Interreg
Co-funded by the European Union
Italy – Croatia
CRESPORT

CRESPORT
"Improving the Cyber REsilience and Security of Adriatic PORTs"

Report on Cross-Border cyber resilience and security assessment (D.1.1.1)

Document Control Sheet

Project number:	ITHR0200152
Project acronym	CRESPORT
Project Title	Improving the Cyber Resilience and Security of Adriatic PORTs
Start /end of the project	01/03/2024 – 31/08/2026

Work package	WP1
Activity	1.1
Deliverable name:	Report on Cross-Border cyber resilience and security assessment
Type of deliverable	Report
Language (s)	English
Dissemination Level	Public /website
Work Package Leader	PP6 NASPA - North Adriatic Sea port Authority (Ports of Venice and Chioggia)
External experts WP leader	IBM Italia spa
Document date	20/11/2024
Version number	Draft 0
Partners peer review #1 due date	27/11/2024
Partners peer review #2 due date	
Approval date deadline	04/12/2024
Submitted by	WP Coordinator PP6 NASPA
Final delivery date	11/12/2024

DISCLAIMER
The content of this deliverable represents the views of the authors only and is their sole responsibility; it cannot be considered to reflect the views of the INTERREG V-A IT-HR CBC Programme or any other body of the ITALY CROATIA CROSS-BORDER COOPERATION PROGRAMME. The INTERREG V-A IT-HR CBC Programme do not accept any responsibility for use that may be made of the information it contains.

Index

Glossary

Name	Description
AI	Artificial Intelligence
BIA	Business Impact Analysis
CRESPORT	Cyber REsilience and Security of Adriatic PORTs
CSF 2.0	NIST Cybersecurity Security Framework 2.0
IDS	Intrusion Detection System
IoT	Internet of Things
IT	Information Technology
MFA	Multi-factor Authentication
NIST	National Institute of Standards and Technologies
OT	Operational Technology
SBQSG	NIST CSF 2.0 : Small Business Quick-Start Guide
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOC	Security Operations Center
UBA	User Behavior Analytics

1. Executive Summary

Purpose and project’s context

CRESPORT project aims to address the challenge of providing ports in the Adriatic area with a more secure and resilient IT infrastructure. Considering ports as critical and vulnerable infrastructures, CRESPORT intends to address this common problem through cooperation and joint actions, which are essential to strengthen territorial cohesion, by adopting a common strategy to ensure compliance with the main international cybersecurity standards (e.g. EU directives, national legislation, IMO recommendations).

The Adriatic ports play a strategic role in terms of logistics and commercial development. In recent years these ports have been experiencing significant growth in the maritime transport sector, both in logistics and goods handling. As known since the last decade, digitalization is growing in ports and in logistics in general and today is one of the key factors for the competitiveness of the supply chain.

Emerging technologies (e.g. IoT, AI, …) are generating a new digital revolution in port infrastructures and in the logistic processes

Given the economic and geographical relevance of the Adriatic Ports, which constitutes a joint economic and environmental resource, the big common challenge is how to empower the capacity of each port to early detect and counter cyber-attacks to make the ports of the Area more secure. In this context, strong multilateral cooperation, through the adoption of joint actions and strategy, represents the concrete response to the building of a strengthening of the port infrastructures, for sure a considerable opportunity of growth and territorial cohesion.

The Project, led by the Port Authority of Ravenna, includes also the Italian Port System Authorities of Ancona, Venice and Trieste, and on the Croatian side, the Port Authorities of Rijeka, Ploče and Dubrovnik.

The purpose of this Security Assessment report is to provide an overview of the cybersecurity posture of the seven Adriatic Port Authorities, hereafter referred to as "Partners", participating to the CRESPORT project.

This assessment aims to support the program’s objective of improving awareness about the cybersecurity of Adriatic port systems by evaluating the current state of cybersecurity and identifying areas for improvement.

Overview

The Partners filled out a questionnaire about the level of implementation of best practice security controls inspired to the widespread NIST CSF 2.0 cybersecurity framework. The responses revealed security strengths and issues that are relevant to the Partners' cybersecurity posture and that are highlighted in this report.

It's worth noting that the findings were not uniform across all Partners, and some of them may not apply to some Partners or only in part. The data presented below are averaged over the Partners, and no findings are attributed to a specific Partner.

Additionally, the Partners were offered the choice of providing only high-level statistics, and the reported findings may or may not apply to the Partners that opted for this approach. Therefore, the findings should be interpreted as general trends and areas for improvement, rather than specific assessments of individual Partners.

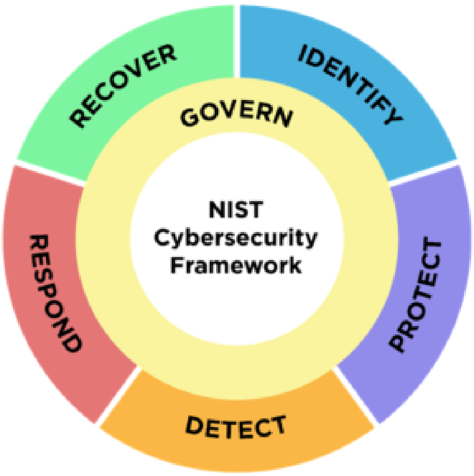
Statistics

The questions were grouped according to the six high level Functions and 22 Categories of the NIST CSF 2.0. Each answer expresses the Partner's implementation level of a distinct best practice security control. The answers were averaged over the Partners and the following diagrams show the resulting distributions of the average implementation level per Function and per Category.

Implementation Levels

The Implementation Level is defined as the percentage of best practice security controls in the questionnaire that have been implemented for a given area. The Implementation Level for a fully implemented control is evaluated as 100%, for a partially implemented one as 50% and for a not implemented one as 0%. The scores are averaged over the controls of the designed security area and over the Partners' responses.

Implementation Levels are evaluated over the six security areas (*Functions*) of the NIST Cybersecurity Security Framework 2.0.



Implementation Index

Each security control in the questionnaire contributes to the overall security posture along three dimensions of cybersecurity management:

1. **Practice**: This dimension assesses the actual implementation of security controls, such as the use of firewalls, intrusion detection systems and encryption.
2. **Procedures**: This dimension evaluates the formalization of requirements and processes into policies, procedures, and standards. This includes the development of security policies, incident response plans and training programs.
3. **Governance**: This dimension examines the controls in place to manage cybersecurity processes, prevent drifts and improve over time. This includes the establishment of a cybersecurity governance framework, risk management processes and continuous monitoring and evaluation.

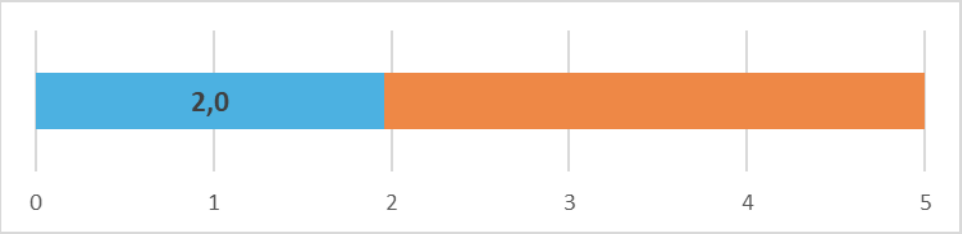
An aggregate statistic is introduced, the **Implementation Index**, which assigns different weights to the three dimensions and results in a number between 0 (worst case) and 5 (best case).

The Implementation Index for a security area is evaluated according to the following formula:

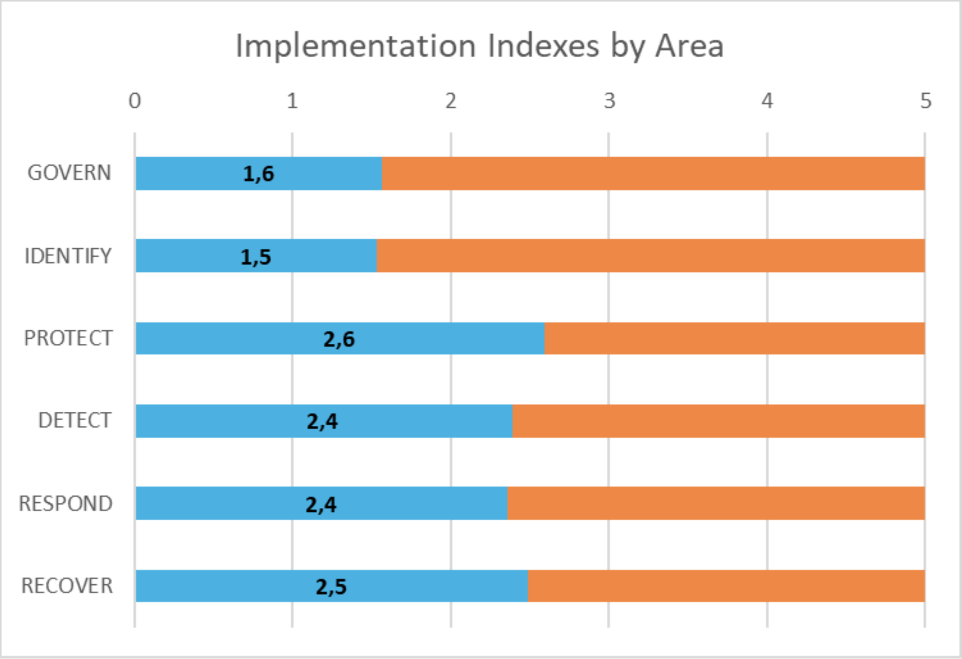
Implementation Index = 2.5 x Practice Implementation Level + 1.5 x Procedures Implementation Level + 1.0 x Governance Implementation Level

The weights represent the relative importance of covering the three dimensions for an organization with limited cybersecurity resources and are based on the extensive experience gained in similar projects by IBM consultants.

Overall Implementation Index



Implementation Indexes by Area



Strengths

During the security assessment, several strengths in the Partners' cybersecurity posture were observed. These strengths demonstrate that the Partners have implemented a layer of effective security controls and practices to protect their cybersecurity posture.

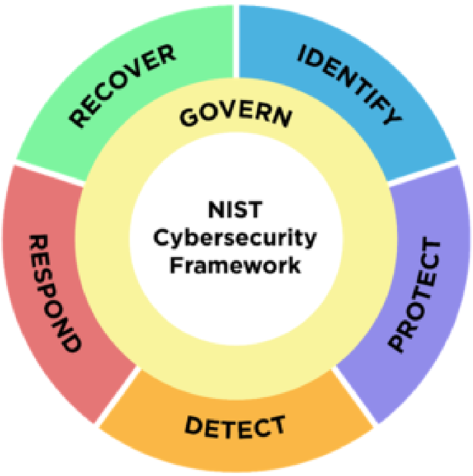
Effective User Authentication
One of the observed strengths was the centralized management of user authentication at endpoints. This practice helps to ensure that only authorized users have access to the endpoints, reducing the risk of unauthorized access and potential security breaches.

Robust Endpoint Protection
Another observed strength was the protection of endpoints by centralized and up-to-date anti-malware agents. This is a critical control that helps to prevent malware infections and protect against various types of cyber threats.

Immutable Backups
The Partners were also found to keep immutable copies of backups, which is a best practice that helps to protect against ransomware and other kinds of malicious tampering attacks. This ensures that backups are not compromised by malware or other types of attacks and can support to restore systems in case of a disaster.

Key Findings

Key findings are grouped by the six security areas (*Functions*) of the NIST Cybersecurity Security Framework 2.0 for easier consultation.



Govern

This area focuses on establishing and maintaining effective cybersecurity measures within an organization. Its main objective is to create a robust foundation upon which the other functions can operate efficiently.

#	Issue	Impact	Suggested Remediations
1	It is not assessed how cybersecurity risks can impede achieving the organization’s goals.	The organization may struggle to effectively integrate cybersecurity risk management with broader strategic initiatives, leading to potential misalignment between cybersecurity measures and overall business objectives.	Assess how cybersecurity risks can impede achieving the organization’s business goals. Assess whether a Business Impact Analysis would be valuable to understand asset dependencies and the impacts of asset losses on your business processes.
2	Legal, regulatory, and contractual cybersecurity requirements are not clearly assessed.	Compliance becomes uncertain, exposing the organization to significant penalties and reputational damage.	State your legal, regulatory, and contractual cybersecurity requirements.

		Failing to comply can lead to fines, lawsuits, and damaged relationships with clients and partners who expect robust cybersecurity protections.	
3	A comprehensive risk management strategy is not set, applied and maintained.	Absent a cohesively defined and sustained risk management strategy, the organization operates reactively instead of strategically.	Establish who within your business will be responsible for developing and executing the cybersecurity strategy. Prioritize managing cybersecurity risks together with other organization risks. Assess whether cybersecurity insurance is appropriate for your organization.
4	Leaders' expectations regarding a secure and ethical culture are not shared or only in part.	Leadership's failure to convey expectations concerning a robust and principled cultural ethos undermines employee engagement and commitment towards safeguarding sensitive information	Communicate leadership's support of a risk-aware, ethical, and continually improving culture.
5	Cybersecurity responsibilities are not clearly articulated.	Unclear assignment of cybersecurity duties leads to confusion and neglect, creating loopholes that malicious actors can capitalize upon.	Define explicit cybersecurity roles and responsibilities.
6	Thorough due diligence is not performed on prospective suppliers	Insufficient scrutiny during vendor selection exacerbates inherent weaknesses, allowing subpar vendors to introduce latent hazards into the value chain, amplifying the aggregate threat landscape.	Assess cybersecurity risks posed by suppliers and other third parties before entering a formal relationship.
7	A comprehensive, understandable, and usable	Partial development or absence of a user-friendly risk	Communicate, enforce, and maintain policies for

	risk management policy is not created, disseminated, and maintained, or only in part.	management policy complicates implementation and enforcement, resulting in inconsistent application across departments.	managing cybersecurity risks with statements of management intent, expectations, and direction.

Identify

This cybersecurity area involves identifying and understanding the organization’s cybersecurity risks, including the identification of critical assets, data, and systems.

#	Issue	Impact	Suggested Remediations
1	A comprehensive inventory of physical devices, network devices, and software/services is not in place, or only in part.	In the absence of a comprehensive inventory some assets may not receive an adequate level of protection.	Develop and maintain a comprehensive inventory of all assets your organization depends upon, including hardware and data assets.
2	An inventory of data assets is usually not maintained.	Data that are not identified and classified may not be adequately protected.	Prioritize inventorying and classifying your business data.
3	Vulnerability management technologies are not used or only in part to identify unpatched and misconfigured software.	The risk of cyberattacks exploiting these weaknesses increases.	Assess your assets (both IT and physical) for potential vulnerabilities.
4	Internal and external threats to the organization are mostly not identified and recorded or only in part.	There is a higher chance of missing crucial warning signs that could otherwise prompt proactive measures against impending cybersecurity incidents.	Document internal and external cybersecurity threats and associated responses using a risk register.
5	The effectiveness of the organization's cybersecurity program is not assessed to	This hinders identifying necessary improvements, leaving the organization vulnerable to emerging	Assess the effectiveness of the organization's cybersecurity program to identify areas that need improvement.

	identify areas that need improvement.	threats without adequate safeguard updates	

Protect

This security area focuses on preventing or deterring cyber threats, including the implementation of security controls and measures to protect critical assets.

#	Issue	Impact	Suggested Remediations
1	Access and privileges are restricted only in part to the minimum necessary (e.g., *least privilege* principle, zero trust architecture).	Partial implementation of the least privilege principle and of Zero Trust Architecture increases the risk of unauthorized access, allowing attackers broader entryways into critical systems.	Understand what information employees should have access to and what they actually have access to. Restrict sensitive information access to only those employees who need it to do their jobs.
2	Multi-factor authentication (MFA) is not implemented or only in part for accessing critical systems and sensitive data.	There's heightened susceptibility to credential-based attacks, significantly increasing the chances of data breaches and system intrusions.	Require multi-factor authentication on all accounts that offer it. Consider using password managers to help generate and protect strong passwords.
3	There is no comprehensive awareness and training program in place.	Lack of a comprehensive awareness and training program leaves employees vulnerable to social engineering tactics like phishing attempts, further exposing the organization to exploitation.	Develop a comprehensive awareness and training program.
4	Not all Partners configure their laptops to enable full-disk encryption to protect data.	This practice jeopardizes sensitive data stored locally during travel or remote work scenarios.	Configure laptops and tablets to enable full-disk encryption to protect data.

5	The use of removable media is not restricted to prevent malware propagation and data exfiltration.	Unregulated use of removable media facilitates easier spread of malicious code and data leakage.	Restrict the use of removable media such as USB keys or USB storage.
6	Some Partners do not test backups and restores, or only in part, for all types of data sources at least annually.	Insufficient backup testing raises concerns about recoverability after ransomware or corruption incidents.	Regularly test your backups.
7	Routine and emergency patching are usually not performed or only in part within the timeframes specified in the vulnerability management plan.	Delays in patches leave known vulnerabilities open longer, inviting persistent threat actors to capitalize on outdated defenses.	Develop and implement a vulnerability management plan that includes routine and emergency patching procedures.

Detect

This area focuses on security controls to promptly detect unusual behaviors, signs of intrusion, and harmful events so that effective measures can be initiated against ongoing cybersecurity issues.

#	Issue	Impact	Remediation
1	Security Information and Event Management (SIEM) or other tools are not used to continuously centralize, protect, monitor and correlate log events from multiple sources for known malicious and suspicious activity, and to estimate the impact and scope of security incidents.	The absence of robust SIEM solutions limits real-time correlation and alert generation, impeding prompt incident detection and response.	Deploy a SIEM solution capable of collecting, aggregating, and scrutinizing large volumes of real-time data from varied origins.
2	A Security Operations Center (SOC) is mostly not used to collect and analyze alerts	The organization faces reduced situational awareness and delayed reaction times to emerging threats.	Use an external security operations center (SOC).

	generated by cybersecurity software.		
3	Remote and onsite administration and maintenance activities performed by external providers are not monitored, or only in part, by some Partners.	The lack of adequate monitoring of remote and onsite administrative tasks poses significant risks to the organization's cybersecurity.	Enforce stringent logging and oversight for remote administrative and third-party sessions. Employ multi-factor authentication (MFA) at least for admin and remote access accounts and record session details extensively. Review logs weekly for abnormal behaviors.
4	Service level agreements (SLAs) with external service providers do not include monitoring and response to potentially adverse events.	Insufficient coverage of SLAs for security event handling increases the risk of not detecting security attacks vehiculated through service providers.	Update SLAs to explicitly require proactive monitoring and rapid response times from vendors.
5	Authentication attempts are not monitored or only in part to identify attacks against credentials and unauthorized credential reuse.	Without proper tracking of authentication attempts, there is increased vulnerability to credential misuse and unauthorized access.	Configure the SIEM to automatically flag suspicious login failures, repeated invalid password entries, and unexpected geographical locations attempting access.
6	Software configurations are usually not monitored or only in part for deviations from security baselines.	Partial or absent monitoring of software configurations exposes the organization to configuration drift and compliance violations.	Automate software configuration checks via scripts running daily comparisons against gold images or configuration standards.

Respond

The main objective of the security controls in this area is to enhance an organization's capability to react effectively to cyber threats.

#	Issue	Impact	Remediation
1	An incident response plan is not in place.	The organization faces significant challenges in containing, investigating, and recovering from cybersecurity incidents efficiently and effectively.	Define an incident response plan including the execution of predefined measures upon detection of an incident, proper validation and triage of incident reports, categorization and prioritization of incidents, communications with internal and external stakeholders, necessary escalation mechanisms, and clear criteria for initiating recovery processes Define and implement incident management playbooks starting with the most likely and impactful types of cybersecurity incidents.

Recover

Security controls in this area serve two main purposes: first, they aim to restore assets and operations that have been affected by a cybersecurity incident. Second, they ensure that these recoveries are conducted promptly to minimize disruptions caused by such incidents.

#	Issue	Impact	Remediation
1	A comprehensive recovery plan is not in place.	The organization faces significant challenges in responding efficiently and	Develop a comprehensive recovery policy that includes procedures for developing

🟩		effectively to and recovering from cybersecurity incidents.	and implementing recovery plans.

Conclusion

This Security Assessment report provides a comprehensive overview of the cybersecurity posture of the CRESPORT port authorities. The findings and recommendations outlined in this report aim to support the Partners in improving their cybersecurity awareness and posture, ultimately contributing to the overall security of the Adriatic ports.

2. Assessment Methodology

The Security Assessment of the seven Adriatic port authorities followed a methodology aligned with the NIST Cyber Security Framework (CSF) 2.0. This framework provides a comprehensive structure for managing and reducing cybersecurity risk. In particular, the Security Assessment was conducted using a questionnaire compiled by the Partners. The questionnaire was designed to evaluate the Partners' cybersecurity posture covering the Functions (security areas) of the framework and across three dimensions of cybersecurity management:

1. **Practice**: This dimension assesses the actual implementation of security controls, such as the use of firewalls, intrusion detection systems, and encryption.
2. **Procedures**: This dimension evaluates the formalization of requirements and processes into policies, procedures, and standards. This includes the development of security policies, incident response plans, and training programs.
3. **Governance**: This dimension examines the controls in place to manage cybersecurity processes, prevent drifts, and improve over time. This includes the establishment of a cybersecurity governance framework, risk management processes, and continuous monitoring and evaluation.

Each question in the questionnaire was weighted along these three dimensions, allowing for a comprehensive evaluation of the Partners' cybersecurity posture. The weights were assigned based on the relative importance of each dimension in achieving a robust cybersecurity posture according to IBM’s extensive experience in the field.

The questionnaire was designed to be comprehensive and cover all aspects of cybersecurity management. The questions were structured to elicit specific information about the Partners' cybersecurity practices, procedures, and governance.

Assessment Criteria

The assessment criteria used to evaluate the Partners' responses to the questionnaire were based on industry best practices and standards, such as the NIST Cybersecurity Framework, NIST CSF 2.0. The criteria were designed to assess the Partners' ability to:

- Implement effective security controls
- Formalize requirements and processes into policies, procedures, and standards
- Control cybersecurity processes to prevent drifts and improve over time

Assessment Process

The assessment process involved the following steps:

1. Questionnaire preparation and distribution: The questionnaire was prepared by IBM assessment team and distributed to the Partners, who were asked to complete it and return it to the assessment team.
2. Questionnaire review: The assessment team reviewed the completed questionnaires to ensure that all questions had been answered and that the responses were complete.
3. Data analysis: The assessment team analyzed the data collected from the questionnaires to identify trends, patterns, and areas for improvement.
4. Report generation: The assessment team generated a report that summarized the findings and provided recommendations for improvement.

Reference Cybersecurity Framework

The Security Assessment was based on the NIST Cybersecurity Framework 2.0 (NIST CSF 2.0), which is a widely recognized and respected framework for managing cybersecurity risk. It consists of six Functions, which are designed to provide a comprehensive view of an organization's cybersecurity posture. The six Functions are:

Govern (GV)

Identify (ID)

Protect (PR)

Detect (DE)

Respond (RS)

Recover (RC)

These Functions are further divided into Categories and Subcategories, which provide a detailed framework for evaluating an organization's cybersecurity controls.

Functions and Categories

The assessment was based on a questionnaire that covered all six Functions, 22 Categories, and 108 Subcategories of the NIST CSF 2.0. Each Function, Category, and Subcategory was evaluated to determine the extent to which the Partner had implemented best practice security controls.

The Functions, Categories, and Subcategories were used to organize the questionnaire and ensure that all aspects of the Partner's cybersecurity posture be evaluated.

Questionnaire Design

The questionnaire was designed to be comprehensive and easy to understand. Each question was closed form and asked whether a specific best practice security control had been implemented. The possible answers were 'Yes', 'No', 'In part', and 'Not Applicable'.

The questionnaire was grouped by NIST CSF 2.0 Function, Category, and Subcategory, for a better navigation and contextualization.

Implementation Level

A scoring system was adopted to evaluate the Partner's **level of implementation** of best practice security controls. The scoring system was as follows:

- 0: the security control is not implemented
- 0.5: the security control is partially implemented
- 1: the security control is fully implemented
- NA: the security control is not applicable in the Partner’s context

Each question in the questionnaire was scored using this system, and the results were used to calculate an overall score for each Function, Category, and Subcategory.

The scoring system provided a clear and consistent way to evaluate the Partner's cybersecurity posture and identify areas for improvement.

Limitations

The assessment methodology had some limitations. The questionnaire was based on self-reported data, which may not always be accurate or complete. Additionally, the assessment was limited to the specific questions and criteria used in the questionnaire, which may not have captured all aspects of the Partners' cybersecurity posture.

The data presented in the Detailed Findings section are averaged over the Partners, and no finding should be attributed to a specific Partner. In particular, the findings were not uniformly distributed across all Partners, and some of them may not apply to some Partners or only in part.
Therefore, the findings of this assessment should be interpreted as general trends and areas for improvement, rather than specific assessments of individual Partners.

Additionally, the Partners were offered the choice of providing only high-level statistics, instead of the actual answers, not to disclose confidential information. Therefore, the reported findings may or may not apply to the Partners who adopted this approach.

3. Detailed Findings

The following section presents the detailed findings of the Security Assessment, organized by the NIST CSF 2.0 Functions and Categories.

The section dedicated to each Function reports its purpose, a description and statistics about its implementation level, followed by detailed findings for its Categories. The findings are presented as one or two tables per Category, “Most Relevant Issues” and “Other Issues”. The “Most Relevant Issues” table lists the issues that present a more significant cybersecurity risk and that should be addressed with a higher priority. The “Other issues” table lists issues that pose a lower risk and that can be addressed with a lower priority. While most Categories will have both tables, some may have only one.

Structure of the issues tables

Following are examples of the two issues tables. The color of the first field for each issue matches the one of the current NIST CSF 2.0 Function.

Most relevant Issues

#	Question id	Issue	Remediation
1	<<ID of the associated questionnaire question>>	<<Description of the issue>>	<<Suggested remediation(s)>>

Other Issues

#	Question id	Issue	Remediation
1	<<ID of the associated questionnaire question>>	<<Description of the issue>>	<<Suggested remediation(s)>>

Note. The color of the first field for each issue matches the one of the current NIST CSF 2.0 Function.

Govern (GV)

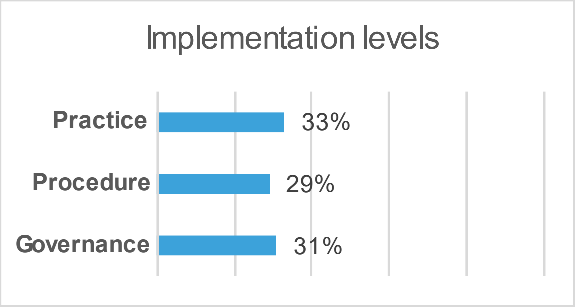
Purpose

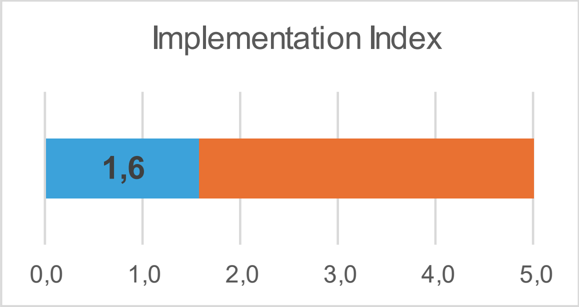
The Govern function plays a crucial role in establishing and maintaining effective cybersecurity measures within an organization. Its main objective is to create a robust foundation upon which the other functions can operate efficiently.

Description

The core responsibility of the Govern function involves setting up and monitoring an organization’s cybersecurity risk management strategy, expectations, and policies. This entails several key tasks aimed at fostering a strong cybersecurity culture throughout the entire organization. Firstly, the Govern function ensures that there is a thorough comprehension of the organization's goals, stakeholder demands, and compliance necessities. This understanding forms the basis for crafting precise and practical cybersecurity protocols aligned with the organization's strategic aims. Secondly, it establishes explicit roles, duties, and authoritative structures necessary for enforcing these policies effectively. Clear demarcation of responsibilities minimizes confusion and boosts efficiency in handling cyber threats. Furthermore, the Govern function oversees the implementation and regular review of these policies to guarantee consistency and relevancy amidst evolving digital landscapes.

Implementation Levels





Categories

GV.OC: Organizational Context

Purpose

The purpose of the NIST CSF 2.0 category “GV.OC: Organizational Context” Category is to ensure that the circumstances, including mission, stakeholder expectations, dependencies, and legal, regulatory and contractual requirements, surrounding an organization’s cybersecurity risk management decisions are thoroughly understood. By doing so, the organization gains insight necessary to formulate effective strategies aligned with its broader goals and compliance necessities.

Description

This category focuses on different elements. Firstly, there is a need to comprehend the organizational mission comprehensively enough to shape cybersecurity risk management initiatives around it. Secondly, identifying and acknowledging the needs and expectations of both internal and external stakeholders concerning cybersecurity becomes paramount. Thirdly, understanding and properly managing legal, regulatory, and contractual demands ensures compliance and minimizes exposure to penalties or litigious issues. Lastly, recognizing the interdependence between the organization and external entities facilitates smoother collaboration and mutual trust.

Strengths

- Relevant internal stakeholders and their cybersecurity-related expectations are identified.
- A process is mostly determined to track and manage legal and regulatory requirements regarding protection of individuals' information (e.g., General Data Protection Regulation).

Most Relevant Issues

#	Question id	Issue	Remediation
1	ea14d1b	Criteria are not usually established, or only in part, for determining the criticality of capabilities and services as viewed by internal and external stakeholders.	State how cybersecurity risks can impede achieving your business goals.
2	cbc397a	The organization's cybersecurity strategy is mostly aligned only in part with legal, regulatory, and contractual requirements	State your legal, regulatory, and contractual cybersecurity requirements.

Other Issues

#	Question id	Issue	Remediation
1	3245ea7	A process is not determined or only in part to track and manage contractual requirements for cybersecurity	Ensure that there are explicit policies and written agreements covering cybersecurity obligations among suppliers, customers, and partners.

		management of supplier, customer, and partner information.	
2	df1349e	An inventory is not created, or only in part, of the organization's dependencies on external resources (e.g., facilities, cloud-based hosting providers) and their relationships to organizational assets and business functions.	Create detailed inventories covering aspects from identifying essential assets to mapping crucial services offered by suppliers. Map out exactly how each dependence relates to crucial business areas and key assets. Prepare proactive countermeasures for likely fault lines stemming from reliance on external elements.
3	d376ec1	External dependencies that are potential points of failure for the organization's critical capabilities and services are not identified and documented or only in part.	Constantly evaluate and record vendor reliability and effectiveness.

GV.RM: Risk Management Strategy

Purpose

The purpose of the "GV.RM: Risk management Strategy" Category is to define and articulate an organization's priorities, constraints, risk tolerances, appetites, and assumptions concerning cybersecurity risks. By establishing these parameters, organizations aim to enhance decision-making around resource allocation and risk management strategies.

Description

This Category focuses on setting up comprehensive risk management protocols aligned with organizational objectives and missions. Specifically, it ensures that there is consensus among stakeholders regarding risk management aims, formulates precise definitions of risk appetite and tolerance thresholds, and integrates cybersecurity risk management seamlessly into wider enterprise risk management initiatives. Moreover, effective communication channels are emphasized to facilitate discussion and dissemination of vital risk-related information across departments, especially involving senior leadership.

Most Relevant Issues

#	Question id	Issue	Remediation
1		A comprehensive risk management strategy is not set and applied	Establish who within your business will be responsible for developing and executing the cybersecurity strategy. Prioritize managing cybersecurity risks together with other organization risks. Assess whether cybersecurity insurance is appropriate for your organization.

Other Issues

#	Question id	Issue	Remediation
1	a87277e	Near-term and long-term cybersecurity risk management objectives are not set and updated or only in part as part of annual strategic planning and when major changes occur.	Establish comprehensive and measurable near-term and long-term risk management goals.
2	e3e5d65	Measurable objectives for cybersecurity risk management (e.g., manage the quality of user training, ensure adequate risk protection for industrial control systems) are not established or only in part.	Define measurable objectives like "manage the quality of user training" and "set clear metrics tied to reducing phishing susceptibility rates among employees after mandatory quarterly trainings".
3	3f443b4	Risk appetite statements that convey expectations about the appropriate level of risk for the organization are not determined and communicated or only in part.	Formulate clear risk appetite statements: define acceptable thresholds for different classes of data, leveraging the structure offered by CSF profiles and tiers.
4	dd33425	Cybersecurity risks are not aggregated and managed, or only in part, alongside other enterprise risks (e.g., compliance, financial, operational, regulatory, reputational, safety).	Aggregate and align all risks: utilize the CSF to merge cybersecurity risks seamlessly with broader enterprise risks, covering areas such as finance, regulation, reputation, and operation.

5	10a7f32	Criteria are not specified or only in part for accepting and avoiding cybersecurity risk for various classifications of data.	Specific criteria for accepting/rejecting risks: develop explicit rules governing acceptance versus avoidance of cybersecurity risks per data categories to ensure consistent decision making aligned with predefined risk tolerances
6	21a25a8	A process is not in place or only in part for updating senior executives, directors, and management on the organization's cybersecurity posture at agreed-upon intervals.	Update senior leadership regularly: establish formal reporting mechanisms to keep executive boards appraised regularly on evolving cybersecurity status via dashboards or periodic meetings.
7	6c656e2	Criteria are not established for risk prioritization at the appropriate levels within the enterprise.	Set up risk prioritization methodologies: employ systematic protocols for ranking cybersecurity risks according to severity and urgency. Engage experts periodically to refine priority lists dynamically.

GV.RR: Roles, Responsibilities, And Authorities

Purpose

The purpose of the "GV.RR: Roles, Responsibilities, and Authorities" Category is to establish and communicate cybersecurity roles, responsibilities, and authorities within an organization. This ensures accountability, facilitates performance assessment, and drives continuous improvement in cybersecurity risk management.

Description

This Category focuses on defining and disseminating the roles, responsibilities, and authoritative positions necessary for effective cybersecurity risk management. By clearly establishing these elements, organizations can create a structured environment where everyone understands their role in maintaining cybersecurity, thereby promoting a proactive and collaborative approach to risk management.

Most Relevant Issues

#	Question id	Issue	Remediation

1	8a0bd82	Leaders' expectations regarding a secure and ethical culture are not shared or only in part.	To promote a secure and ethical culture, leaders must explicitly define and communicate their expectations concerning cybersecurity behaviors. Ensure that internal and external stakeholders' needs and expectations regarding cybersecurity risk management are thoroughly understood and addressed. Regular updates and reinforcement of these messages are essential to embed cultural norms deeply.
2	6a1535c	Lack of clear articulation of cybersecurity responsibilities: • cybersecurity responsibilities and performance requirements are not included or only in part in personnel descriptions.	
3	33acc11	• Cybersecurity responsibilities are not clearly articulated or only in part within operations, risk functions, and internal audit functions.	Define explicit cybersecurity roles and responsibilities.

Other Issues

#	Question id	Issue	Remediation
1	a4ca471	Lack of resources: • Resource allocation and investment are not identified, or only in part, in line with risk tolerance and response.	Address resource allocation issues: align resource allocations closely with the organization's risk tolerance levels. Adequate resources should be assigned proportionately to match the policies laid out for cybersecurity. Enhanced budgeting mechanisms and regular review sessions should be instituted to evaluate whether investments adequately mirror the desired cybersecurity state.
2	8b97c48	• Adequate and sufficient people, process, and technical resources are not provided to support the cybersecurity strategy.	

3	f7f8072	Cybersecurity training is not included or only in part in the onboarding process for new employees.	Ensure comprehensive onboarding includes cybersecurity training: make sure every employee receives thorough cybersecurity education right upon joining the team. Extend this approach to periodic refresher courses to maintain up-to-date competencies.

GV.PO: Policy

Purpose

The main objective of the "GV.PO: Policy" Category revolves around establishing, disseminating, and implementing organizational cybersecurity policies.

Description

This Category's target involves creating robust policies aligned with the organization's strategic aims, cybersecurity strategies, and evolving requirements. Effective implementation requires regular review and updating of said policies to accommodate shifts in technological advancements, changing threats, and modifications in the organizational mission. Enforcement ensures compliance throughout the entire organization.

Strengths

- Senior management approval is required for cybersecurity policies.

Most Relevant Issues

#	Question id	Issue	Remediation
1	ad73238	A comprehensive, understandable, and usable risk management policy is not created, disseminated, and maintained, or only in part.	Communicate, enforce, and maintain policies for managing cybersecurity risks with statements of management intent, expectations, and direction.

Other Issues

#	Question id	Issue	Remediation

1	2fc81ce	Lack of cybersecurity policy reviews: • The cybersecurity policy and supporting processes and procedures are not periodically reviewed, or only in part, to ensure alignment with risk management strategy objectives and priorities, as well as the high-level direction of the cybersecurity policy.	Review and adjust the cybersecurity risk management strategy regularly to keep up with evolving organizational demands and risks. Make sure improvements are consistently derived from various sources like evaluation feedback, testing, daily operation observations, and documented plans.
2	567fcaf	• The cybersecurity policy is mostly not updated or only in part 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).	Ensure that the policy for managing cybersecurity risks is clearly stated, aligned with the organizational context, cybersecurity strategy, and priorities, then effectively communicated and enforced. Regularly review, update, communicate, and enforce the policy to adapt to changing requirements, threats, technologies, and missions.
3	3f26462	Personnel are usually not required, or only in part, to acknowledge receipt of policy when first hired, annually, and whenever policy is updated.	Emphasis must be placed on making certain that every member understands and complies with the latest iterations of the policy. Trainings and awareness sessions should equip everyone, especially those holding special functions, with adequate comprehension of cybersecurity protocols and compliance obligations.

GV.OV: Oversight

Purpose

The “GV.OV: Oversight” Category purpose is to establish mechanisms for monitoring compliance with the organization’s cybersecurity strategies, policies, and performance metrics. Ensuring alignment with internal goals and external requirements is crucial here

Description

This Category focuses on key tasks necessary for effective supervision. These involve reviewing and updating strategic directives, evaluating program effectiveness against defined criteria, tracking compliance with laws and contracts, and facilitating regular reviews involving senior leadership. Effective implementation ensures ongoing assessment and improvement aligned with evolving threats and technological advancements.

Most Relevant Issues

#	Question id	Issue	Remediation
1	3eb7c11	The cybersecurity risk management strategy is only partially reviewed and adjusted to ensure coverage of organizational requirements and risks	Review regularly. Ensure there's a regular schedule for reviewing the cybersecurity risk management strategy. Even without dedicated personnel, periodic reviews, perhaps quarterly or annually, can keep strategies up to date. Use checklists or simple audit forms to guide these sessions efficiently.
2	c53480c		

GV.SC: Cybersecurity Supply Chain Risk Management

Purpose

The purpose of the "GV.SC: Cybersecurity Supply Chain Risk Management" Category is to identify, establish, manage, monitor, and improve cybersecurity supply chain risk management processes. This ensures that organizations proactively address and mitigate risks arising from their supply chains, thereby protecting against vulnerabilities introduced via third parties like suppliers, vendors and service providers.

Description

This Category focuses on creating comprehensive measures to safeguard an organization's cybersecurity through effective supply chain management. Specifically, this entails establishing a robust cybersecurity supply chain risk management program complete with clearly articulated strategies, objectives, policies, and processes. Moreover, defining roles and responsibilities for all stakeholders, both internal and external, and integrating these elements seamlessly into wider corporate risk management initiatives forms another crucial aspect. Continuous monitoring and regular reviews enhance the effectiveness of these protocols, contributing significantly towards maintaining a strong defensive stance against evolving cyber threats originating from the supply chain network.

Strengths

- Supplier access to organization resources is verified to be deactivated promptly when it is no longer needed.

Most Relevant Issues

#	Question id	Issue	Remediation
1	f1e322d	Thorough due diligence is not performed on prospective suppliers that is consistent with procurement planning and commensurate with the level of risk, criticality, and complexity of each supplier relationship.	Assess cybersecurity risks posed by suppliers and other third parties before entering formal relationships.

Other Issues

#	Question id	Issue	Remediation
1	6c1b660	A cybersecurity supply chain risk management program is not established.	Develop a formal program that outlines the processes and procedures for managing cybersecurity risks within the supply chain. This program should include guidelines for identifying, assessing, and mitigating risks associated with suppliers and third parties.
2	2c885fa	One or more specific roles or positions are mostly not identified, or only in part, that will be responsible and accountable for planning, resourcing, and executing cybersecurity supply chain risk management activities.	Clearly define roles and responsibilities for planning, resourcing, and executing cybersecurity supply chain risk management activities. Assign these roles to existing staff members or consider hiring part-time or contracted cybersecurity experts.
3	c8298ac	Criteria for supplier criticality are mostly not developed, or only in part, based on, for example, the sensitivity of data processed or possessed by suppliers, the degree of access to the organization's systems, and the importance of the	Establish criteria for evaluating the criticality of suppliers based on factors such as data sensitivity, system access, and the importance of products or services. This will help prioritize risk management efforts.

		products or services to the organization's mission.	
4	00f79b7	Cybersecurity and supply chain requirements that third parties must follow, and how compliance with the requirements may be verified, are not included or only in part in default contractual language.	Update default contractual language to include specific cybersecurity and supply chain requirements that third parties must follow. Ensure that the contracts also outline how compliance with these requirements will be verified.
5	77f5bfd	A documented response plan is not in place for addressing risks posed by suppliers and third parties.	Develop a documented response plan for addressing risks posed by suppliers and third parties. This plan should include steps for incident detection, response, and recovery.
6	c90feab	Relevant suppliers and other third parties are usually not included, or only in part, in incident planning, response, and recovery activities.	Engage relevant suppliers and other third parties in incident planning, response, and recovery activities. This collaboration will help ensure a coordinated and effective response to cybersecurity incidents.
7	a65e818		

Identify (ID)

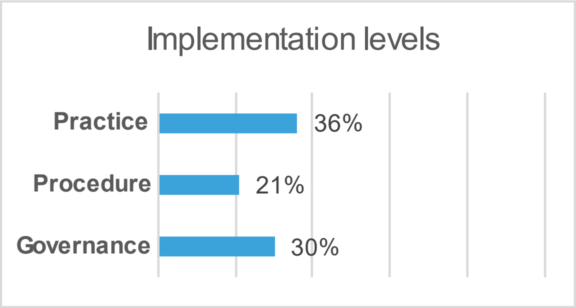
Purpose

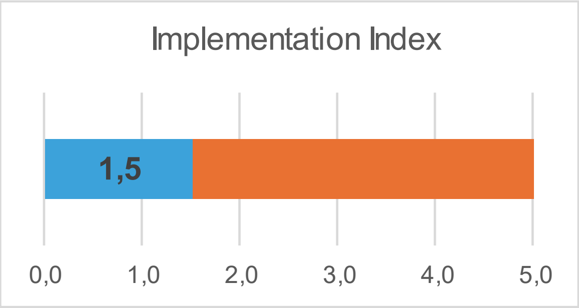
The Identify Function involves identifying and understanding the organization’s cybersecurity risks, including the identification of critical assets, data, and systems.

Description

This Function is critical in understanding the organization’s cybersecurity posture and identifying areas that require attention.

Implementation levels





Categories

ID.AM: Asset Management

Purpose

The purpose of the “ID.AM: Asset Management” Category within the Identify function of the NIST Cybersecurity Framework (CSF) 2.0 is to identify and manage assets crucial to the operation of the organization. By maintaining inventories of hardware, software, systems, networks, and services, along with representations of authorized communications, organizations can effectively safeguard against cybersecurity risks.

Description

This category focuses on identifying and cataloguing various elements, such as data, devices, personnel and services, that contribute to the functioning of the organization. This entails creating and updating thorough inventories of hardware, software and systems. Moreover, it requires mapping out authorized network connections and tracking the lifecycle stages of digital assets like data and IT solutions.

Underpinning this effort is the necessity to classify assets according to their significance and potential impact on core missions, thereby enabling targeted protective measures aligned with the organization's broader risk strategy.

Strengths

- Inventories are maintained for all types of hardware, including IT, IoT, OT, and mobile devices.

Most Relevant Issues

#	Question id	Issue	Remediation
1	55c412c	A comprehensive inventory of physical devices, network devices, and software/services is not in place, or only in part.	Develop and maintain a comprehensive inventory of all assets your organization depends upon, including hardware and data assets. Each inventory entry should contain at least the following information [ref. SBQSG]: – Software/ hardware/ system/ service – Asset's official use – Asset administrator or owner – Sensitive data the asset has access to – Is multi-factor authentication required to access this asset? – Risk to business if access to this asset is lost
2	19cde4b	An inventory of data assets is usually not maintained.	Prioritize inventorying and classifying your business data.

Other Issues

#	Question id	Issue	Remediation
1	5a920cc	Lack of constant monitoring of network and platforms to detect changes and update inventories.	Implement SIEM tools to continuously monitor log events for known malicious and suspicious activity. This will help in

			detecting changes and updating inventories in real-time.
2	ac1d985	Regular audits of the physical device inventory are not conducted.	Establish a regular schedule for auditing the physical device inventory. This will ensure that all devices are accounted for and any unauthorized devices are identified and addressed promptly.
3	ab431ca	Asset management processes are not formalized or documented, leading to potential security risks and compliance issues.	Formalize and document asset management processes

ID.IM: Improvement

Purpose

Improvement involves the processes and activities used to identify and implement changes to the organization's cybersecurity posture, including the identification of areas for improvement, the development of plans to address those areas, and the implementation of changes to improve the organization's cybersecurity.

Description

This Category is critical to improve cybersecurity posture over time and to ensure better alignment with industry best practices and regulatory requirements.

Most Relevant Issues

#	Question id	Issue	Remediation
1	c1b4058	The effectiveness of the organization's cybersecurity program is not assessed to identify areas that need improvement.	Assess the effectiveness of the organization's cybersecurity program to identify areas that need improvement.

Other Issues

#	Question id	Issue	Remediation

1	bb6f4b3	Cybersecurity policies, processes, and procedures are not annually reviewed or only in part to take lessons learned into account.	Develop a process for annually reviewing and updating cybersecurity policies, processes, and procedures to: • Take lessons learned into account. • Ensure that they aligned with industry best practices and regulatory requirements. • Identify areas for improvement. Assign a team or individual to be responsible for conducting the review and implementing updates. Provide training and resources to ensure that the team or individual has the necessary skills and knowledge to effectively conduct the review and implement updates.
2	74d6631	A vulnerability management plan is not created to identify and assess all types of vulnerabilities and to prioritize, test, and implement risk responses.	Develop a comprehensive vulnerability management plan that includes: • Identifying and assessing all types of vulnerabilities. • Prioritizing vulnerabilities based on risk. • Testing and implementing risk responses. • Continuously monitoring and evaluating the effectiveness of the plan. Assign a team or individual to be responsible for implementing and maintaining the plan. Provide training and resources to ensure that the team or individual has the necessary skills and knowledge to effectively implement the plan.

3	1318fd7	Contingency plans (e.g., incident response, business continuity, disaster recovery) are not established or only in part 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.	Develop comprehensive contingency plans (e.g., incident response, business continuity, disaster recovery) that include: • Procedures for responding to and recovering from adverse events • Communication plans for stakeholders and affected parties • Training and exercises to ensure that the plans are effective Assign a team or individual to be responsible for implementing and maintaining the plans Provide training and resources to ensure that the team or individual has the necessary skills and knowledge to effectively implement the plans.

ID.RA: Risk Assessment

Purpose

The purpose of the "ID.RA: Risk Assessment" Category is to enable organizations to comprehensively understand the cybersecurity risks posed to themselves, their assets, and individuals. By identifying and recording vulnerabilities, gathering and utilizing cyber threat intelligence, recognizing internal and external threats, and calculating the potential impacts and likelihoods of these threats, organizations gain insights necessary for effective risk management strategies.

Description

Within the "Risk Assessment" category, several key tasks are performed to fulfill its objective. Firstly, vulnerabilities present in the organization’s assets are meticulously documented. Secondly, ongoing reception and integration of cyber threat intelligence from reliable sources aid in maintaining up-to-date threat landscapes. Thirdly, both internal and external threats affecting the organization are pinpointed and catalogued. Furthermore, the likely consequences and probabilities of these threats materializing are evaluated and logged. Collectively, this information facilitates a thorough grasp of intrinsic risks, thereby guiding the selection, planning, tracking, and dissemination of suitable risk responses. Additional measures involve establishing protocols for dealing with newly discovered vulnerabilities and verifying the genuineness and completeness of acquired hardware and software before implementation. Lastly, crucial vendors are scrutinized preemptively to ascertain reliability and minimize associated hazards.

Most Relevant Issues

#	Question id	Issue	Remediation
1	2bae83b	Vulnerability management technologies are not used or only in part to identify unpatched and misconfigured software.	Assess your assets (IT and physical) for potential vulnerabilities. • Use vulnerability management technologies to identify unpatched and misconfigured software.
2	ef6c73a	Internal and external threats to the organization are mostly not identified and recorded or only in part.	Prioritize documenting internal and external cybersecurity threats and associated responses using a risk register.
3	e3297b0		

Other Issues

#	Question id	Issue	Remediation
1	1191330	Procedures for the formal documentation, review, testing, and approval of proposed changes and requested exceptions are not implemented and followed, or only in part.	Implement procedures for the formal documentation, review, testing, and approval of proposed changes and requested exceptions; partial implementation compromises consistency and introduces gaps that adversely affect cybersecurity.

2		Some Partners do not have a comprehensive risk assessment process in place. Risk assessments are not conducted regularly or formally documented.	Conduct regular, formally documented assessments to better prepare for and defend against potential threats.
3	af4400c	Supplier risk assessments are not conducted against business and applicable cybersecurity requirements, including the supply chain. A standardized approach or checklist is not used to assess critical suppliers' capabilities and compliance with organizational requirements.	Conduct supplier risk assessments using a standardized approach or checklist to verify critical suppliers' capabilities and compliance with organizational requirements, thus fortifying the entire supply chain.

Protect (PR)

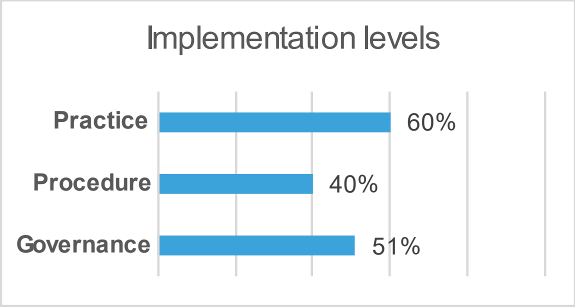
Purpose

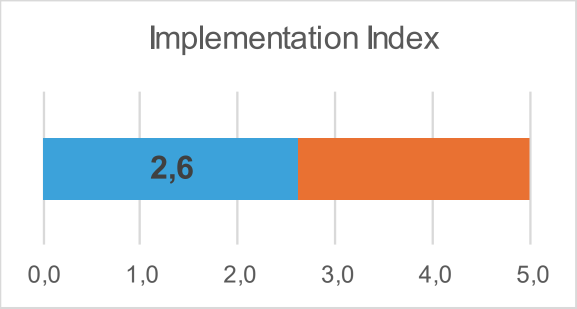
The Protect Function involves implementing measures to prevent or deter cyber threats, including the implementation of security controls and measures to protect critical assets.

Description

This Function is critical in preventing or deterring cyber threats and protecting critical assets.

Implementation Levels





Categories

PR.AA: Identity Management, Authentication, And Access Control

Purpose

The primary objective of the "PR.AA: Identity Management, Authentication, and Access Control" Category is to limit access to physical and logical assets exclusively to authorized users, services, and devices. This ensures that sensitive information remains safeguarded against unauthorized access, thereby reducing the risk of cybersecurity incidents. By employing robust identity verification methods and controlling user privileges, organizations aim to enhance their overall security posture.

Description

Identity Management, Authentication, and Access Control focuses on several core elements necessary for maintaining strong cyber defenses. Firstly, it emphasizes the proper administration of digital identities and credentials assigned to users, services, and hardware. Secondly, it underscores the significance of verifying identities through reliable authentication protocols. Additionally, it stresses the enforcement of strict access rules guided by the principle of least privilege, granting minimal necessary rights to fulfill job obligations without exposing excess data or functionality. Furthermore, this category highlights the necessity of protecting physical premises containing vital assets and continually reviewing access logs to spot unusual behavior promptly. Through meticulous management of identifications, stringent validation measures, and controlled entry parameters, companies strive to uphold a fortified defense barrier around crucial resources.

Strengths

- Policies for the minimum strength of passwords, PINs, and similar authenticators are usually enforced.
- Credentials are encrypted and protected against unauthorized access.
- Credentials are mostly not shared (group accounts are not in use).
- Logical and physical access privileges are usually reviewed periodically and whenever someone changes roles or leaves the organization, and privileges that are no longer needed are promptly rescinded.
- Physical controls are used to monitor facilities and restrict access.
- Guests, vendors, and other third parties are escorted within areas that contain business-critical assets.

Most Relevant Issues

#	Question id	Issue	Remediation
1	e0f1e4e	Access and privileges are restricted only in part to the minimum necessary (e.g., least privilege principle, zero trust architecture).	Understand what information employees should have access to and what they have access to. Restrict sensitive information access to only those employees who need it to do their jobs.
2	0465016	Multi-factor authentication (MFA) is not implemented or only in part for accessing critical systems and sensitive data.	Require multi-factor authentication on all accounts that offer it and consider using password managers to help generate and protect strong passwords. For example, start from these types of accounts: • Administrative Accounts • Remote Access User Accounts • Banking Accounts • Accounting and Tax Accounts • Merchant Accounts

			- Google, Microsoft, and/or Apple ID Accounts - Email Accounts - Password Managers - Website Accounts Provide training and resources to ensure that users understand the MFA process and can use it effectively.

Other Issues

#	Question id	Issue	Remediation
1	2e8bdbd	Policies and processes are not in place to manage the identities, credentials and access permissions of authorized users within the organization.	Develop and implement a documented identity and access management (IAM) process that includes: - User account creation and management - Password management and rotation - Role-based access control (RBAC) - Identity federation and single sign-on (SSO) - Procedures for requesting and approving access to systems, data, and resources - Guidelines for assigning permissions, entitlements, and authorizations - Requirements for access control reviews and audits
2	f368ee9	Some Partners do not maintain, or only in part, logs and records of physical access to critical assets.	Educate staff on the necessity of keeping precise and current records to facilitate quicker investigation and action in case of anomalous occurrences.

PR.AT: Awareness and Training

Purpose

The "PR.AT: Awareness and Training" Category aim is to ensure that an organization's personnel receive adequate cybersecurity awareness education and training. This empowers employees to recognize and effectively deal with cybersecurity risks in their daily responsibilities, thereby contributing to the overall safeguarding of the organization against cyber threats.

Description

Within the broader goal of protecting the organization's digital assets, the PR.AT Category focuses specifically on educating staff members. By providing regular and targeted cybersecurity training sessions, workshops, and educational material, the aim is to instill a culture of vigilance and preparedness. Employees learn how to spot phishing attempts, avoid malicious websites, follow password protocols, and comply with other necessary safety measures. Such initiatives enhance the collective readiness of the workforce to detect and deter cybersecurity issues proactively.

Most Relevant Issues

#	Question id	Issue	Remediation
1	ca139d7	There is no comprehensive awareness and training program in place.	Develop a comprehensive awareness and training program that includes regular training and awareness activities. • Communicate to your staff how to recognize common attacks, report attacks or suspicious activity, and perform basic cyber hygiene tasks.
2	43b1236	Users are not periodically assessed or tested on their understanding of basic cybersecurity practices.	• Assess timeliness and quality of the cybersecurity training over time.

PR.DS: Data Security

Purpose

The purpose of the PR.DS: Data Security Category is to outline measures aimed at protecting sensitive information against unauthorized access, modification, destruction, or leakage. By implementing robust data security protocols, organizations seek to preserve the confidentiality, integrity, and availability of their digital assets.

Description

Data Security (PR.DS) focuses on maintaining stringent protections around stored, transmitted, and processed data. This ensures that sensitive information remains intact and out of reach from malicious actors. Specific strategies involve encryption techniques, regular backup creation, verification of data integrity, and constant vigilance over data movement patterns. Comprehensive data security initiatives contribute significantly towards minimizing exposure to cyberthreats and bolstering an organization's defensive stance.

Strengths

- Full disk encryption is mostly used, fully or in part, to protect data stored on user endpoints.
- Access controls are in place to ensure that only authorized personnel can access backup data.
- Most Partners follow established backup and practices.
    - Critical data are continuously backed up in near-real-time (Continuous Data Protection, CDP), and other data are backed up frequently at agreed-upon schedules.

Most Relevant Issues

#	Question id	Issue	Remediation
1	04d8af4	Not all Partners configure their laptops to enable full-disk encryption to protect data.	Configure laptops and tablets to enable full-disk encryption to protect data.
2	3ecb0e8	The use of removable media is not restricted to prevent malware propagation and data exfiltration.	Restrict the use of removable media such as USB keys or USB storage. Implement technical controls to block or limit the use of removable media, such as: • USB drive blocking Group Policies or software • USB port locks
3	bb3a4bb	Some Partners do not test backups and restores, or only in part, for all types of data sources at least annually.	Regularly back up your data and test your backups.

Other Issues

#	Question id	Issue	Remediation

1	8c5a0b3	Removable media containing unencrypted sensitive information are not physically secured, such as within locked offices or file cabinets, or only in part.	Physically secure removable media containing unencrypted sensitive information within locked offices or file cabinets where feasible; alternatively, transition to encrypting such media wherever practical.
2	a014c06	Encryption, digital signatures, and cryptographic hashes are not used or only in part to protect the confidentiality and integrity of stored data in files, databases, virtual machine disk images, container images, and other resources.	Implement encryption, digital signatures, and cryptographic hashes comprehensively to protect the confidentiality and integrity of stored data in files, databases, virtual machine disk images, container images, and other resources.

PR.PS: Platform Security

Purpose

The purpose of Platform Security is to protect the organization's platforms, including operating systems, applications, and devices, from unauthorized access, use, disclosure, modification, or destruction.

Description

This Category involves the implementation of security controls and procedures to protect platforms from various types of threats, including malware, unauthorized access, and denial of service attacks. This includes implementing secure configuration and maintenance practices, generating logs, preventing the installation and execution of unauthorized software, developing software securely.

Strengths

- Established practices about secure configuration and maintenance are in place.
- The source and the integrity of new software are verified before installing it.
- Software execution is usually restricted to permitted products only, or the execution of prohibited and unauthorized software is denied.
- Hardware is usually replaced, or adequate compensating security controls are implemented, when it lacks needed security capabilities or when it cannot support software with needed security capabilities.

- Software used in production environments is maintained and is securely disposed of once it is no longer needed.

Most Relevant Issues

#	Question id	Issue	Remediation
1	5e1c778	Routine and emergency patching are usually not performed or only in part within the timeframes specified in the vulnerability management plan.	Develop and implement a vulnerability management plan that includes routine and emergency patching procedures. • Establish a process for reviewing and testing patches before they are applied. • Ensure that patching is performed within the timeframes specified in the vulnerability management plan. • Consider implementing a patch management system to automate the patching process. • Ensure that all systems and devices are patched to prevent vulnerabilities.

Other Issues

#	Question id	Issue	Remediation
1	b3abd74	Hardened baselines that enforce the organization's cybersecurity policies and provide only essential capabilities (i.e., principle of least functionality) are usually not established, tested, deployed, and maintained, or only in part.	Develop and implement hardened baselines that enforce the organization's cybersecurity policies and provide only essential capabilities.
2	a7299e5	Log generators are not configured to securely share their logs with the organization's logging infrastructure systems and services.	Configure log generators to securely share their logs with the organization's logging infrastructure systems and services.

			• Consider implementing a centralized logging system that can collect, store and analyze log data from multiple sources. • Ensure that logs are generated and stored in a secure and tamper-evident manner.
3	49a2b13	Policies and procedures are not in place for log generation, storage, and management.	• Develop a policy to govern log collection, storage, and management
4	276fe50	Platforms are not configured or only in part to allow the installation of organization-approved software only.	Configure platforms to allow only organization-approved software to be installed. • Consider implementing a software whitelisting system to ensure that only approved software is installed. • Develop a policy to govern software installation and management. • Develop and implement a process for reviewing and approving software before it is installed on platforms. • Ensure that all platforms are configured to prevent the installation of unauthorized software.
5	5e42273	Policies are not in place to ensure secure software development practices throughout the software development life cycle (SDLC).	Develop and implement policies to ensure secure software development practices throughout the software development life cycle (SDLC). • Consider implementing a secure software development framework, such as OWASP, to guide software development practices. • Ensure that software developers are trained on secure coding

			practices and secure software development methodologies. • Develop a process for reviewing and testing software code for security vulnerabilities. • Develop a policy to govern secure software development practices.

PR.IR: Technology Infrastructure Resilience

Purpose

The purpose of "PR.IR: Technology Infrastructure Resilience" is to ensure that the organization's technology infrastructure is resilient and can withstand disruptions, failures, and other types of adverse events.

Description

This Category involves the implementation of security controls and procedures to ensure that the organization's technology infrastructure, including networks, systems, and applications, is designed and operated to be resilient and fault tolerant. This includes the use of technologies and techniques such as network protection, protection of technology assets from environmental threats, redundancy and capacity management.

Strengths

- Organization networks and cloud-based platforms are logically segmented according to trust boundaries and platform types (e.g., IT, IoT, OT, mobile, guests), and permit required communications only between segments.
- Protection from environmental threats and provisions for adequate operating infrastructure are included in requirements for service providers that operate systems on the organization's behalf.
- High-availability components like redundant storage and power supplies are mostly used to improve system reliability.
- Single points of failure are usually avoided in systems and infrastructure.
- Future needs are forecast, and resources are scaled accordingly.

Most Relevant Issues

#	Question id	Issue	Remediation

1	cf9b112	The cyber health of endpoints is not checked or only in part before allowing them to access and use production resources.	Check endpoints cybersecurity health. • Use tools such as endpoint detection and response (EDR) software or vulnerability scanning software to assess the cybersecurity health of endpoints. • Consider implementing a Network Access Control (NAC) system to control and manage access to production resources based on the cybersecurity health of endpoints. • Ensure that all endpoints are up to date with the latest security patches and software updates. • Implement a policy to require endpoints to meet certain security standards before allowing them to access production resources. • Implement a process to check the cybersecurity health of endpoints before allowing them to access and use production resources.

Other Issues

#	Question id	Issue	Remediation
1	0cf54df	Not all single points of failure are avoided in systems and infrastructure.	Identify and mitigate all single points of failure in critical systems and infrastructure that have not been already managed.

2	16399e8	Policies and procedures are not in place to protect technology assets from environmental threats.	Develop policies and procedures to protect technology assets from environmental threats.
3	bf46712	Policies are not in place or only in part to control and manage logical access to networks and environments.	Develop policies to control and manage logical access to networks and environments

Detect (DE)

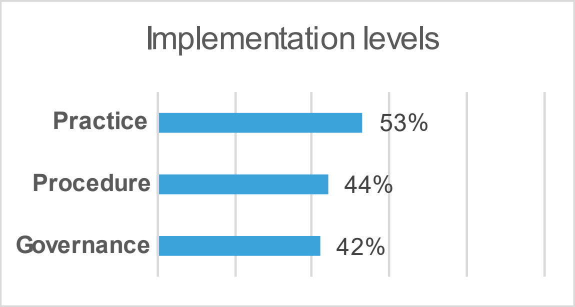
Purpose

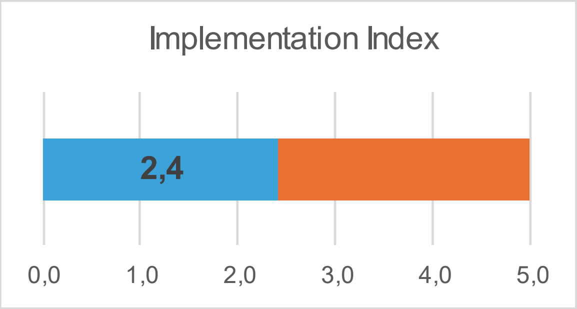
The goal of the DETECT Function in the NIST Cybersecurity Framework (CSF) 2.0 is to promptly detect unusual behaviors, signs of intrusion, and harmful events so that effective measures can be initiated against ongoing cybersecurity issues.

Description

The "DETECT" Function focuses on identifying and analyzing possible cybersecurity attacks and compromises. It enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. It also supports successful incident response and recovery activities.

Implementation Levels





Categories

DE.CM: Continuous Monitoring

Purpose

The purpose of the "DE.CM: Continuous Monitoring" Category is to ensure that an organization's assets, including networks, personnel activity, technology usage, computing hardware and software, and even external service provider activities, are consistently observed to identify potential cybersecurity issues early. By implementing robust continuous monitoring mechanisms, organizations aim to promptly detect and react to anomalous behavior or signs of compromise before significant damage occurs.

Description

The "DE.CM" Category focuses specifically on establishing measures to continually observe various elements within an organization's technological and operational domains. According to the NIST CSF 2.0, continuous monitoring encompasses several crucial areas:

- *Networks and Services*: Ensuring constant surveillance of network traffic and connected devices to spot unusual patterns or suspicious behaviors.

- *Physical Environment*: Keeping tabs on the physical surroundings where IT assets are located to guard against tampering or intrusion attempts.

- *Personnel Activity & Tech Usage*: Tracking employee conduct and tech tool interaction to flag deviant actions that might signal insider threats or misuse.

- *External Service Activities*: Observing the workings of vendors and third-party solutions to catch vulnerabilities introduced via partnerships or supply chains.

- *Computing Environments*: Scanning hardware, software, and runtimes to pinpoint weaknesses or malicious code that could jeopardize sensitive data.

Strengths

- The physical environment is monitored using alarm systems, cameras, and security guards.
- Email, web, file sharing, collaboration services, and other common attack vectors are monitored to detect malware, phishing, data leaks and exfiltration, and other adverse events.
- Hardware and software are monitored for signs of tampering.

Most Relevant Issues

#	Question id	Issue	Remediation
1	c9985f9	Remote and onsite administration and maintenance activities performed by external providers are not monitored or only in part by some Partners.	Enforce stringent logging and oversight for remote administrative and third-party sessions. Employ multi-factor authentication (MFA) at least for admin and remote access accounts and record session details extensively. Review logs weekly for abnormal behaviors.

2	aad6eed	Service level agreements (SLAs) with external service providers do not include monitoring and response to potentially adverse events.	Update SLAs to explicitly require proactive monitoring and rapid response times from vendors. Consider engaging in periodic reviews and drills to validate readiness.
3	47eb1c8	Authentication attempts are not monitored or only in part to identify attacks against credentials and unauthorized credential reuse.	Configure the SIEM to detect and notify sequences of authentication attempts.
4	1a646ca	Software configurations are usually not monitored or only in part for deviations from security baselines.	Automate software configuration checks via scripts running daily comparisons against gold images. Any discrepancy should trigger instant notification to administrator groups for resolution. Keep meticulous change logs accessible for historical referencing.

Other Issues

#	Question id	Issue	Remediation
1	1fca69a	Logs from logical access control systems are usually not monitored or only in part to find unusual access patterns and failed access attempts.	Set up log aggregation and correlation engines like SIEMs (Security Information & Event Management). Automatically flag suspicious login failures, repeated invalid password entries, and unexpected geographical locations attempting access.
2	ea53f1b	Facilities are not monitored or only in part for unauthorized or rogue wireless networks.	Implement regular audits and deploy automated solutions to scan for unauthorized or rogue wireless networks. Ensure thorough inventory tracking and real-time monitoring of all connected devices and networks.

3	851eb4a	Wired and wireless networks are sometimes not monitored for connections from unauthorized endpoints.	Utilize intrusion detection systems (IDS), firewall logs, and endpoint monitoring tools to keep tabs on all incoming and outgoing traffic. Regularly review and audit connection histories to spot inconsistencies.
4	27ce082	Physical environment monitoring is not integrated or only in part with cybersecurity monitoring to provide a comprehensive security posture.	Integrate surveillance cameras, motion sensors, biometric readers, and alarm systems with IT security measures. Deploy centralized dashboards capable of correlating alerts from disparate systems to offer holistic situational awareness.
5	7d6283e	Policies and procedures are not in place to monitor networks and network services for potentially adverse events.	Create detailed policies and procedures for cybersecurity monitoring. Update existing policies periodically to adapt to evolving threats.

DE.AE: Adverse Event Analysis

Purpose

The "DE.AE: Adverse Event Analysis" Category serves the critical function of scrutinizing suspicious activities thoroughly so that organizations can swiftly recognize genuine cybersecurity issues.

Description

The role of this Category involves analyzing observed abnormal behaviors, signs of intrusion, and other possibly harmful events to fully comprehend their characteristics and confirm actual cybersecurity incidents. Through meticulous examination, this category ensures accurate event classification and facilitates prompt reaction measures against impending dangers.

Strengths

- Estimates of impact and scope of adverse events are created, at least manually.
- Vulnerability disclosures for the organization's technologies are rapidly acquired and analyzed, and known false positives are considered when applying incident criteria.

Most Relevant Issues

#	Question id	Issue	Remediation
1	cf99f61	Security Information and Event Management (SIEM) or other tools are not used to continuously centralize, protect, monitor and correlate log events from multiple sources for known malicious and suspicious activity, and to estimate the impact and scope of security incidents.	Deploy a SIEM solution capable of collecting, aggregating, and scrutinizing large volumes of real-time data from varied origins.
2	9889ad6	Cybersecurity software is mostly not used to generate alerts and provide them to the security operations center (SOC), incident responders, and incident response tools.	Use an external security operations center (SOC) leveraging skilled personnel and cutting-edge applications adept at recognizing emerging hazardous signatures and rapidly conveying detailed advisory messages to respective channels, facilitating quick countermeasures.

Respond (RS)

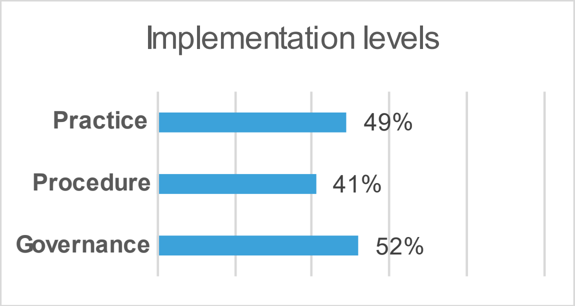
Purpose

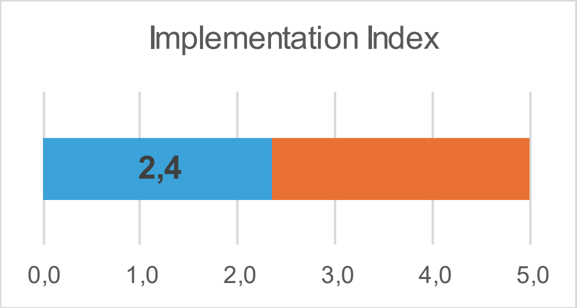
The main objective of the “Respond” Function is to enhance an organization’s capability to react effectively to cyber threats.

Description

This Function focuses on taking necessary actions concerning a detected cybersecurity incident. This involves containing the effects of cybersecurity incidents, performing thorough analyses, implementing mitigation strategies, generating reports, maintaining effective communications, and ensuring proper recording and preservation of critical details throughout the incident lifecycle.

Implementation Levels





Categories

RS.MA: Incident Management

Purpose

The purpose of the “RS.MA: Incident Management” Category is to outline the necessary measures for handling and controlling detected cybersecurity incidents efficiently. By implementing structured protocols and best practices, organizations aim to minimize damage, restore functionality swiftly, and safeguard sensitive information against further intrusions.

Description

Incident Management encompasses several crucial elements aimed at preparing for, identifying, containing, investigating, remediating, and recovering from cybersecurity incidents. Effective incident management ensures that predefined response plans are activated promptly after an attack is discovered.

Moreover, detailed logging and validation of every step undertaken during the resolution phase guarantee transparency and traceability, facilitating future improvements and compliance checks.

Most Relevant Issues

#	Question id	Issue	Remediation
1	2b96f8e	An incident response plan including a comprehensive set of incident management protocols and best practices is not in place. • Criteria are not applied or only in part to estimate the severity of an incident.	Define an incident response plan including the execution of predefined measures upon detection of an incident, proper validation and triage of incident reports, categorization and prioritization of incidents, communications with internal and external stakeholders, necessary escalation mechanisms, and clear criteria for initiating recovery processes Define and implement incident management playbooks starting with the most likely and impactful types of cybersecurity incidents.
2	a4a14dc	• Incidents are not prioritized, or only in part, based on their scope, likely impact, and time-critical nature.	
3	2dfbbf5	• The status of all ongoing incidents is not tracked and validated or only in part.	
4	f51dd1e	• Procedures are not in place for escalating incidents.	

RS.AN: Incident Analysis

Purpose

The purpose of the RS.AN category is to conduct investigations to ensure effective response and support forensic and recovery activities. By performing thorough analyses, organizations aim to determine the details surrounding a cybersecurity incident and ascertain its causes.

Description

Incident Analysis involves several crucial tasks aimed at gathering accurate and reliable insights into ongoing cybersecurity issues. Specifically, this entails examining what took place during an incident, identifying the underlying reasons behind it, recording analytical findings meticulously, collecting necessary data, preserving evidence integrity, estimating the scale of damage caused, and maintaining transparent communications with concerned entities. Through systematic examination, Incident Analysis ensures that lessons learned contribute effectively towards strengthening defenses against similar future threats.

Strengths

- An attempt is usually made to determine what vulnerabilities, threats, and threat actors were directly or indirectly involved in the incident, its severity, what happened and its root causes.

Other Issues

#	Question id	Issue	Remediation
1	08d0154	Policies and processes are not in place to analyze security incidents.	Develop a comprehensive incident analysis policy that includes procedures for analyzing incidents.

RS.CO: Incident Response Reporting and Communication

Purpose

The purpose of the "RS.CO - Incident Response Reporting and Communication" Category is to coordinate response activities with internal and external stakeholders according to laws, regulations, or policies. Effective communication ensures that everyone involved understands the nature of the incident and the necessary next steps.

Description

This category focuses on maintaining open channels of communication to notify relevant parties promptly about ongoing incidents. By keeping stakeholders informed, organizations facilitate quick decision-making and efficient resolution strategies. Clear communication protocols minimize confusion and expedite remediation efforts.

Strengths

- Law enforcement agencies and regulatory bodies are mostly notified of incidents based on criteria in the incident response plan and management approval.
- HR is usually notified when malicious insider activity occurs.

Other Issues

#	Question id	Issue	Remediation

1	a71f88c	A comprehensive incident response communication policy to communicate a confirmed cybersecurity incident to all internal and external stakeholders (e.g., customers, business partners, law enforcement agencies, regulatory bodies) as required by laws, regulations, contracts, or policies is mostly not in place. • The rules and protocols defined in contracts are mostly not followed or only in part for incident information sharing between the organization and its suppliers.	Develop a comprehensive communication policy that includes procedures for communicating with stakeholders during a security incident.
2	9d4bb1a	• Information about an attacker's observed TTPs, with all sensitive data removed, is mostly not voluntarily shared with an Information Sharing and Analysis Center (ISAC).	

RS.MI: Incident Mitigation

Purpose

The purpose of the "RS.MI - Incident Mitigation" Category is to outline necessary measures aimed at containing and minimizing the spread and damage caused by cybersecurity incidents. Its goal is to limit further exposure and minimize the detrimental consequences resulting from such incidents.

Description

This category focuses on two tasks: containing and eradicating incidents. Containing refers to isolating affected areas to stop the problem from spreading further, whereas eradicating aims to remove the source of the issue entirely. Both elements work cohesively towards reducing the severity and duration of ongoing cybersecurity issues.

Strengths

- Most Partners use a third party (e.g., internet service provider, managed security service provider) to support performing containment actions on their behalf.

Other Issues

#	Question id	Issue	Remediation
1	50c0d99	There is no defined process for incident containment or eradication.	Develop comprehensive incident response policy and procedures for incident containment and eradication.
2	02c0b1c		

Recover (RC)

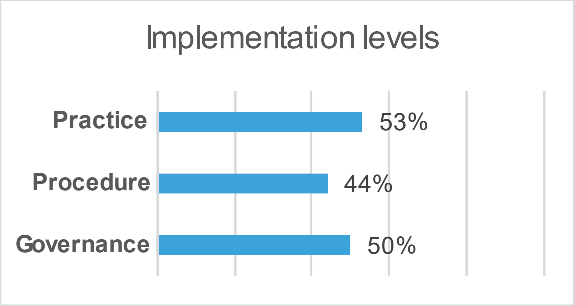
Purpose

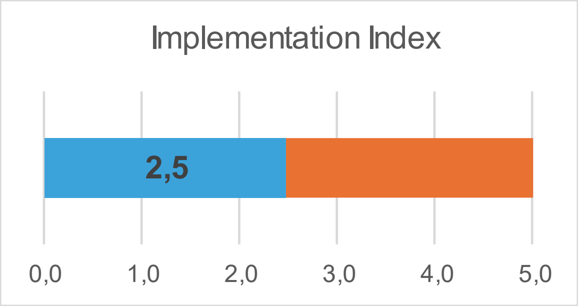
The function "Recover (RC)" in the NIST Cybersecurity Framework (CSF) 2.0 serves two main purposes: first, it aims to restore assets and operations that have been affected by a cybersecurity incident. Second, it ensures that these recoveries are conducted promptly to minimize disruptions caused by such incidents. During recovery efforts, effective communication plays a crucial role in keeping key personnel and stakeholders informed about ongoing developments and the status of recovery measures.

Description

This function focuses on performing necessary restoration tasks according to predefined protocols to guarantee the operability of systems and services impaired by cybersecurity issues. Specific subcategories within this area involve verifying backup integrity, confirming complete functionality upon restoration, and declaring the conclusion of the recovery phase based on specified conditions. Another significant aspect is maintaining open lines of dialogue with both internal teams and external entities concerning the advancement of recovery initiatives and providing public announcements via authorized channels.

Implementation Levels





Categories

RC.RP: Incident Recovery Plan Execution

Purpose

“RC:RP - Incident Recovery Plan Execution” involves restoring assets and operations affected by a cybersecurity incident. Its goal is to execute predefined recovery protocols swiftly and efficiently to minimize downtime and resume regular functioning.

Description

This category outlines several crucial tasks necessary for recovering from a cybersecurity incident. These involve performing restoration activities to bring systems and services back to full functionality, verifying backup integrity, confirming the accuracy of recovered data, establishing post-incident operational norms, and declaring the completion of recovery efforts according to specified criteria. Effective communication with stakeholders throughout the entire recovery phase ensures transparency and alignment.

Strengths

- Incident response practices mostly include a recovery portion.
- System owners are involved to confirm the successful restoration of systems and the return to normal operations.

Most Relevant Issues

#	Question id	Issue	Remediation
1	647b812	A comprehensive recovery plan is not in place. • Incident response plans do not define criteria for prioritizing recovery actions, or recovery actions are not selected based on those criteria.	Prepare incident response plans and define criteria for prioritizing recovery actions to guide the sequence of recovery efforts accurately.
2	2de9d52	A comprehensive recovery plan is not in place. • Business impact analysis (BIA) results are not available or are not used to validate that essential services are restored in the appropriate order.	Perform regularly a BIA. Validate the incident response plans against BIA results to ensure that essential services are restored in the correct order, enhancing efficiency and minimizing disruption.

A comprehensive recovery plan is not in place.

#	Question id	Issue	Remediation
1	caea7b4	Some Partners do not check restoration assets or only in part for indicators of	Thoroughly inspect restoration assets, like backups, for indicators of compromise, file corruption, and other integrity issues

		compromise, file corruption, and other integrity issues before use.	before deployment to avoid reinfection or additional problems.

RC.CO: Incident Recovery Communication

Purpose

The purpose of the 'Incident Recovery Communication' category is to coordinate restoration activities with internal and external entities, providing transparency and alignment during the critical phase of recovering from a cybersecurity incident. Effective communication ensures that everyone understands the ongoing measures and the progress towards full functionality, thereby maintaining trust and minimizing disruptions.

Description

"RC.CO - Incident Recovery Communication" focuses on disseminating accurate and timely information about recovery initiatives undertaken following a cybersecurity incident. This entails updating stakeholders, both inside and outside the organization, on the status of recovery tasks, verifying the success of remediation steps, and confirming the return to standard operations. Clear and structured communication plays a pivotal role in reassuring stakeholders and facilitating smooth transitions back to regular workflows.

Strengths

- Crisis communication is mostly coordinated between the organization and its critical suppliers.

Other Issues

#	Question id	Issue	Remediation
1	3e080e1	The organization's breach notification procedures are mostly not followed or only in part for recovering from a data breach incident.	Document the organization's breach notification procedures comprehensively and ensure all relevant stakeholders are aware of and trained to execute these procedures accurately.
2	728cd6f	A documented communication plan is not in place for reporting recovery activities to stakeholders.	Develop a comprehensive coordination policy that includes procedures for coordinating recovery efforts and communication paths.