Office of the Commissioner of Insurance

Implementation Guide for Cybersecurity Controls for the Insurance Industry

v. 1.0

Drafted to supplement the adoption of Rule No. 108, "*Cybersecurity Standards for the Insurance Industry*"

Table of Contents

Objectives and Scope

The purpose of this document is to provide guidance to any person holding a license or authorization to transact insurance business, issued by the Office of the Commissioner of Insurance of Puerto Rico (OCS), on the best practices for the effective implementation of cybersecurity controls. This document is published to support licensees in complying with Rule No. 108, "Cybersecurity Standards for the Insurance Industry."

Insurance data security is a key factor in developing an industry of excellence, competitiveness, solvency, and global strength focused on protecting public interest and promoting the economic well-being of Puerto Rico. This is the main objective of Rule No. 108, which is based on the NAIC Insurance Data Security Model Law.

Although Rule No. 108 includes exceptions to its applicability, this guide serves as a reference for any insurer, health care organization, agent, general agent, broker, adjuster, rating organization, and advisory service organization. The controls established below are included so that each entity may assess, understand, and identify the appropriate implementation of policies, processes, and safeguards to protect the data stored, processed, controlled, and transferred by such entity, depending on the complexity of its operation. The end result will be effective cybersecurity risk mitigation and a conscious and controlled awareness of cybersecurity risk in your organization.

This guide adheres to the National Institute of Standards and Technology (NIST) Cybersecurity Framework to meet the following main objectives:

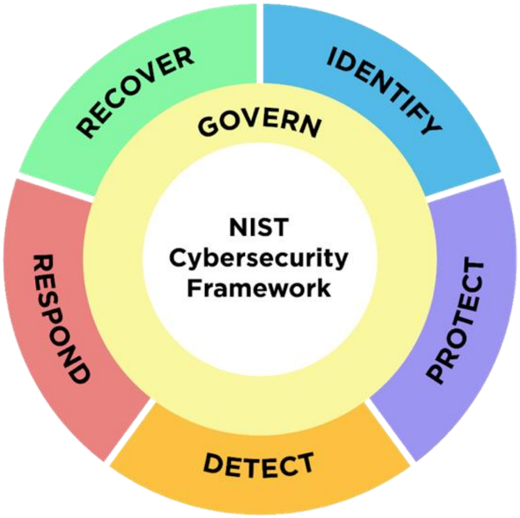
(1) Protect and ensure the confidentiality, integrity, and availability of Insurance industry data;

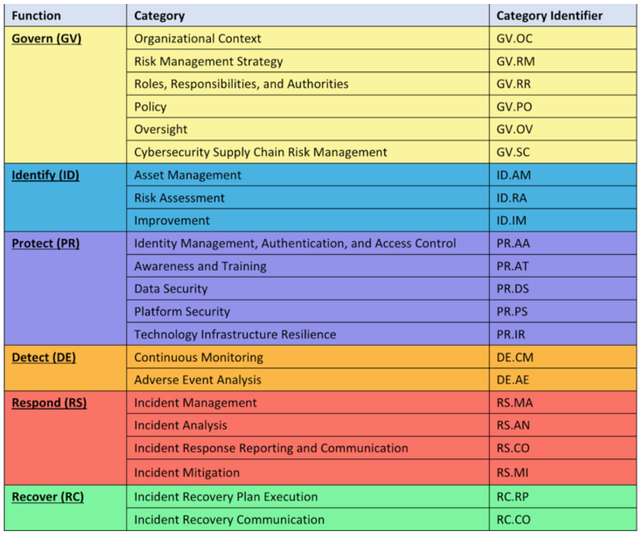
(2) Protect data against unauthorized access or use to prevent harm to the consumer;

(3) Define and periodically reevaluate the data retention period as necessary for operations.

NIST Cybersecurity Framework

NIST provides a cybersecurity framework (CSF) for best practices to mitigate cybersecurity risks to your entity's operations and determine what cybersecurity controls your entity should implement. The NIST Cybersecurity Framework (CSF) 2.0, released in 2024, consists of six functions: govern, identify, protect, detect, respond, and recover.





Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

1. **Govern**: Describes the organizational context, risk management strategy, roles, responsibilities, authority, policies, processes, and oversight.

2. **Identify**: Describes the categories within each function to manage cybersecurity risk as may be required during operations. Includes identification of assets, risk assessment, impact, and improvements.

3. **Protect:** Covers controls and processes to ensure authorized availability, integrity, and access to critical infrastructure and services.

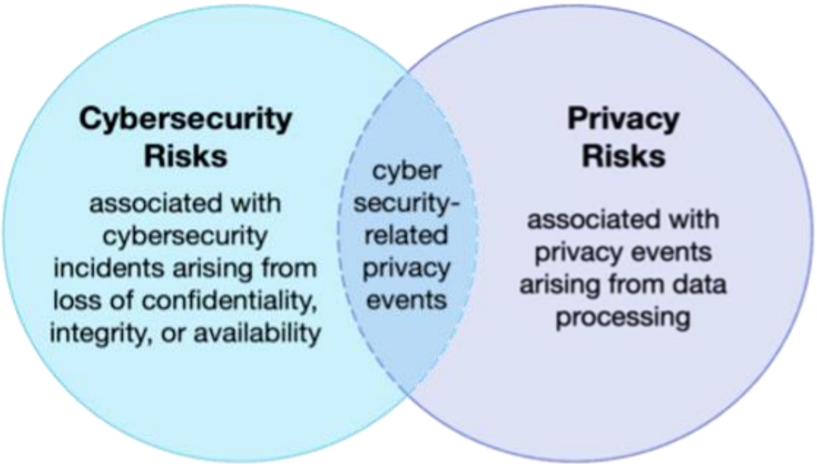
4. **Detect:** Focuses on activities to detect cybersecurity events, either proactively or through alerts and monitoring.

5. **Respond:** Defines the actions that will be taken during a cybersecurity incident, from forensic analyses to communications and mitigation.

6. **Recover:** Restores systems or assets affected by a cybersecurity incident to resume the organization's normal operations.

Relationship between Cybersecurity and Privacy

While cybersecurity and privacy are independent disciplines, their objectives overlap in certain circumstances. A comprehensive cybersecurity program will mitigate privacy risks related to the loss of data confidentiality, integrity, and availability.


Cybersecurity Risks
associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
cyber security-related privacy events
Privacy Risks
associated with privacy events arising from data processing

SOURCE: NIST Cybersecurity Framework (CSF) 2.0

GOVERNANCE Controls

NIST CSF Function
GOVERN

Governance controls are administrative and intended to establish, communicate, and monitor the organization's cybersecurity strategy and policies.

Governance functions for all types of entities:

1. UNDERSTAND

- All stakeholders understand and take into consideration the enterprise's cybersecurity needs and expectations. (GV. OC-02)

- Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed. (GV. OC-03)

Section 8.E of Rule No. 108 requires ***Oversight by the Board of Directors*** *to ensure that the executive management discusses the cybersecurity program and its regular updates.*

Example:
Establish an internal awareness and tracking process of your entity's compliance requirements with the OCS and other regulatory entities, as well as your cybersecurity contractual obligations with suppliers, partners, and customers. If your operation is complex, you will benefit to the extent that these processes are formally documented.

- Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced (GV. RR-02)

Examples:
Document who is responsible and accountable for cybersecurity activities and how those teams and individuals are to be consulted and informed.

Include cybersecurity responsibilities and performance requirements in each job description.

Rule No. 108, Sec. 8.C:
"The Licensee shall conduct a Risk Assessment to:
(1) Designate one or more employees, affiliates, third-party vendors, or Service Contractors designated to act on behalf of the Licensee to be responsible for the Cybersecurity Program"

There are several frameworks and methodologies for assessing cybersecurity risk. Visit the OCS Cybersecurity Portal for more information: https://ciberseguridad.ocs.pr.gov

2. ASSESS

- Critical objectives, capabilities, and services offered by or expected from the organization are effectively understood and communicated. (GV. OC-04)

Examples:
Determine assets and operations that are vital to achieving business objectives. Establish and communicate resilience objectives (e.g., recovery time objectives) for delivering critical services under different conditions (under attack, during recovery, normal operation, etc.).

According to Sec. 8.C of Rule No. 108, the risk assessment shall also:

- ***Identify reasonably foreseeable internal or external threats...***
- ***Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Nonpublic Information;***
- ***Design and assess the sufficiency of the policies, procedures, and safeguards, including:***
  - *(a)* ***Employee training and management;***
  - *(b)* **Information systems, including network and software design, as well as data classification, governance, processing, electronic storage, transmission, and disposition; and**
  - *(c)* **Detecting, preventing, and responding to attacks, intrusions, or other system failures.**
- ***Implement information safeguards to manage threats identified in its ongoing assessment, and at least annually, assess the effectiveness of key controls, systems, and procedures...***

According to best practices...

Assess the risk to your operations

Review the activities and tasks of each division to assess the cybersecurity risk each could pose in order to identify potential threats and damages.

Perform regular vulnerability scans

To identify vulnerabilities in your information systems conducting vulnerability scans at least every three months is recommended. CISA offers these services free of charge.

Understanding your cybersecurity risk will help you create administrative controls:

Implement policies and procedures to be adopted by your staff to protect your equipment, network, user accounts, and company data. Some examples of key policies include:

- ○ *Cybersecurity Policy*
- ○ *Technology Use Policy*
- ○ *Data Management Policy*
- ○ *Asset Management Policy*
- ○ *Cybersecurity Employee Training Policy*
- ○ *Access Control Policy*
- ○ *Incident Response Policy*

Once the administrative controls (policies, standards, and procedures) are created, implement the technical controls accordingly.

The policies show conscious awareness of the identified risk and a statement about the protective measures that the company will use. Each technical tool must be configured according to these policies.

- Planning and due diligence are performed to reduce risks before entering into contracts with service suppliers and third parties. (GV. SC-06)

  Example:

  Thoroughly assess prospective suppliers and third parties, that is commensurate with the level of risk, criticality, and complexity of each supplier or third-party relationship and integrated consistently with the procurement process.

Rule No. 108, Sec. 8.D.2.d:

“(d) Maintain an oversight program for service providers with access to Nonpublic Information, which includes service agreements and requires cybersecurity controls."

Refer to NIST's guidance on how to assess the cybersecurity risk of a prospective provider: https://nist.gov/itl/smallbusinesscyber/guidance-topic/choosing-vendorservice-provider

Rule No. 108, Sec. D.3:
"Include cybersecurity risks in the Licensee's business risk management process and in the reports required in Sections 32.040, and 53.070 of the Insurance Code of Puerto Rico and Rule 104 on Corporate Governance."

3. PRIORITIZE

- Cybersecurity risk assessment activities and outcomes are included in enterprise risk management processes. (GV. RM-03)

  Examples:
  Aggregate cybersecurity matters when discussing and planning compliance, financial, operational, regulatory, and reputational risk management, among other risk.

  Include a cybersecurity manager in enterprise risk planning activities and discussions.

4. COMMUNICATE

- Senior management is responsible and accountable for communicating cybersecurity risks and fosters a culture that is risk-aware, ethical, and continually improving. (GV. RR-01)

  Example:
  Share leaders' expectations regarding a secure and ethical culture, especially when current events present the opportunity to highlight positive or negative examples of cybersecurity risk management.

- The cybersecurity policy is established based on organizational context, cybersecurity strategy, and priorities, and is communicated and enforced effectively. (GV. PO-01)

  Examples:
  Communicate the cybersecurity policy to all personnel across the organization, as well as the supporting standards and processes.
  Require personnel to acknowledge receipt of the cybersecurity policy when first hired, annually, and whenever it is updated.

IDENTIFICATION Controls

NIST CSF Function
IDENTIFY

In order to protect the assets of an organization, such assets must first be identified. By doing so, the appropriate level of protection for each asset can be determined based on its sensitivity and criticality to your business mission.

Identification functions for all types of entities:

1. UNDERSTAND

- Inventories of hardware managed by the organization are maintained. (ID.AM-01)

- Inventories of software, services, and systems managed by the organization are maintained. (ID.AM-02)

- Inventories of the services provided by suppliers are maintained. (ID.AM-04)

  Example:
  Maintain inventory of computers, servers, tablets, and cell phones used by the organization, as well as **third-party online platforms and services** used in your processes.

> Rule No. 108, Sec. 8.D.2.e:
> ***"Identify and manage the information, personnel, devices, systems, and facilities that enable the Licensee to achieve its business purposes in accordance with their relative importance to the business objectives and risk management strategy of the organization."***

> Rule No. 108, Sec. 8.D.2.j:
> ***"Regularly test and monitor systems and procedures to detect actual and attempted attacks on or intrusions into the Information System and the network, as well as document the outcome of these tests."***
>
> *Sec. 8.D.5:*
> ***"Perform regular vulnerability tests on their Information Systems with tools that clearly identify vulnerabilities, as indicated by this Office."***

2. ASSESS

- The effectiveness of the cybersecurity program is assessed, and improvements to processes, procedures, and activities are identified from these evaluations. (ID.IM-01)

  Example:
  Assess your critical services, taking into consideration current threats.

- Vulnerabilities are identified, validated, and recorded across all information assets. (ID.RA-01)

3. PRIORITIZE

- An up-to-date data inventory is maintained, including its corresponding categories, metadata, and classifications. (ID.AM-07)

  Example:
  Maintain a list of nonpublic information so that the where and how said information is stored, processed, and used can be easily identified.

- The cybersecurity risk to the organization, assets, and individuals is understood by the organization. (ID.RA)

> Rule No. 108, Sec. 8.D.2.e:
> ***"Identify and manage the information, personnel, devices, systems, and facilities that enable the Licensee to achieve its business purposes in accordance with their relative importance to the business objectives and risk management strategy of the organization."***

4. COMMUNICATE

- Cybersecurity policies and plans are established, maintained, and improved, and communicated to all personnel and relevant third parties. (ID.IM-04)

  Example:
  Create and adopt an incident response plan, business continuity plan, and disaster recovery plan for responding to and recovering from adverse events that may interfere with operations, expose confidential information, or endanger the organization's mission and viability.

- Communicate to staff the importance of identifying improvements to cybersecurity processes, procedures, and activities. (ID.IM)

NIST CSF Function
PROTECT

PROTECTION Controls

The protect function consists of implementing security controls to prevent or reduce cybersecurity risks.

Protection functions for all types of entities:

1. UNDERSTAND

- Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege (PoLP) and separation of duties. (PR.AA-05)

  Examples:
  Create and adopt a policy to **restrict access and privileges to the minimum necessary** for each employee to perform their duties.

2. ASSESS

- Personnel are provided with cybersecurity awareness and training workshops so that they can perform their cybersecurity-related tasks (PR.AT)
  - Personnel are trained so that they possess the knowledge necessary to perform general tasks with security risks in mind. (PR.AT-01)
  - Individuals in specialized roles are trained so that they possess the knowledge and skills to perform relevant tasks with security risks in mind. (PR.AT-02)

Rule No. 108, Sec. 8.D.2:

"Implement the following security measures, as warranted by the Licensee's infrastructure, staff, operation, and information systems:

a) Maintain a formal training program on cyber risk modalities for the staff and keep track of employee performance in the program.

b) Provide employees with Cybersecurity Program training and assign them responsibilities within the program;

c) Establish effective access controls on Information Systems, including controls to authenticate (such as multi-factor authentication) and allow access only to authorized individuals to protect against the unauthorized acquisition, alteration, disclosure, or destruction of Nonpublic Information"

3. PRIORITIZE

- Users, services, and hardware are authenticated using a password manager to help staff generate and protect strong passwords. (PR.AA-03)

- Default manufacturer credentials are always changed, and all personnel credentials, as well as the identity of users, services, and equipment, are properly managed. (PR.AA-01)

  Examples:
  Process through the IT area requests for any new access or additional access assigned to an employee, contractor, or third party, as needed.
  Issue **different and unique credentials;** no sharing of accounts or passwords between employees.

- The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are updated regularly and perform patching as it becomes available, using automation and reminders whenever possible. (PR.PS-02)

For updated information on new vulnerabilities that have been exploited and verified, go to: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- Backups of data are created and tested regularly. (PR.DS-11)

- Enable full-disk encryption on tablets and other mobile devices to protect the data stored in them. (PR.DS-01)

4. COMMUNICATE

- Communicate to staff how to recognize common attacks, report attacks or suspicious activity, and perform basic cyber hygiene tasks. (PR.AT-01/02)

  Examples:
  Explain the potential impact and consequences of cybersecurity policy violations, both for individual users and for the organization as a whole.
  Periodically assess staff on their understanding of basic cybersecurity practices.

NIST CSF Function
DETECT

DETECTION Controls

The detect function focuses on finding and analyzing possible cyberattacks and threats.

Rule No. 108, Sec. 8.D.2:

f) Restrict physical access to areas where Nonpublic Information is located so that it is only accessible to authorized individuals; […]

j) Regularly test and monitor systems and procedures to detect actual and attempted attacks on or intrusions into the Information System and the network, as well as document the outcome of these tests.

k) Include backup, safekeeping, and management processes ("audit logs") within the Cybersecurity Program designed to detect and respond to Cybersecurity Incidents and to reconstruct material financial transactions in order to provide adequate support to the normal operations and obligations of the Licensee.

Detection functions for all types of entities:

1.UNDERSTAND

- Understand how to identify common indicators of a cybersecurity incident. (DE.CM)

2.ASSESS

- Information systems and external services are regularly assessed to detect deviations from expected or typical behavior. (DE.CM-06/09)

- Physical security is regularly assessed to identify signs of tampering or other suspicious activity. (DE.CM-02)

3.PRIORITIZE

- Update antivirus and antimalware software on all business devices (e.g., servers, computers, and smartphones). (DE.CM-09)

- Engage a service provider to monitor computers and networks for suspicious activity if the entity does not have the ability to do it internally. (DE.CM)

4. COMMUNICATE

- Communicate with a certified incident responder about the relevant details from the incident to help them analyze and mitigate it. (DE.AE-06/07)

RESPONSE Controls

NIST CSF Function
RESPOND

The response function increases your ability to make decisions regarding a detected cybersecurity incident.

Response functions for all types of entities:

1. UNDERSTAND

- Understand your incident response plan and who has authority and responsibility for implementing the various aspects of the plan. (RS.MA-01)

2. ASSESS

- Assess your ability to respond to a cybersecurity incident. (RS.MA-01)
- Assess the incident to determine its severity, what happened, and the attack vector. (RS.AN-03, RS.MA-03)

3. PRIORITIZE

- Prioritize decisions to contain and eradicate the incident to prevent further damage. (RS.MI)

Rule No. 108, Sec.10:
"The Licensee shall notify the Commissioner of a Cybersecurity Incident as promptly as possible, within 72 hours after the time it has been determined that a Cybersecurity Incident has occurred..."
[Read more about how and to whom you should report a cybersecurity incident]

4. COMMUNICATE

- Communicate a confirmed cybersecurity incident with all internal and external stakeholders (e.g., customers, business partners, law enforcement agencies, regulatory bodies) as required by laws, regulations, contracts, or policies. (RS. CO-02/03)

See NIST's guide to responding to a cybersecurity incident (SP 800-61 Rev. 2):
https://csrc.nist.gov/pubs/sp/800/61/r2/final

Rule No. 108, Sec. 8.H.2:
"The incident response plan shall address the following: [...]
(a) The internal process for responding to a Cybersecurity Incident;
(b) The objectives of the incident response plan;
(c) A clear definition of the roles, responsibilities, and levels of decision-making authority, including names of employees and incident response providers;
(d) External and internal communications and the manner in which information is shared."

RECOVERY Controls

NIST CSF Function
RECOVER

The recover function involves restoring assets and operations affected by a cybersecurity incident.

Recovery functions for all types of entities:

1. UNDERSTAND

- Understand who within and outside your business has recovery responsibilities.
- (RC. RP-01)

2. ASSESS

- Assess what happened by preparing an after-action report, on your own or in consultation with a vendor, that documents the incident, the response and recovery actions taken, and lessons learned. (RC. RP-06)

- Assess the integrity of your backed-up data and assets before using them for restoration. (RC. RP-03)

3. PRIORITIZE

- Prioritize your recovery actions based on organizational needs, resources, and assets impacted. (RC. RP-02).

Rule No. 108, Sec. 8.H.2:
"The incident response plan shall address the following: [...]
e) Identification of requirements for the remediation of any identified weaknesses in the Information Systems and associated controls;
f) Documentation and preparation of reports regarding Cybersecurity Incidents and related response activities; and
g) The evaluation and revision of the incident response plan, as necessary after a Cybersecurity Incident."

4. COMMUNICATE

- Communicate regularly and securely with internal and external stakeholders. (RC.CO)
- Communicate and document the incident and its remediation before resumption of normal activities. (RC. RP-06)

To create recovery plans, you can use the resources available at:
https://www.ready.gov/business/emergency-plans/recovery-plan

Revision History

Version	Date	Revisions	Approved by

Implementation Guide for Cybersecurity Controls for the Insurance Industry

Version:	1.0
Published:	September 25, 2024
Approved by:	Alexander S. Adams-Vega, Esq., Commissioner of Insurance
Contact:	ciberseguridad@ocs.pr.gov