment of organizational needs and resources

RC.RP-05:

- **Ex1:** Check restored assets for indicators of compromise and remediation of root causes of the incident before production use
- **Ex2:** Verify the correctness and adequacy of the restoration actions taken before putting a restored system online

RC.RP-06:

- **Ex1:** Prepare an after-action report that documents the incident itself, the response and recovery actions taken, and lessons learned
- **Ex2:** Declare the end of incident recovery once the criteria are met

Incident Recovery Communication RC.CO-03 / RC.CO-04

Summary:
Progress updates sent to internal stakeholders and clients; a public status-page post closed the incident.

Implementation Examples:

RC.CO-03:

- **Ex1:** Securely share recovery information, including restoration progress, consistent with response plans and information sharing agreements
- **Ex2:** Regularly update senior leadership on recovery status and restoration progress for major incidents
- **Ex3:** Follow the rules and protocols defined in contracts for incident information sharing between the organization and its suppliers
- **Ex4:** Coordinate crisis communication between the organization and its critical suppliers

RC.CO-04:

- **Ex1:** Follow the organization's breach notification procedures for recovering from a data breach incident
- **Ex2:** Explain the steps being taken to recover from the incident and to prevent a recurrence