GOBIERNO DE ESPAÑA MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

TLP:WHITE

National Scheme on Industrial Security

ENSI_C4V_01 Value Chain Cyber Security (C4V) Capability Building Model

certsi_

CERT DE SEGURIDAD E INDUSTRIA

CONTENTS

GRAPHICS

TABLES

APRIL 2017

1. PURPOSE AND SCOPE OF THIS DOCUMENT

1.1. Purpose

The purpose of the present model for building cyber security capabilities for industrial control systems is to help all parties interested in protecting their security to have a method that allows them to be aware of the degree of maturity and robustness of controls and protection measures implemented on such systems, paying special attention to dependence of essential services and to risk management in the ICT supply chain.

1.2. Scope

The model for cyber security capacity building presented in this document is specially designed for industrial control systems.

This document has adopted the Industrial Control System definition of the International Society of Automation (ISA), which defines ICSs as a wide-ranging group of components and systems which includes, without limitation:

- SCADA (Supervisory Control And Data Acquisition) systems. Used in case of wide geographical dispersion, when centralised monitoring and control are needed.
- Distributed Control Systems (DCS). An architecture composed by subsystems for controlling localised processes.
- Programmable Logic Controllers (PLC). Computer devices provided with non-volatile memory used to control devices and processes.
- Safety Instrumented Systems (SIS). Hardware and software controls used in hazardous processes in order to prevent or mitigate negative consequences.

Although there are equivalent models for general purpose information technologies, the specific characteristics of these systems support the need of a specific model, in particular the following:

- Focus on security and availability
- Specific and proprietary technologies
- Equipment life cycle

In case that the capacity level is affected by third party service providers, the organization in charge of the service must establish mechanisms to ensure that such third parties comply with the necessary requirements for the corresponding level of capability defined in the present document, and have monitoring procedures available to ensure that such level is maintained throughout the service life cycle.

This present model is not intended for third parties that are an integral part of the value chain, unless they are themselves responsible for providing a fundamental service.

1.3. Stakeholders

Within an organization, stakeholders are any individual, group or organization belonging to or affected by it, understood as being benefited or damaged, and which holds their own interests. The model presented in the document intends to provide an answer to the

different needs of each of them, pursuant to the following table, and considering both internal stakeholders and external most relevant stakeholders (**table 1**)

Stakeholders	Need	Model purpose
	Internal	
Governing and management bodies	Being aware of ICS protection capability level	Ongoing improvement of ICS cyber security capabilities
Operational area	Improve ICS capability level	Ongoing improvement of ICS cyber security capabilities
Risk / security managers	Having a model to define ICS cyber security capabilities	Ongoing improvement of ICS cyber security capabilities
	External	
Shareholders	Being aware of ICS protection capability level	Information on ICS cyber security capabilities
Partners	Ensuring comparable level of cyber security capabilities	Information on ICS cyber security capabilities
Suppliers	Ensuring a homogeneous framework for requirement definition.	Assessment of cyber security capability level of services provided.
Regulator/Authorities	Being aware of ICS cyber security level	Information on ICS cyber security capabilities
External users	Being aware of ICS cyber security level	Information on ICS cyber security capabilities
Consultants/Auditors	Having a model to define ICS cyber security capabilities	Method for ongoing improvement / assessment of ICS cyber security capabilities

Table 1: Stakeholder needs and usefulness of the model

2. ABOUT THE NATIONAL SCHEME ON INDUSTRIAL SECURITY

The passing of Act 8/2011, of 28 April, which establishes measures for the Protection of Critical Infrastructures (PIC Act), evidenced the importance of security in Critical Infrastructures within National Security. Besides, National Security Strategy [1] 2013 acknowledges for the first time cyber threats as one of the risks threatening national security. In line with the above, National Cyber Security Strategy [2] 2013 completes the commitment to the protection of industrial control systems as a key element in a comprehensive approach of cyber security.

In this context, the Spanish National Cyber Security Institute (INCIBE), an agency of the Ministry for Energy, Tourism, and Digital Agenda, and the National Centre for the Protection of Critical Infrastructures (CNPIC), an agency of the Ministry of the Interior, pursuant to an agreement executed in 2012 and renewed in 2015 between the State Secretariat for Information Society and Digital Agenda (SESIAD) and the State Secretariat of Security (SES), agree to promote the use of National Industrial Security Scheme (ENSI) as an instrument to improve security of industrial critical infrastructure and with a global approach insofar that it may be applied to industrial control of any organization.

In this scenario, favouring a harmonized approach to security and extending its application throughout the value chain of industrial organizations, recognizing the role or providers and clients, are key to understand the whole picture addressed by ENSI. This could be the base for new initiatives that would allow ENSI to grow and would approach security from a more integral perspective.

The ENSI activities are divided in four fundamental scopes that were established to cover the specific needs of its scope of application:

- LRA-IS: Methodology of Light Risk Analysis of Integral Security, as a starting point and cornerstone of the security improvement process. Since it is an independent method within this methodology, ARLI-CIB allows for a specific, lighter approach to the ICS Cyber Security Risk Analysis.
- ICRI: Indicators for Cyber Resilience Improvement, as an instrument for diagnosis and measurement of the capability to withstand and overcome disasters and stresses coming from the digital world.
- C4V: Capability Building Model in Cyber Security of the Value Chain as the main element in operator service provider activities and operations: providers and clients.
- AS: Cyber Security Certification System, which guarantees application of a minimum level of equivalent security measures in all architectures providing similar or comparable services.

A practical and light approach dominates all ENSI elements and establishes a complete framework for improving cyber security in industrial control systems.

Here, the different guides and design document, which are in all cases aligned with all premises established in the Operator Security Plans, Specific Protection Plans, and Sector Strategic Plans, shall provide instructions, criteria and tools to make implementation by different stakeholders easier.

3. INTRODUCTION AND BACKGROUND

3.1. What are capability building models?

3.1.1. Definition

Capability building models (also known as capability development models) are a conceptual approach focused in understanding the obstacles that prevent people, governments and organizations to achieve their developmental objectives, and at the same time, in improving the abilities that will allow them to achieve measurable and sustainable results.

The steps for building this organizational capability include: Developing a conceptual framework, establishing an organizational attitude, developing a vision and a mission, developing an organizational structure, and acquiring skills and resources.

3.1.2. Origins

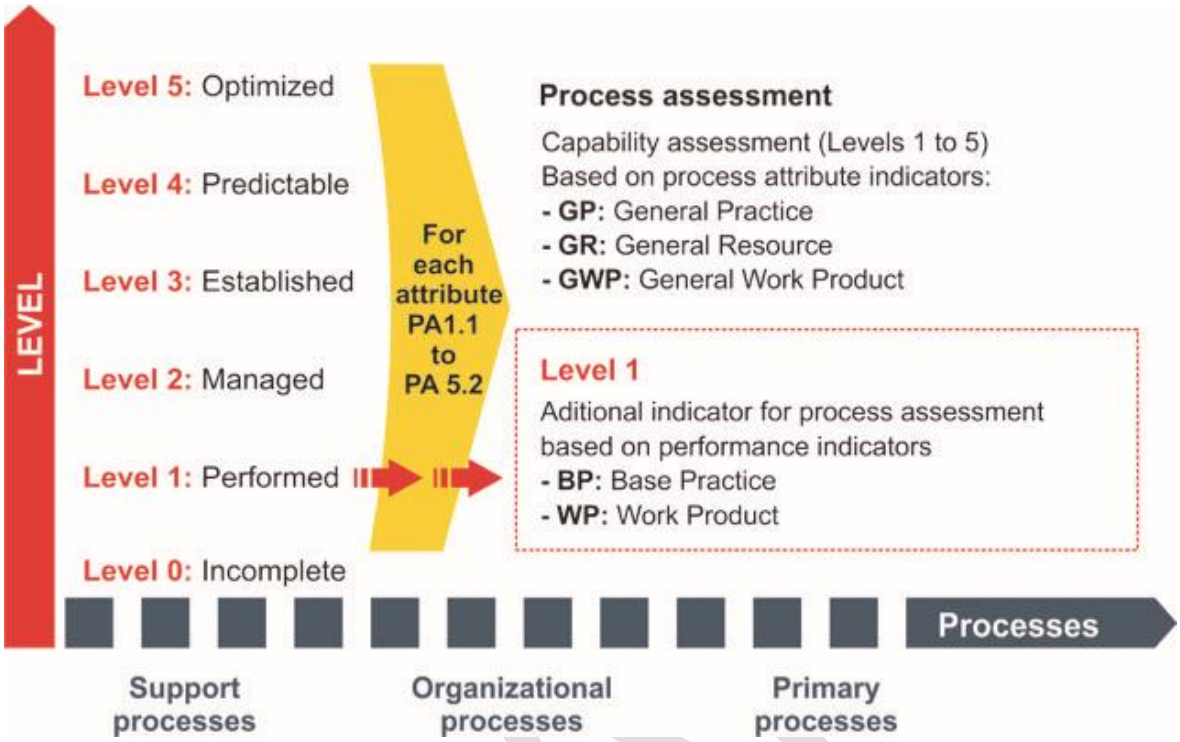
This term was created in 1991 by the United Nations Development Programme (UNDP) and, since then, this type of models has been continuously applied by international organizations (such as the World Bank or United Nations itself) to refer to development programmes in specific regions or communities. Originally, the terms referred to the development of abilities, competences and skills by persons in those developing societies so they may overcome the causes for lack of growth and exclusion.

3.1.3. An approach from the ICT environment

In the IT environment, two approaches to the concept described above are especially known:

- The Capability Maturity Models (CMM) designed in early 1990s were intended, originally, to assess software development processes, although their use has been later extended to other processes. Their precursor is the IT stages of growth model by Richard L. Nolan (1973). Its subsequent development has been carried out by the Software Engineering Institute of the Carnegie Mellon University.
- Capability Models, leaded by the group of standards ISO/IEC 15504 (grouped under the common title Software Process Improvement and Capability Determination or its acronym SPICE). As in the previous example, they were initially developed for software development and have later been extended to other processes. The work group that created this model was formed in 1993; the model underwent significant revision in 2004. For this reason, the process reference model has diverged from the standard, establishing said standard specifically as the measurement framework which may be used with any process reference model. That is, SPICE defines two dimensions:
    - Capability dimension (levels 2 to 5), which focuses on the process and deals exclusively with generic attributes, that is, attributes applicable to any process: metrics, control mechanisms, innovation management, optimization...

- Process dimension, which includes specific indicators of the process being assessed.



Caption 1: Assessment Indicators

The main difference between the two models lays in the idea of **maturity**, since this concept is applied at an organizational level for the whole company or entity, while **capability** is assessed at a process level and is carried out with the aim of improving such process.

A maturity-based level may be understood as a group of structured levels which describe the level of trustworthiness and sustainability of behaviours, practices and processes within an organization which still lead to expected results.

In fact, standard ISO/IEC 15504 understands that these maturity models consist in capability levels characterised by a series of process attributes that include generic practice; it is the assessors' role to find evidence in order to determine capabilities of an organization for creating the expected products (either software, systems or IT services).

Although, in both cases, there are five levels, as expected, no general equivalence can be established and, in fact, assessments based on SPICE usually yield lower results than those based on CMM (fundamentally because achieving SPICE level 1 requires that the product already produces the intended results).

Maturity level	Capability level	Attribute
5 Optimised	5 Optimised	PA 5.1 Process Innovation PA 5.2 Process Optimisation
4 Managed and Measurable	4 Predictable	PA 4.1 Process Measurement PA 4.2 Process Monitoring
3 Defined	3 Established	PA 3.1 Process Definition PA 3.2 Process Deployment
2 Repeatable but intuitive	2 Managed	PA 2.1 Performance Management PA 2.2 Work Product Management
1 Initial / Ad Hoc	1 Performed	PA 1.1 Process Performance
0 Non-existent	0 Incomplete	

Table 2: Comparing CMM and SPICE levels.

3.1.4. Difference with other types of documents

Capability building models are not intended for defining essential minimum requirements for the collectives to which they are applied. They have, in contrast, a more constructive approach, contemplating better prepared organizations to react to the challenges that prevent them to achieve their development goals.

3.2. Public-Private Partnership

With the purpose of acquiring a model with these characteristics in the minimum time possible, the Spanish National Cyber Security Institute and LEET Security have entered a Collaboration Agreement for developing a model based on the security qualification method developed by LEET Security.

4. MODEL

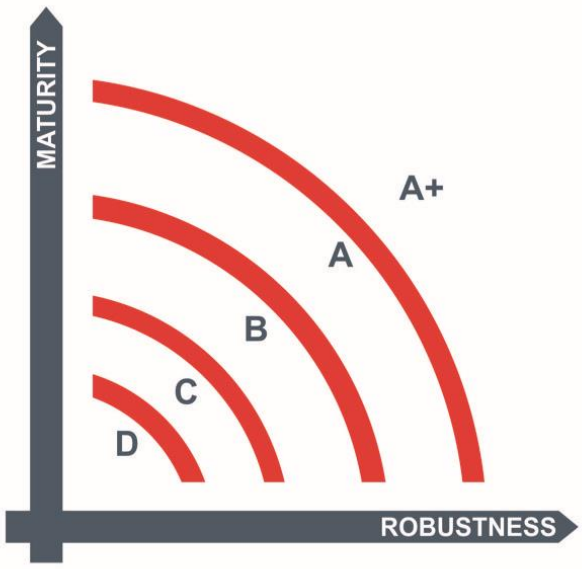
4.1. General Description

A cyber security programme represents a sum of processes, technologies, policies, governance, alignment with business, awareness activities and other elements necessary to manage in an effective manner the organizations policy on cyber security. As described above, capability models can be traced back to Richard L. Nolan's stage model, and using them has the following benefits:

- It's easy to understand and to explain to non-experts.
- A seasoned professional may use this model to assess capability based on interviews, observations and other evidence.
- They provide a qualitative measurement of capability.
- It allows for benchmarking with common criteria.
- It has been originally designed to assess information technologies, and they are easily adapted to a cyber security environment.

The model described in this document has not been designed to assess maturity in the organization as a whole, but to offer a mechanism as objective as possible in order to assess the capability level in terms of cyber security presented by an industrial control system.

In this sense, the model exposed here diverges from existing maturity based models in the fact that not only does it assess the processed implemented within the organization; it also assesses robustness of technical security levels applied, in an effective manner on industrial control systems included in the scope.



Caption 2: New model capabilities

This dual approach, which combines process maturity and technical robustness, allows organisations to have a complete, easily comprehensible vision of their cyber security capability level regarding protection of those industrial control systems with which it operates. That is, it allows organisations to be aware of their current level of capabilities and, which is more important, to establish a target level and to be aware of the steps to be followed in order to achieve this higher cyber security capability level.

4.2. Levels

The capability building level has five levels, from A+ to D (A+ being the highest mark). The system assesses security measures and resilience in ICS management; as a consequence, different ICSs operated by the same organization may obtain different results in their capabilities assessment.

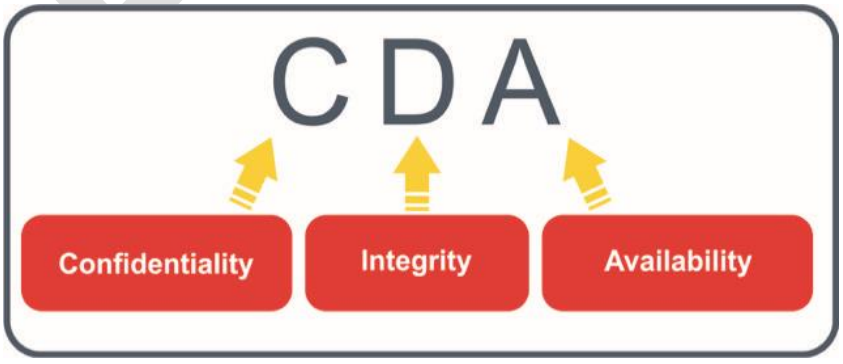
Unlike the models evaluating processes, the level used in this document may not have a name for identifying processes, so that a generic name, without any adjectives, was chosen: However, the factors that contribute to higher levels would be the following:

- Policies and procedures
- Management involvement
- Monitoring mechanisms
- Awareness
- Budget
- Professionalisation of the role
- Robustness of technical measures
- Relationships with third parties (including service providers)
- Resilience

4.3. Dimensions

Since different security measures may be established for each ICS, the model carries out a three dimensional assessment of security, with regard to confidentiality, integrity and availability. This way, an assessment of capabilities is expressed by a triad of letters:

- The first letter corresponds to the **confidentiality** level.
- The second letter corresponds to the **integrity** level.
- And the third letter corresponds to the **availability** level.

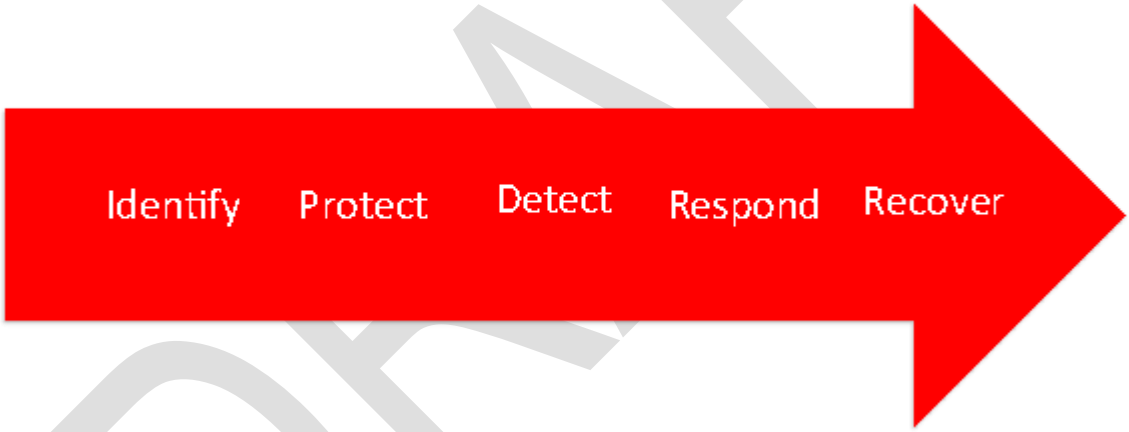


Caption 3: Capability assessment format

4.4. Key functions of cyber security and cyber resilience

Functions organise basic cyber security activities at a high level and, besides, allow their alignment with existing methodologies for incident management, which serves as an evidence for cyber security investments. Key functions generally identified regarding cyber security by several frameworks and documents are the following five:

- **Identify:** Development of the necessary organizational comprehension requested to manage cyber security risks affecting systems, assets, data and capabilities.
- **Protect:** Development and implementation of the appropriate safeguards to ensure that critical services are delivered.
- **Detect:** Development and implementation of the appropriate activities to identify cyber security events as they occur.
- **Respond:** Development and implementation of the appropriate activities in order to adopt actions regarding identified cyber security events.
- **Recover:** Development and implementation of the appropriate activities for maintaining plans oriented to promote resilience and recover activities or services affected by cyber security events.



Caption 4: Key cyber security functions

These five key functions have been developed in a cyber security framework by the National Institute of Standards and Technology (NIST) to include:

- **Categories:** Groups of cyber security results in close relationship with the needs of a cyber security programme and with specific activities.
- **Subcategories:** More detailed divisions that represent results of specific management or technical activities. They provide a set of results which, without being exhaustive, help achieving the goals for each category.

This division shall allow to design the cyber security measures included in this capability building model.

On the other hand, and provided that organizations may be subject to many types of cyber attack, including attacks aimed at service interruption, or attacks that explore

vulnerabilities of their systems with the purpose of accessing valuable information for cyber espionage or for criminal purposes, threatening national interests and violating the trust of their clients, progress has to be made in acquiring cyber resilience capabilities. Cyber resilience is defined as the capability of a process, business, organisation or nation to anticipate, resist, recover and evolve in order to improve their capabilities to address adverse conditions, stress or attacks against cyber resources they need in order to operate.

In order to achieve such cyber resilience, we start with a set of goals, capabilities and techniques; in the first place we must be able to measure them in a manner that is both efficient, coordinated and methodical, with the purpose of ensuring that organizations have implemented a reasonable set of measures that guarantee that their data, systems and equipment are protected. This has been the reason that has lead National Cyber Security Institute (INCIBE) to organise a series of cyber resilience metrics and indicators.

In such metrics and indicators, capabilities are organized in six levels of maturity:

- **Non-existent** (level 0)
- **Initial / ad-hoc** (level 1)
- **Repeatable but intuitive** (level 2)
- **Defined** (level 3)
- **Managed and measurable** (level 4)
- **Optimised** (level 5)

These levels shall include measures oriented to achieve such cyber resilience in the capability construction model detailed in this document.

5. ASSESSMENT METHODOLOGY

5.1. Assignment of a capability level

5.1.1. Model attributes

Determination of the capacity level is based in the assessment of attributes classified in 14 chapters:

Model attributes	
■ Information Security Management Program	■ Protection against malicious code
■ System operation	■ Network controls
■ Personnel security	■ Monitoring
■ Security of installations	■ Access control
■ Third parties processing	■ Secure development
■ Resilience	■ Incident Management
■ Compliance	■ Cryptography

Each chapter is divided in different controls that have to be assessed in order to determine the level of capability. The assessment methodology establishes the conditions that have to be met in order to achieve each level, considering that these conditions are cumulative; that is, that, to reach level A, conditions associated to levels D, C and B must also be met.

Considering that the assessment is three-dimensional (confidentiality - integrity - availability), the final capability shall be composed by three letters, one for each security dimension. In order to determinate each dimension, the minimal number of levels corresponding to common security measures and to those measures applicable to each dimensions. For this reason, control are divided in four types:

- Common security measures
- Confidentiality-related security measures
- Integrity-related security measures
- Availability-related security measures

5.1.2. Definition of scope

As stated above, capabilities are assessed with regard to the protection of a ICS. Consequently, the scope shall depend on the specific architecture of the system over which the model is applied.

Such scope should include all connected and not completely segregated systems for any ICS components, since they may affect ICS security.

Systems are composed by persons, processes and technology, such as servers, software, network components, including virtualised components, and, naturally, those components inherent to an ICS. Examples of the above include:

- Servers: web, applications, database, authentication, e-mail, proxy, network protocols, DNS ...
- Applications: internal / external, purchased / adapted…
- Network components: firewalls, switches, routers, wireless access points, network appliances, security appliances...
- ICS components: PLC, SIS…

If there is no network segmentation of any kind, the full network must be included in the scope of the assessment. Network segmentation may be implemented by different physical or logical methods that limit access to a specific network segment (such as, for instance, the network of field devices network or the network of control points).

If network segmentation is used to reduce the scope of the assessment, the mechanisms used must be documented, as well as the methods followed to guarantee that configuration is appropriate (network configuration, deployed technologies and any other implemented control) to facilitate its assessment and allow for subsequent evaluation.

5.1.3. Value Chain Assessment

The assessment of capability is based on all ICS components. Therefore, any service providers involved in any aspect of the services provided by such ICSs or in the management of any component (routers, firewalls, databases, physical security, applications, security, servers, PLCs, etc.) may, obviously, impact system security.

For those ICS organizations that outsource part of their infrastructure management to third party service providers, the capability assessment must include the function of each service provider, clearly identifying which requirements is the responsibility of which provider. There are two options to assess third party capabilities.

1. The provider may undergone its own capability assessment and provide the results of such assessment to the ICS manager; or
2. If providers do not carry out their own assessment, then their service must be included in the scope of the assessment carried out by the ICS manager.

The ultimate goal is to ensure that all components of the chain value have a level or cyber security capabilities, at least, equal to the goal established for the service manager.

In general, the service managers must establish a risk management procedure oriented to guarantee that their providers comply with the requirements defined in this document regarding the achieved level of capacity, both when the contract was executed and throughout the entire service life cycle.

Such procedure shall be based in the following elements that the service manager must define, establish and ensure that they are implemented (ideally, working together with security and procurement areas).

- Identification of services outsourced to third parties with potential impact in the provided service.

- Identification of the level of potential impact in outsourced services.
- Definition of cyber security requirements depending on the level of criticality.
- Definition of supervision mechanisms depending on the level of criticality.
- Process management and continuous improvement.

5.1.4. Criteria for determining the level of capability

The criteria defined to determine the level of cyber security capability is based on the method established in standard ISO/IEC 15504, but considering that the assessment does not only apply to the maturity of a process but also to the robustness of security measures established for the provision of a service.

For this reason, each control has been assigned a level of priority (from 1 to 3), in the levels where it applies. As described below, such levels shall be used to assess the level of capability of a service according to the following criterion: In order to achieve a certain level, the service must have implemented:

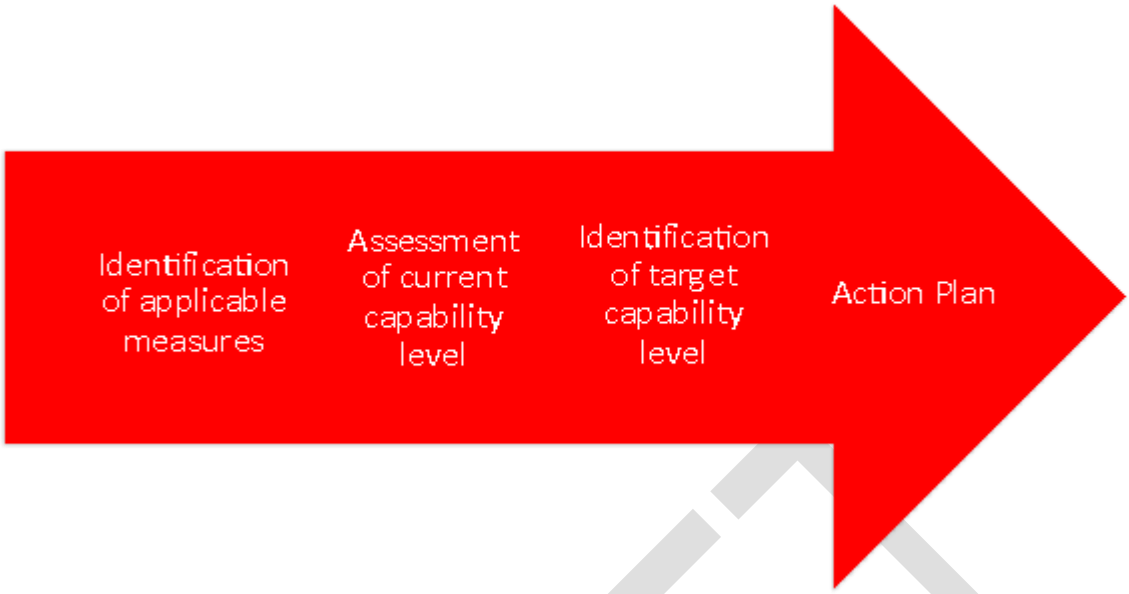
- 100% of priority 1 controls corresponding to the relevant level;
- at least 85% of priority 2 controls corresponding to the relevant level; and
- at least 50% of priority 3 controls corresponding to the relevant level.

5.1.5. Use of capability model

This section includes basic guidelines on the use of this model in order to address a process for identifying the current capability level and an improvement plan for said model (the reasons causing such need for improvement depend on each situation and each organisation).

The recommended steps to address this improvement process are the following:

1. Identification of applicable measures.
2. Assessment of current capability level
3. Identification of target capability level
4. Definition of an action plan



Caption 5: Use of capability model

5.1.5.1. Identification of applicable measures

In the first place, in line with the previous section regarding the scope definition (see 4.1.2) and the dependences to external providers (see 4.1.3), it is necessary to identify which of the security measures included in the model are applicable to the actual system to be assessed.

This step is equivalent to the step present in information security system management methodologies consisting in preparing the so-called "Statement of applicability"; that is, which measures, out of all, shall be considered in a specific situation.

5.1.5.2. Assessment of current capability level

In order to determine current capability level, it is recommended to use an assessor independent from the people responsible for systems operation; such assessor may be either internal (security or auditor) or external (from a company unrelated to the operation). In both cases, it must be ensured that the professionals in charge have sufficient knowledge and expertise to carry out this assessment.

5.1.5.3. Identification of target capability level

By definition, capability building models do not have "appropriate" or "better" levels. Instead, each organisation, depending on the system being assessed, the existing level of risk and defined acceptable risk criteria, must establish what the most appropriate level of capability is.

Usually, the more critical the assessed system is or the more serious the threats are, the higher the level of target capacity shall be.

Due to the model structure, capability levels are defined by the three dimensions described above (confidentiality, integrity and availability), so that the organization must identify a target capability level for each one of those dimensions.

5.1.5.4. Definition of an action plan

In case that it is desired to reach a capability level higher than the current one, an action plan for implementing the corresponding necessary measures must be implemented. In order to facilitate implementation of measures, priorities included in each security measure and level help identifying basic measures (priority 1), which have to be implemented first, since they subsequent measures (priorities 2 and 3) are based on them.

In order to address measure implementation, organizations may use project management methodologies or even organizational change methodologies, such as the proposal included in COBIT 5 Implementation

6. ACRONYMS

CMM: Capability Maturity Model

IEC: International Electrotechnical Commission

ISO: International Organization for Standardization

SPICE: Software Process Improvement and Capability Determination

PIC: Critical Infrastructure Protection

UNDP: United Nations Development Programme

7. REFERENCES

[1] Government of Spain, “NATIONAL SECURITY STRATEGY,” 2013. [Online]. Available: http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf.

[2] Government of Spain, “NATIONAL CYBER SECURITY STRATEGY,” 2013. [Online]. Available: http://www.dsn.gob.es/es/file/146/download?token=Kl839vHG

8. BIBLIOGRAPHY

United Nations Committee of Experts on Public Administration (2006). "Definition of basic concepts and terminologies in governance and public administration" (PDF). United Nations Economic and Social Council.

Kaplan, Allan (Aug 2000). "Capacity Building: Shifting the Paradigms of Practice". Development in Practice. 3/4 10 (10th Anniversary Issue): 517–526.

Paulk, Mark C.; Weber, Charles V; Curtis, Bill; Chrissis, Mary Beth (February 1993). "Capability Maturity Model for Software (Version 1.1)" (PDF). Technical Report (Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University). CMU/SEI-93-TR-024 ESC-TR-93-177.

Nolan, R. L. (July 1973). "Managing the computer resource: A stage hypothesis". Comm. ACM 16 (7): 399–405

Anderson, Kerry A. (December, 2014). “From Here to Maturity-Managing the Information Security Life Cycle. ISACA Journal, Volume 6, 2014.

ISO/IEC 15504-4:2004 Information technology — Process assessment — Part 4: Guidance on use for process improvement and process capability determination

“Process Assessment Model (PAM): Using COBIT® 5” , ISACA, 2013

“Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans”, National Institute of Standards and Technology Special Publication 800-53, 2008

“Guide to Industrial Control Systems (ICS) Security”, National Institute of Standards and Technology Special Publication 800-82 Revision 2,May 2015

“Framework for Improving Critical Infrastructure Cybersecurity” Version 1.0, National Institute of Standards and Technology, February 2014

Cyber Security Capability Maturity Model (CMM) – Pilot, Global Cyber Security Capacity Centre University of Oxford (15/12/2014)

“Rating guide” Version 2, LEET Security, 2016, www.leetsecurity.com/descargar-guia/

“COBIT® 5 Implementation”, ISACA, 2012

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

GOBIERNO DE ESPAÑA MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

CERT DE SEGURIDAD E INDUSTRIA