TLP:CLEAR

IMC_01 – Methodology for Assessing Cyberresilience Improvement Indicators (CII)

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

February 2023

IMC_01 – Methodology for assessing version 1.9

INDEX

FIGURES INDEX

TABLE INDEX

1. GOAL AND SCOPE OF THE DOCUMENT

1.1. Goal

The objective of this Methodology for Assessing Cyberresilience Improvement Indicators (CII) at Industrial Control Systems and ICT systems is to assist all stakeholders in the enhancement of their cyberresilience capabilities, and to provide a procedure to understand the maturity level of their controls to anticipate, resist, recover and evolve after suffering adverse conditions, stress or attacks against the organizational cyberresources.

1.2. Scope

The methodology presented in this document is designed to evaluate the cyberresilience of organizations related to their Industrial Control Systems (ICS) and ICT systems.

In this document, the definition of the Industrial Control System (ICS) has been adopted according to the *International Society of Automation (ISA)*, which means a broad set of components and systems, including, among others:

- Supervisory Control and Data Acquisition (*SCADA Systems*). They are used in cases of wide geographic dispersion, when centralized supervision and control are needed.
- Distributed Control Systems (*DCS*). It is an architecture composed of subsystems in charge of controlling localized processes.
- Programmable Logic Controllers (*PLC*). Computer devices equipped with non-volatile memory used to control equipment and processes.
- Safety Instrumented Systems (*SIS*). Hardware and software controls used in dangerous processes to prevent or mitigate negative consequences.

This model is intended for use in the form of consultations that can be launched among organizations in any essential sector, and as a self-assessment tool of cyberresilience for these organizations.

1.3. Stakeholders

Stakeholders in the cyberresilience of an organization can be any individual, group or organization that is part of or is affected by it, obtaining some benefit or harm, and each of them has their own interests. The model presented seeks to respond to the different needs of each one of them as set out below, considering both the most relevant internal and external stakeholders (Table 1).

Stakeholders	Needs	Function of the model
Internal		
Governance and management	Know the cyberresilience level of the ICS	Cyberresilience continuous improvement
Operations	Improve the cyberresilience level in ICS	Cyberresilience continuous improvement

Risk / Security managers	A model for measuring the cyberresilience level of ICS	Cyberresilience continuous improvement
External		
Shareholders	Know the cyberresilience level of ICS	Information about cyberresilience
Partners	Improve the business continuity through the partners or associates cyberresilience	Information about partners' or associates' cyberresilience capabilities

Table 1: Stakeholder Needs and Model Utility

2. MODEL FOR ASSESSING CYBERRESILIENCE IMPROVEMENT INDICATORS (CII)

2.1. Definition of cyberresilience

Cyberresilience is the ability of a process, business, organization or nation to anticipate, resist, recover, and evolve to improve its capabilities, when faced with adverse conditions, stress or attacks against the cyberresources it needs to operate properly.

2.2. Conceptual framework

For the construction of the CII model, a framework is proposed. This framework articulates the metrics and indicators (that will be defined later) that allow the state of cyberresilience to be measured. The aim is to provide a vision, as complete as possible, based on these metrics.

This framework is mainly based on the cyberresilience indicators proposed by MITRE [1], and also adopted by INCIBE-CERT in its initiative for the construction of a comprehensive framework of indicators [2], in accordance with the National Cybersecurity Strategy [3-4] of the Government of Spain.

Following a GQM (Goal-Question-Metric) approach, a set of high-level goals are set, subsequently, a series of general and specific objectives are stablished, and finally, the necessary questions are defined in order to achieve these objectives. This approach allows starting from the highest (strategic) level and developing new metrics from them, without losing sight of the operational objectives of the organizations for the maintenance of their essential services.

In this way, three conceptual levels are established.

At a **first layer** is the concept of governance, associated with meeting high-level goals. In it we can find goals that will establish the bases of the rest of the levels.

- ***General objectives or goals*:** specific statements of expected results expressed in order to facilitate its assessment.

The **second layer** is made up of a series of functional groups or domains, each of which is associated with achieving a general cyberresilience objective.

- ***Functional domains*:** areas in which main cyberresilience organizational aspects can be grouped, containing the set of practices that the organization must implement to ensure the protection and maintenance of an essential service.

The **lowest** and "tangible" **layer** of the framework is made up by cyberresilience metrics, each of which is associated with the measurement of a more specific objective:

- ***Specific objectives*:** ways to achieve one or more general cyberresilience goals. Those objectives apply to the architecture or design of an essential service and the resources that support them.
- ***Cyberresilience metric*:** variable to which a value is assigned as a result of measuring an organizational cyberresilience aspect.

Associated with these three layers, cyberresilience indicators can be defined.

- **Cyberresilience Indicators:** graphical representations of cyberresilience metric data that allows statistical comparisons. It could show goal current status, and its progress over time, to enable decision making.

2.3. CII assessment model

Based on the above conceptual framework, a model to assess the cyberresilience level of an essential service has been designed. This conceptual framework consists on the following elements:

- Four goals:
  - **Anticipate (A):** To maintain an informed readiness state in order to avoid compromising an essential service by cyberattacks.
  - **Resist (T):** To continue the essential services despite the successful execution of the cyberattack.
  - **Recover (R):** To restore the essential services to the greatest extent possible after the successful execution of a cyberattack.
  - **Evolve (E):** To change functions and capabilities, aiming a strategy redesign, in order to minimize the negative impacts of real or future cyberattacks.
- Nine functional domains, grouped by goal:
  - **Cybersecurity policy (CP):** Having a policy that establishes cyberresilience requirements, addresses cybersecurity risks, assigns responsibilities, and is communicated throughout the organization.
  - **Risk management (RM)**: Identifying, analyzing and mitigating risks that impact the organizational assets, and that could adversely disturb in the operation and delivery of services.
  - **Cybersecurity training (CT)**: Promoting the development of individual knowledge and skills, that supporting their tasks, allows the achievement and maintenance of operational protection and cyberresilience.
  - **Vulnerability management (VM)**: Identifying, analyzing and managing vulnerabilities on the assets that support the delivery of the essential service.
  - **Continuous supervision (CS)**: Collecting, compiling and distributing information about the behaviour and activities of systems and individuals, to support the ongoing process of identifying and analyzing risks of the organizational assets that impact the essential services and may adversely disturb its operation and delivery.
  - **Incident management (IM)**: Establishing processes for identifying, analyzing events, detecting incidents, determining and implementing an appropriate organizational response.
  - **Service continuity management (SCM):** Determining how the organization performs planning activities to ensure continuity of essential services in the event of an incident or disaster.

- **Configuration and change management (CCM):** Establishing processes to maintain the integrity of all assets (technology, information and facilities) needed to provide essential services.
- **Communication (CM)**: Establishing processes that guarantee communications between those, both internal and external to the organization, involved in the operation of essential services.

The grouping of domains within the goals can be seen in Figure 1:

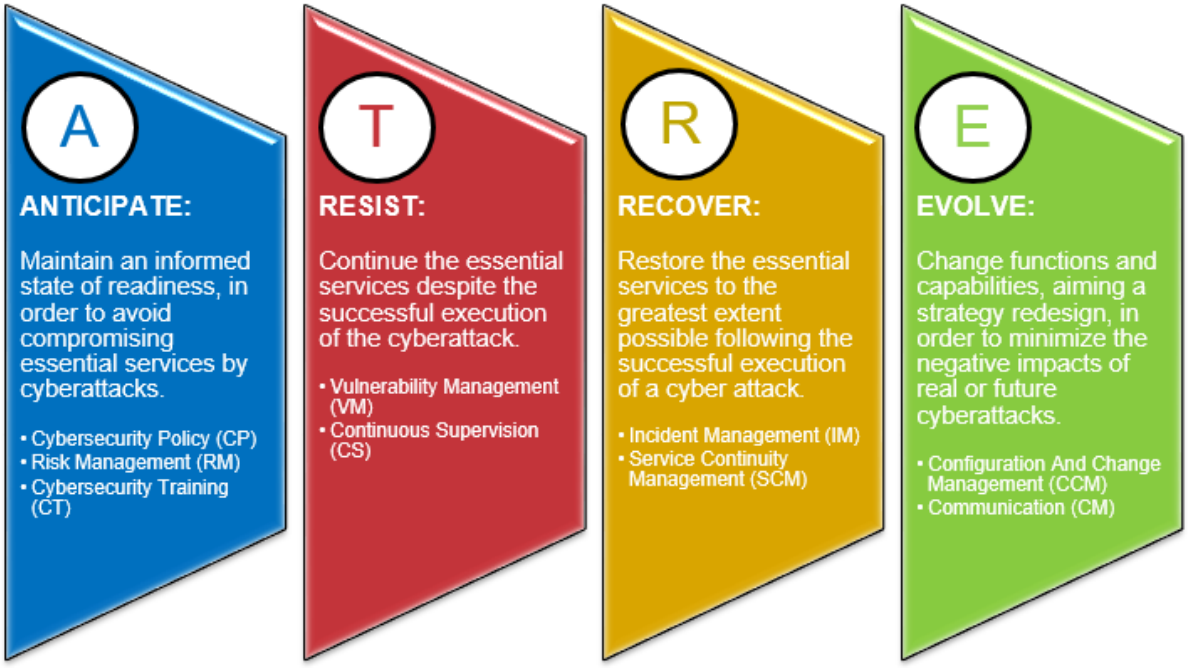

Figure 1: Cyberresilience Framework

To follow with this framework, there have been defined:

- A set of cyberresilience metrics grouped by functional domain.
- A set of cyberresilience indicators based mainly on Key Performance Indicators (KPIs) and on the eventual definition of Key Risk Indicators (KRIs).
- This model of goals, domains, metrics and indicators that will be used for the cyberresilience assessment, make up the Model for Assessing Cyberresilience Improvement Indicators (CII).

2.4. Documents in the model

The Model for assessing Cyberresilience Improvement Indicators (CII) consists of the following documents:

CII Model Documentation	
IMC_01 – Methodology for Assessing Cyberresilience Improvement Indicators	Document containing the conceptual framework and methodology for performing the assessment of Cyberresilience Improvement Indicators.
IMC_02 - Dictionary of Cyberresilience Improvement Indicators	Document summarizing each of the metrics used in the assessment of the Cyberresilience Improvement Indicators.
IMC_ 03 – Question Form for Cyberresilience Measurement	Template document for the assessment of Cyberresilience Improvement Indicators.

Table 2: CII's Assessment Model Documentary Kit

2.5. CII assessment methodology

The Methodology for Assessing Cyberresilience Improvement Indicators that must be applied by each participating company or organization is developed in the following stages:

- Outline the scope of the analysis.
- Perform self-assessment test or questionnaire.
- Implement a series of corrective measures within the scope.
- Repeat the consultation to analyze the effectiveness of the measures.

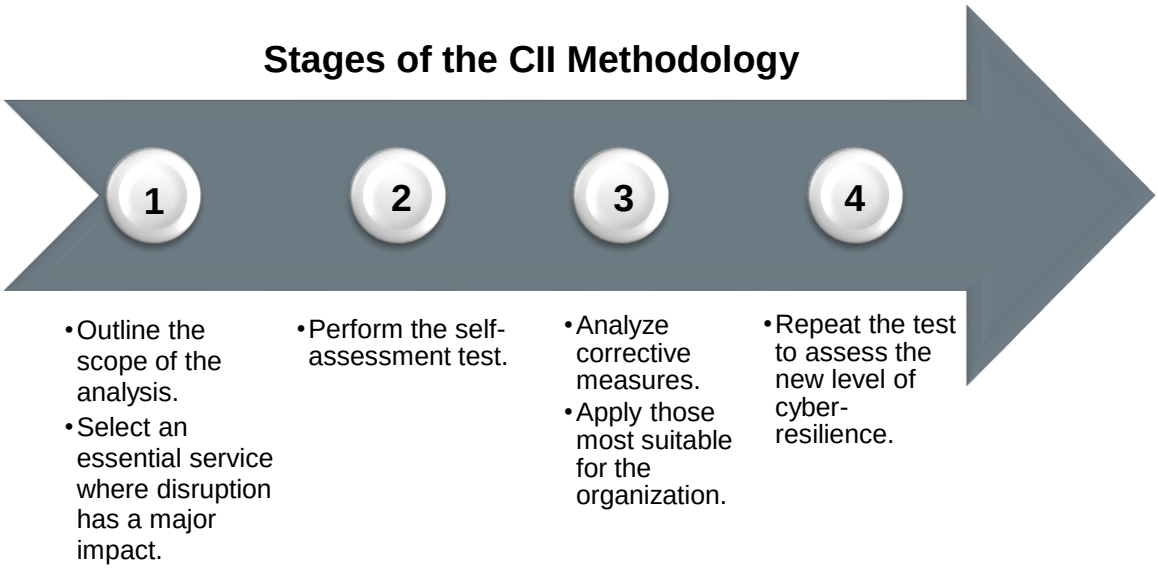

Figure 2: General Approach to the CII Assessment Methodology

The application of corrective measures to be carried out by the organization, which cyberresilience is under study, is outside the scope of this model.

3. METHODOLOGICAL APPLICATION OF THE MODEL

In order to facilitate the implementation of the model, the stages proposed for this model are described below:

3.1. Stage 1: Scope outline

The first step for applying the Model for Assessing Cyberresilience Improvement Indicators is to determine the essential service to be evaluated. Within this context, the **scope** is defined with respect to the specific provision of an **essential service whose interruption presumably has a great impact on the organization** (or in the case of critical infrastructures, on Spanish society). Therefore, each organization that would like to go through this model must determine the scope of its own questionnaire.

As a general guideline, the questionnaire should be completed with respect to the specific provision of at least one essential service whose interruption would presumably have a significant impact. The questionnaire may be completed for more than one essential service, thus obtaining a cyberresilience value for each of the services considered essential by the respondent.

Conducting a comprehensive analysis that includes several services will enable stakeholders locate synergies that allow an overall improvement in the cyberresilience of the organization.

3.2. Stage 2: Performing self-assessment

Once the essential service object of the analysis has been identified, the self-evaluation questionnaire should be completed by assessing the selected metrics according to their own degree of maturity.

The form presents a section for each goal: Anticipate, Resist, Recover and Evolve. For each section, the company must insert the measure taken for the different metrics. Each of these metrics could be implemented in the company with a level of maturity that must be chosen. The maturity levels are adapted for each metric, and must correspond to one of the offered by the tool, as shown in the example in Figure 3:

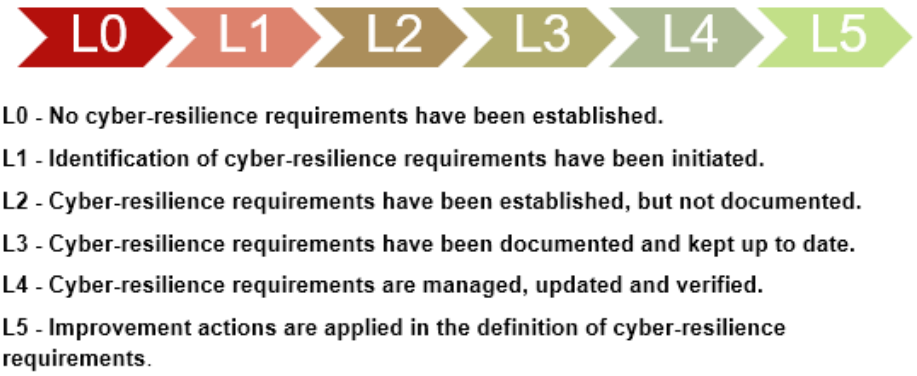

Figure 3: CII Maturity Levels

Once the maturity level corresponding to each of the metrics has been selected, it will be possible to calculate, assigning a value to each level and adding the results of all the metrics

of each goal, the result obtained for each of them. The example (Figure 4) shows how these results could be represented as a bar diagram.

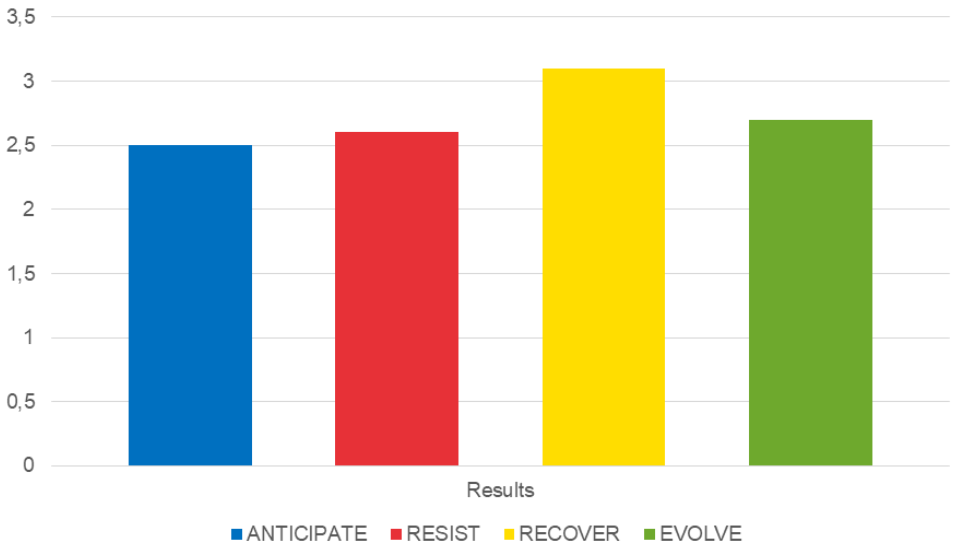

Figure 4: CII Consultation Example Result

Optionally, for any other essential services identified in the previous point, another consultation can be made, thus obtaining the cyberresilience value of each essential service identified whose deterioration or failure causes a great impact.

3.3. Stage 3: Implementation of corrective measures

Once self-assessment consultation has been carried out, the company should implement the corrective measures. In the document IMC_02 - Dictionary of Cyberresilience Improvement Indicators, corrective actions can be looked up for metrics whose evaluation has not been sufficiently satisfactory, as it is shown in the following example, corresponding to one of the metrics of the Resist goal:

ANALYSIS		
Objective Measure	L5	
Indicator	**Positive Values**	Values tending to L5 indicate that the organization maintains an updated repository of all known vulnerabilities, storing information on them and their resolution.
	Corrective Measures	Establish a vulnerability repository with vulnerability lifecycle information. Such repository should contain basic information such as: • Unique identifier for internal reference of the vulnerability in the organization. • Description of the vulnerability. • Date of entry into the repository. • References to the source of the vulnerability. • Importance of the vulnerability for the organization (critical, moderate, etc.). • Persons or teams assigned to analyze and resolve it. • Record of resolution actions taken to reduce or eliminate the vulnerability.

Figure 5: Corrective Actions Example

The study of the suitability of applying the proposed corrective measures or others more appropriate for the organization participating in a consultation, as well as the process of their implementation, are outside the scope of this model.

3.4. Stage 4: Repeat the consultation periodically

The assessment of cyberresilience is a process that allows stakeholders to know their ability to anticipate, resist, recover and evolve from cybersecurity incidents. It is important to carry out these analyses on a regular basis to assess the effectiveness of the corrective measures taken, and thus try to enhance those aspects that need improvement, thereby increasing the cyberresilience of those services deemed essential.

4. ACRONYMS

- INCIBE-CERT: reference Security Incident Response Center for citizens and private law entities in Spain, operated by INCIBE.
- CNPIC: Centro Nacional de Protección de Infraestructuras Críticas.
- GQM: Goal-Question-Metric.
- CII: Cyberresilience Improvement Indicators.
- INCIBE: Instituto Nacional de Ciberseguridad.
- KPI: Key Performance Indicator.
- KRI: Key Risk Indicator.
- ISA: International Society for Automation.
- ICS: Industrial Control Systems.
- ICT: Information and Communication Technologies.

5. REFERENCES

Reference	Title, author and link
[Ref.- 1]	MITRE (2018), Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring. https://www.mitre.org/news-insights/publication/cyber-resiliency-metrics-measures-effectiveness-and-scoring
[Ref.- 2]	INCIBE_CERT (2014), CIBER-RESILIENCIA: Aproximación a un marco de medición. https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/int_ciber_resiliencia_marco_medicion.pdf
[Ref.- 3]	España (2019), ESTRATEGIA NACIONAL DE CIBERSEGURIDAD. https://www.boe.es/buscar/act.php?id=BOE-A-2019-6347
[Ref.- 4]	España (2021), ESTRATEGIA DE SEGURIDAD NACIONAL. https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021
[Ref.- 5]	NIST (2022). SP 800-53A, Assesing Security and Privacy Controls in Information Systems and Organizations. https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final

Other documents of interest	Title, author and link
[Doc.- 1]	MITRE (2023). MITRE Launches Cyber Resiliency Engineering Framework Navigator. https://www.mitre.org/news-insights/news-release/mitre-launches-cyber-resiliency-engineering-framework-navigator
[Doc.- 2]	MITRE. (s.f). Navigator. https://crefnavigator.mitre.org/navigator
[Doc.- 3]	NIST (2021). SP 800-160 Vol. 2 Rev. 1. Developing Cyber-Resilient System: A System Security Engineering Approach. https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final