This workbook is the self-assessment tool for the CyberFundamentals Framework. The CyberFundamentals Framework is developed by the Centre for Cybersecurity Belgium (CCB), which operates under the authority of the Prime Minister of Belgium. The framework includes a set of concrete measures to protect data, significantly reduce the risk of the most common cyber-attacks, and increase the cyber resilience of organisations.

The framework is available for both voluntary and mandatory use.

In case of voluntary use, it is considered as National Certification Scheme for Cybersecurity Certification implementing the statutory mandate of the CCB (RD 10 Oct 2014, Art. 3 8°).

For mandatory use of the certification scheme, the laws and regulations imposing mandatory use apply.

The Cyberfundamentals Conformity self-declaration is based on a self-assessment using this tool. The self-declaration can be verified by an independent third-party Conformity Assessment Body (CAB) and will then result in a label, a verified claim or a certificate in accordance with the Conformity Assessment Scheme.

Directions:

(1) Each "details" section contains the controls of the respective cyberfundamentals framework level (BASIC-IMPORTANT- ESSENTIAL).

The way each control is assessed considers 2 angles: How the controle is documented (documentation maturity) and how that documentation is implemented (implementation maturity). The maturity of each of the controls is assessed using the explanation in the Maturity Levels tab.

(2) Based on the assessment and according to the maturity level, a value from 1 to 5 is entered per control in the "details" tab of each assurance level. This level is determined for both documentation maturity and implementation maturity.

(3) The "summary" tab for the respective cyberfundamentals levels shows the maturity score that determines whether or not one is compliant in accordance with the Conformity Assessment Scheme. The target scores indicated in the "summary" tab are as determined in the Conformity Assessment Scheme.

CyberFundamentals Framework — Maturity Levels Overview

The **CyberFundamentals Framework**, developed by the **Centre for Cybersecurity Belgium (CCB)** under the authority of the **Prime Minister of Belgium**, defines a structured approach to assessing and improving organizational cybersecurity resilience.
 This framework supports both voluntary and mandatory adoption for organizations operating under Belgian jurisdiction.

When used voluntarily, it serves as a **National Certification Scheme for Cybersecurity Certification**, implementing the statutory mandate of the CCB (Royal Decree 10 October 2014, Article 3, §8).
 For mandatory application, compliance is required as specified in the applicable laws and regulations.

The **CyberFundamentals Conformity Self-Declaration** is based on a **self-assessment** using this tool.
 Verification by an independent **Conformity Assessment Body (CAB)** may result in an official **label**, **verified claim**, or **certificate** under the **Conformity Assessment Scheme**.

Directions for Using the Self-Assessment Tool

1. Each **Details** section contains the controls for the respective CyberFundamentals framework levels — **BASIC**, **IMPORTANT**, and **ESSENTIAL**.
   Each control is assessed on two dimensions:
   - **Documentation Maturity** — how well the control is formally defined and approved.
   - **Implementation Maturity** — how effectively the documented control is applied in practice.
1. Based on the assessment, each control is assigned a **maturity value (1 to 5)** for both **documentation** and **implementation**.
   These values are entered in the "Details" tab of each assurance level.
2. The **Summary** tab displays overall maturity scores that determine compliance in accordance with the Conformity Assessment Scheme.
   Target scores per level (Basic, Important, Essential) are also defined within this tab.

Maturity Levels and Descriptions

Level 1 — Initial

Maturity Value: 1
Documentation Maturity:

- No process documentation or documentation not formally approved by management.
  Implementation Maturity:
- Standard process does not exist.

Level 2 — Repeatable

Maturity Value: 2
Documentation Maturity:

- Formally approved process documentation exists but has not been reviewed in the previous two years.
  Implementation Maturity:
- Ad-hoc process exists and is done informally.

Level 3 — Defined

Maturity Value: 3
Documentation Maturity:

- Formally approved process documentation exists.
- Exceptions are documented and approved.
- Documented and approved exceptions occur less than 5% of the time.
  Implementation Maturity:
- Formal process exists and is implemented.
- Evidence is available for most activities.
- Fewer than 10% of process exceptions occur.

Level 4 — Managed

Maturity Value: 4
Documentation Maturity:

- Formally approved process documentation exists.
- Exceptions are documented and approved.
- Documented and approved exceptions occur less than 3% of the time.
  Implementation Maturity:
- Formal process exists and is implemented for all activities.
- Detailed process metrics are captured and reported.
- Minimal target metrics established.
- Fewer than 5% of process exceptions occur.

Level 5 — Optimizing

Maturity Value: 5
Documentation Maturity:

- Formally approved process documentation exists.
- Exceptions are documented and approved.
- Documented and approved exceptions occur less than 0.5% of the time.
  Implementation Maturity:
- Formal process exists and is implemented.
- Evidence available for all activities.
- Metrics are established, tracked, and continually improved.
- Less than 1% of process exceptions occur.

Assessment Definitions

Documentation Maturity:
Measures how well an organization's written rules and procedures satisfy the controls of the CyberFundamentals Framework.

Implementation Maturity:
Assesses how effectively an organization's actual operational practices align with the CyberFundamentals Framework.

Maturity Level Thresholds

Evaluation Criteria	BASIC	IMPORTANT	ESSENTIAL
Each Key Measure Maturity Level	≥ 2.5 / 5	≥ 3 / 5	≥ 3 / 5
Each Category Maturity Level	n/a	n/a	≥ 3 / 5
Total Maturity Level (average)	≥ 2.5 / 5	≥ 3 / 5	≥ 3.5 / 5

BASIC Details:

Function: IDENTIFY (ID)

Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

Subcategory: ID.AM-1: Physical devices and systems within the organization are inventoried

Requirement: ID.AM-1.1: An inventory of assets associated with information and information processing facilities within the organization shall be documented, reviewed, and updated when changes occur.

Guidance: â€¢ This inventory includes fixed and portable computers, tablets, mobile phones, Programmable Logic Controllers (PLCs), sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices.

â€¢ This inventory must include all assets, whether or not they are connected to the organization's network.

â€¢ The use of an IT asset management tool could be considered.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Category Documentation Maturity Score: 1

Category Implementation Maturity Score: 1

Function: IDENTIFY (ID)

Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organizationâ€™s risk strategy.

Subcategory: ID.AM-2: Software platforms and applications within the organization are inventoried

Requirement: ID.AM-2.1: An inventory that reflects what software platforms and applications are being used in the organization shall be documented, reviewed, and updated when changes occur.

Guidance: â€¢ This inventory includes software programs, software platforms and databases, even if outsourced (SaaS).

â€¢ Outsourcing arrangements should be part of the contractual agreements with the provider.

• Information in the inventory should include for example: name, description, version, number of users, data processed, etc.

• A distinction should be made between unsupported software and unauthorized software.

• The use of an IT asset management tool could be considered.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Function: IDENTIFY (ID)

Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

Subcategory: ID.AM-3: Organizational communication and data flows are mapped

Requirement: ID.AM-3.1: Information that the organization stores and uses shall be identified.

Guidance: •   Start by listing all the types of information your business stores or uses. Define "information type" in any useful way that makes sense to your business. You may want to have your employees make a list of all the information they use in their regular activities. List everything you can think of, but you do not need to be too specific. For example, you may keep customer names and email addresses, receipts for raw material, your banking information, or other proprietary information.

‚•   Consider mapping this information with the associated assets identified in the inventories of physical devices, systems, software platforms and applications used within the organization (see ID.AM-1 & ID.AM-2).

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

Subcategory

Implementation Maturity Score: 1

Function: IDENTIFY (ID)

Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

Subcategory: ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value

Requirement: ID.AM-5.1: The organization's resources (hardware, devices, data, time, personnel, information, and software) shall be prioritized based on their classification, criticality, and business value.

Guidance: •   Determine organization's resources (e.g., hardware, devices, data, time, personnel, information, and software):

o   What would happen to my business if these resources were made public, damaged, lost…?

o   What would happen to my business when the integrity of resources is no longer guaranteed?

o   What would happen to my business if I/my customers couldn't access these resources? And rank these resources based on their classification, criticality, and business value.

•   Resources should include enterprise assets.

Documentation Score: 1

Subcategory Documentation Maturity Score: 1

Subcategory

Implementation Maturity Score: 1

Function: IDENTIFY (ID)

Category: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

Subcategory: ID.GV-1: Organizational cybersecurity policy is established and communicated

Requirement: ID.GV-1.1: Policies and procedures for information security and cyber security shall be created, documented, reviewed, approved, and updated when changes occur.

Guidance: •   Policies and procedures used to identify acceptable practices and expectations for business operations, can be used to train new employees on your information security expectations, and can aid an investigation in case of an incident. These policies and procedures should be readily accessible to employees.

•   Policies and procedures for information- and cybersecurity should clearly describe your expectations for protecting the organization's information and systems, and how management expects the company's resources to be used and protected by all employees.

•   Policies and procedures should be reviewed and updated at least annually and every time there are changes in the organization or technology. Whenever the policies are changed, employees should be made aware of the changes.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Category Documentation Maturity Score: 1

Category Implementation Maturity Score: 1

Function: IDENTIFY (ID)

Category: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organizationâ€™s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

Subcategory: ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

Requirement: ID.GV-3.1: Legal and regulatory requirements regarding information/cybersecurity, including privacy obligations, shall be understood and implemented.

Guidance: There are no additional guidelines.

Documentation Score: 1

Implementation Score: 1

Function: IDENTIFY (ID)

Category: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organizationâ€™s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

Subcategory: ID.GV-4: Governance and risk management processes address cybersecurity risks

Requirement: ID.GV-4.1: As part of the company's overall risk management, a comprehensive strategy to manage information security and cybersecurity risks shall be developed and updated when changes occur.

Guidance: This strategy should include determining and allocating the required resources to protect the organisation's business-critical assets.

Documentation Score: 1

Implementation Score: 1

Function: IDENTIFY (ID)

Category: Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Subcategory: ID.RA-1: Asset vulnerabilities are identified and documented

Requirement: ID.RA-1.1: Threats and vulnerabilities shall be identified.

Guidance: â€¢   A vulnerability refers to a weakness in the organizationâ€™s hardware, software, or procedures. It is a gap through which a bad actor can gain access to the organizationâ€™s assets. A vulnerability exposes an organization to threats.

â€¢   A threat is a malicious or negative event that takes advantage of a vulnerability.

â€¢   The risk is the potential for loss and damage when the threat does occur.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Category Documentation Maturity Score: 1

Category Implementation Maturity Score: 1

Function: IDENTIFY (ID)

Category: Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Subcategory: ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk

Requirement: ID.RA-5.1: The organization shall conduct risk assessments in which risk is determined by threats, vulnerabilities and impact on business processes and assets.

Guidance: â€¢   Keep in mind that threats exploit vulnerabilities.

• Identify the consequences that losses of confidentiality, integrity and availability may have on the assets and related business processes.

Documentation Score: 1

Implementation Score: 1

Function: PROTECT (PR)

Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Key Measure: Key Measure

Subcategory: PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

Requirement: PR.AC-1.1: Identities and credentials for authorized devices and users shall be managed.

Guidance: Identities and credentials for authorized devices and users could be managed through a password policy. A password policy is a set of rules designed to enhance ICT/OT security by encouraging organization's to:

(Not limitative list and measures to be considered as appropriate)

• Change all default passwords.

• Ensure that no one works with administrator privileges for daily tasks.

• Keep a limited and updated list of system administrator accounts.

• Enforce password rules, e.g. passwords must be longer than a state-of-the-art number of characters with a combination of character types and changed periodically or when there is any suspicion of compromise.

• Use only individual accounts and never share passwords.

• Immediately disable unused accounts

• Rights and privileges are managed by user groups.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Category Documentation Maturity Score: 1

Category Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Subcategory: PR.AC-2: Physical access to assets is managed and protected

Requirement: PR.AC-2.1: Physical access to the facility, servers and network components shall be managed.

Guidance: •   Consider to strictly manage keys to access the premises and alarm codes. The following rules should be considered:

o   Always retrieve an employee's keys or badges when they leave the company permanently.

o   Change company alarm codes frequently.

o   Never give keys or alarm codes to external service providers (cleaning agents, etc.), unless it is possible to trace these accesses and restrict them technically to given time slots.

•   Consider to not leaving internal network access outlets accessible in public areas. These public places can be waiting rooms, corridors...

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Subcategory: PR.AC-3: Remote access is managed

Requirement: PR.AC-3.1 The organisation's wireless access points shall be secured.

Guidance: Consider the following when wireless networking is used:

â€¢   Change the administrative password upon installation of a wireless access points.

â€¢   Set the wireless access point so that it does not broadcast its Service Set Identifier (SSID).

â€¢   Set your router to use at least WiFi Protected Access (WPA-2 or WPA-3 where possible), with the Advanced Encryption Standard (AES) for encryption.

â€¢   Ensure that wireless internet access to customers is separated from your business network.

â€¢   Connecting to unknown or unsecured / guest wireless access points, should be avoided, and if unavoidable done through an encrypted virtual private network (VPN) capability.

â€¢   Manage all endpoint devices (fixed and mobile) according to the organization's security policies.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Key Measure: Key Measure

Requirement: PR.AC-3.2: The organization's networks when accessed remotely shall be secured, including through multi-factor authentication (MFA).

Guidance: Enforce MFA (e.g. 2FA) on Internet-facing systems, such as email, remote desktop, and Virtual Private Network (VPNs).

Documentation Score: 1

Implementation Score: 1

 Subcategory

Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Key Measure: Key Measure

Subcategory: PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

Requirement: PR.AC-4.1: Access permissions for users to the organizationâ€™s systems shall be defined and managed.

Guidance: The following should be considered:

• Draw up and review regularly access lists per system (files, servers, software, databases, etc.), possibly through analysis of the Active Directory in Windows-based systems, with the objective of determining who needs what kind of access (privileged or not), to what, to perform their duties in the organization.

• Set up a separate account for each user (including any contractors needing access) and require that strong, unique passwords be used for each account.

• Ensure that all employees use computer accounts without administrative privileges to perform typical work functions. This includes separation of personal and admin accounts.

• For guest accounts, consider using the minimal privileges (e.g. internet access only) as required for your business needs.

• Permission management should be documented in a procedure and updated when appropriate.

• Use 'Single Sign On' (SSO) when appropriate.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Key Measure: Key Measure

Requirement: PR.AC-4.2: It shall be identified who should have access to the organization's business's critical information and technology and the means to get access.

Guidance: Means to get access may include: a key, password, code, or administrative privilege.

Documentation Score: 1

Implementation Score: 1

 Subcategory

Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Key Measure: Key Measure

Requirement: PR.AC-4.3: Employee access to data and information shall be limited to the systems and specific information they need to do their jobs (the principle of Least Privilege).

Guidance: The principle of Least Privilege should be understood as the principle that a security architecture should be designed so that each employee is granted the minimum system resources and authorizations that the employee needs to perform its function. Consider to:

â€¢   Not allow any employee to have access to all the businessâ€™s information.

â€¢   Limit the number of Internet accesses and interconnections with partner networks to the strict necessary to be able to centralize and homogenize the monitoring of exchanges more easily.

â€¢   Ensure that when an employee leaves the business, all access to the businessâ€™s information or systems is blocked instantly.

Documentation Score: 1

Implementation Score: 1

 Subcategory

Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Key Measure: Key Measure

Requirement: PR.AC-4.4: Nobody shall have administrator privileges for daily tasks.

Guidance: Consider the following:

â€¢   Separate administrator accounts from user accounts.

â€¢   Do not privilege user accounts to effectuate administration tasks.

â€¢   Create unique local administrator passwords and disable unused accounts.

â€¢   Consider prohibiting Internet browsing from administrative accounts.

Documentation Score: 1

Implementation Score: 1

 Subcategory

Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Key Measure: Key Measure

Subcategory: PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)

Requirement: PR.AC-5.1: Firewalls shall be installed and activated on all the organization's networks.

Guidance: Consider the following:

â€¢   Install and operate a firewall between your internal network and the Internet. This may be a function of a (wireless) access point/router, or it may be a function of a router provided by the Internet Service Provider (ISP).

â€¢   Ensure there is antivirus software installed on purchased firewall solutions and ensure that the administratorâ€™s log-in and administrative password is changed upon installation and regularly thereafter.

â€¢   Install, use, and update a software firewall on each computer system (including smart phones and other networked devices).

â€¢   Have firewalls on each of your computers and networks even if you use a cloud service provider or a virtual private network (VPN). Ensure that for telework home network and systems have hardware and software firewalls installed, operational, and regularly updated.

â€¢   Consider installing an Intrusion Detection / Prevention System (IDPS). These devices analyze network traffic at a more detailed level and can provide a greater level of protection.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Key Measure: Key Measure

Requirement: PR.AC-5.2: Where appropriate, network integrity of the organization's critical systems shall be protected by incorporating network segmentation and segregation.

Guidance: • Consider creating different security zones in the network (e.g. Basic network segmentation through VLAN's or other network access control mechanisms) and control/monitor the traffic between these zones.

• When the network is "flat", the compromise of a vital network component can lead to the compromise of the entire network.

Documentation Score: 1

Implementation Score: 1

 Subcategory

Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

Subcategory: PR.AT-1: All users are informed and trained

Requirement: PR.AT-1.1: Employees shall be trained as appropriate.

Guidance: • Employees include all users and managers of the ICT/OT systems, and they should be trained immediately when hired and regularly thereafter about the company's information security policies and what they will be expected to do to protect company's business information and technology.

• Training should be continually updated and reinforced by awareness campaigns.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Category Documentation Maturity Score: 1

Category Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

Subcategory: PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition

Requirement: PR.DS-3.1: Assets and media shall be disposed of safely.

Guidance: •   When eliminating tangible assets like business computers/laptops, servers, hard drive(s) and other storage media (USB drives, paper…), ensure that all sensitive business or personal data are securely deleted (i.e. electronically "wiped") before they are removed and then physically destroyed (or re-commissioned). This is also known as ,"sanitization" and thus related to the requirement and guidance in PR.IP-6.

,•   Consider installing a remote-wiping application on company laptops, tablets, cell phones, and other mobile devices.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Key Measure: Key Measure

Subcategory: PR.IP-4: Backups of information are conducted, maintained, and tested

Requirement: PR.IP-4.1: Backups for organization's business critical data shall be conducted and stored on a system different from the device on which the original data resides.

Guidance: â€¢   Organization's business critical system's data includes for example software, configurations and settings, documentation, system configuration data including computer configuration backups, application configuration backups, etc.

â€¢   Consider a regular backup and put it offline periodically.

â€¢   Recovery time and recovery point objectives should be considered.

â€¢   Consider not storing the organization's data backup on the same network as the system on which the original data resides and provide an offline copy. Among other things, this prevents file encryption by hackers (risk of ransomware).

Documentation Score: 4

Subcategory Documentation Maturity Score: 4

Category Documentation Maturity Score: 2.5

Category Implementation Maturity Score: 2.5

Function: PROTECT (PR)

Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Subcategory: PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)

Requirement: PR.IP-11.1: Personnel having access to the organizationâ€™s most critical information or technology shall be verified.

Guidance: â€¢   The access to critical information or technology should be considered when recruiting, during employment and at termination.

• Background verification checks should take into consideration applicable laws, regulations, and ethics in proportion to the business requirements, the classification of the information to be accessed and the perceived risks.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

Key Measure: Key Measure

Subcategory: PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools

Requirement: PR.MA-1.1: Patches and security updates for Operating Systems and critical system components shall be installed.

Guidance: The following should be considered:

• Limit yourself to only install those applications (operating systems, firmware, or plugins) that you need to run your business and patch/update them regularly.

• You should only install a current and vendor-supported version of software you choose to use. It may be useful to assign a day each month to check for patches.

• There are products which can scan your system and notify you when there is an update for an application you have installed. If you use one of these products, make sure it checks for updates for every application you use.

• Install patches and security updates in a timely manner.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Category Documentation Maturity Score: 1

Category Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Key Measure: Key Measure

Subcategory: PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

Requirement: PR.PT-1.1: Logs shall be maintained, documented, and reviewed.

Guidance: â€¢	Ensure the activity logging functionality of protection / detection hardware or software (e.g. firewalls, anti-virus) is enabled.

â€¢	Logs should be backed up and saved for a predefined period.

â€¢	The logs should be reviewed for any unusual or unwanted trends, such as a large use of social media websites or an unusual number of viruses consistently found on a particular computer. These trends may indicate a more serious problem or signal the need for stronger protections in a particular area.

Documentation Score: 1

Subcategory Documentation Maturity Score: 1

Category Documentation Maturity Score: 1

Category Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Subcategory: PR.PT-4: Communications and control networks are protected

Requirement: PR.PT-4.1: Web and e-mail filters shall be installed and used.

Guidance: â€¢   E-mail filters should detect malicious e-mails, and filtering should be configured based on the type of message attachments so that files of the specified types are automatically processed (e.g. deleted).

â€¢   Web-filters should notify the user if a website may contain malware and potentially preventing users from accessing that website.

Documentation Score: 1

Implementation Score: 1

Function: DETECT (DE)

Category: Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.

Key Measure: Key Measure

Subcategory: DE.AE-3: Event data are collected and correlated from multiple sources and sensors

Requirement: DE.AE-3.1: The activity logging functionality of protection / detection hardware or software

(e.g. firewalls, anti-virus) shall be enabled, backed-up and reviewed.

Guidance: â€¢   Logs should be backed up and saved for a predefined period.

• The logs should be reviewed for any unusual or unwanted trends, such as a large use of social media websites or an unusual number of viruses consistently found on a particular computer. These trends may indicate a more serious problem or signal the need for stronger protections in a particular area.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Category Documentation Maturity Score: 1

Category Implementation Maturity Score: 1

Function: DETECT (DE)

Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

Subcategory: DE.CM-1: The network is monitored to detect potential cybersecurity events

Requirement: DE.CM-1.1: Firewalls shall be installed and operated on the network boundaries and completed with firewall protection on the endpoints.

Guidance: •   Endpoints include desktops, laptops, servers...

• Consider, where feasible, including smart phones and other networked devices when installing and operating firewalls.

• Consider limiting the number of interconnection gateways to the Internet.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Category Documentation Maturity Score: 1

Category Implementation Maturity Score: 1

Function: DETECT (DE)

Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

Subcategory: DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events

Requirement: DE.CM-3.1: End point and network protection tools to monitor end-user behavior for dangerous activity shall be implemented.

Guidance: Consider deploying an Intrusion Detection/Prevention system (IDS/IPS).

Documentation Score: 1

Implementation Score: 1

Function: DETECT (DE)

Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

Key Measure: Key Measure

Subcategory: DE.CM-4: Malicious code is detected

Requirement: DE.CM-4.1: Anti-virus, -spyware, and other -malware programs shall be installed and updated.

Guidance: â€¢ Malware includes viruses, spyware, and ransomware and should be countered by installing, using, and regularly updating anti-virus and anti-spyware software on every device used in companyâ€™s business (including computers, smart phones, tablets, and servers).

â€¢ Anti-virus and anti-spyware software should automatically check for updates in â€œreal-timeâ€ù or at least daily followed by system scanning as appropriate.

,€¢   It should be considered to provide the same malicious code protection mechanisms for home computers (e.g. teleworking) or personal devices that are used for professional work (BYOD).

Documentation Score: 1

Implementation Score: 1

Function: RESPOND (RS)

Category: Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

Subcategory: RS.RP-1: Response plan is executed during or after an incident

Requirement: RS.RP-1.1: An incident response process, including roles, responsibilities, and authorities, shall be executed during or after an information/cybersecurity event on the organization's critical systems.

Guidance: â€¢   The incident response process should include a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack.

â€¢   The roles, responsibilities, and authorities in the incident response plan should be specific on involved people, contact info, different roles and responsibilities, and who makes the decision to initiate recovery procedures as well as who will be the contact with appropriate external stakeholders.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Category Documentation Maturity Score: 1

Category Implementation Maturity Score: 1

Function: RESPOND (RS)

Category: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

Subcategory: RS.CO-3: Information is shared consistent with response plans

Requirement: RS.CO-3.1: Information/cybersecurity incident information shall be communicated and shared with the organization's employees in a format that they can understand.

Guidance: There are no additional guidelines.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Category Documentation Maturity Score: 1

Category Implementation Maturity Score: 1

Function: RESPOND (RS)

Category: Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Subcategory: RS.IM-1: Response plans incorporate lessons learned

Requirement: RS.IM-1.1: The organization shall conduct post-incident evaluations to analyse lessons learned from incident response and recovery, and consequently improve processes / procedures / technologies to enhance its cyber resilience.

Guidance: Consider bringing involved people together after each incident and reflect together on ways to improve what happened, how it happened, how we reacted, how it could have gone better, what should be done to prevent it from happening again, etc.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Category Documentation Maturity Score: 1

Category Implementation Maturity Score: 1

Function: RECOVER (RC)

Category: Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

Subcategory: RC.RP-1: Recovery plan is executed during or after a cybersecurity incident

Requirement: RC.RP-1.1: A recovery process for disasters and information/cybersecurity incidents shall be developed and executed as appropriate.

Guidance: A process should be developed for what immediate actions will be taken in case of a fire, medical emergency, burglary, natural disaster, or an information/cyber security incident.

This process should consider:

â€¢   Roles and Responsibilities, including of who makes the decision to initiate recovery procedures and who will be the contact with appropriate external stakeholders.

â€¢   What to do with companyâ€™s information and information systems in case of an incident. This includes shutting down or locking computers, moving to a backup site, physically removing important documents, etc.

â€¢   Who to call in case of an incident.

Documentation Score: 1

Implementation Score: 1

Subcategory Documentation Maturity Score: 1

 Subcategory

Implementation Maturity Score: 1

Category Documentation Maturity Score: 1

Category Implementation Maturity Score: 1

CyberFundamentals Framework — BASIC Summary

CyberFundamentals Categories and Maturity Scores
IDENTIFY

- **Asset Management (ID.AM)**
  - Target Maturity Score: 2.50
  - Category Maturity Score: 1.00
  - Documentation Maturity Score: 1.10
  - Implementation Maturity Score: 1.10
- **Governance (ID.GV)**
  - Target Maturity Score: 2.50
  - Category Maturity Score: 1.00
  - Documentation Maturity Score: 1.00
  - Implementation Maturity Score: 1.00
- **Risk Assessment (ID.RA)**
  - Target Maturity Score: 2.50
  - Category Maturity Score: 1.00
  - Documentation Maturity Score: 1.00
  - Implementation Maturity Score: 1.00

PROTECT

- **Identity Management, Authentication and Access Control (PR.AC)**
  - Target Maturity Score: 2.50
  - Category Maturity Score: 1.00
  - Documentation Maturity Score: 1.00
  - Implementation Maturity Score: 1.00
- **Awareness and Training (PR.AT)**
  - Target Maturity Score: 2.50
  - Category Maturity Score: 1.00
  - Documentation Maturity Score: 1.00

- o Implementation Maturity Score: 1.00
- **Data Security (PR.DS)**
  - o Target Maturity Score: 2.50
  - o Category Maturity Score: 1.00
  - o Documentation Maturity Score: 1.00
  - o Implementation Maturity Score: 1.00
- **Information Protection Processes and Procedures (PR.IP)**
  - o Target Maturity Score: 2.50
  - o Category Maturity Score: 2.50
  - o Documentation Maturity Score: 2.50
  - o Implementation Maturity Score: 2.50
- **Maintenance (PR.MA)**
  - o Target Maturity Score: 2.50
  - o Category Maturity Score: 1.00
  - o Documentation Maturity Score: 1.00
  - o Implementation Maturity Score: 1.00
- **Protective Technology (PR.PT)**
  - o Target Maturity Score: 2.50
  - o Category Maturity Score: 1.00
  - o Documentation Maturity Score: 1.00
  - o Implementation Maturity Score: 1.00

DETECT

- **Anomalies and Events (DE.AE)**
  - o Target Maturity Score: 2.50
  - o Category Maturity Score: 1.00
  - o Documentation Maturity Score: 1.00
  - o Implementation Maturity Score: 1.00
- **Security Continuous Monitoring (DE.CM)**
  - o Target Maturity Score: 2.50
  - o Category Maturity Score: 1.00
  - o Documentation Maturity Score: 1.00
  - o Implementation Maturity Score: 1.00

RESPOND

- **Response Planning (RS.RP)**
  - o Target Maturity Score: 2.50
  - o Category Maturity Score: 1.00
  - o Documentation Maturity Score: 1.00
  - o Implementation Maturity Score: 1.00

- **Communications (RS.CO)**
  - Target Maturity Score: 2.50
  - Category Maturity Score: 1.00
  - Documentation Maturity Score: 1.00
  - Implementation Maturity Score: 1.00
- **Improvements (RS.IM)**
  - Target Maturity Score: 2.50
  - Category Maturity Score: 1.00
  - Documentation Maturity Score: 1.00
  - Implementation Maturity Score: 1.00

RECOVER

- **Recovery Planning (RC.RP)**
  - Target Maturity Score: 2.50
  - Category Maturity Score: 1.00
  - Documentation Maturity Score: 1.00
  - Implementation Maturity Score: 1.00

Key Measures (KM) and Target Maturity Scores

- **PR.AC-1.1** — Identities and credentials for authorized devices and users shall be managed.
  Target Maturity Score: 2.50
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-3.2** — The organization's network, when accessed remotely, shall be secured through multi-factor authentication (MFA).
  Target Maturity Score: 2.50
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-4.1** — Access permissions for users to the organization's systems shall be defined and managed.
  Target Maturity Score: 2.50
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-4.2** — Employee access to data and information shall be limited to the systems and specific information they need to do their jobs (principle of Least Privilege).
  Target Maturity Score: 2.50

KM Maturity Score: 1.00
Documentation Maturity Score: 1.00
Implementation Maturity Score: 1.00

- **PR.AC-4.4** — Nobody shall have administrator privileges for daily tasks.
  Target Maturity Score: 2.50
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-5.1** — Firewalls shall be installed and activated on all the organization's networks.
  Target Maturity Score: 2.50
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-5.2** — Where appropriate, network integrity of the organization's critical systems shall be protected by incorporating network segmentation and segregation.
  Target Maturity Score: 2.50
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.IP-4.1** — Backups for organization's business-critical data shall be conducted and stored on a system different from the device on which the original data resides.
  Target Maturity Score: 2.50
  KM Maturity Score: 4.00
  Documentation Maturity Score: 4.00
  Implementation Maturity Score: 4.00
- **PR.MA-1.1** — Systems and critical system components shall be patched and updated.
  Target Maturity Score: 2.50
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.PT-1.1** — Logs shall be maintained, documented, and reviewed.
  Target Maturity Score: 2.50
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **DE.AE-3.1** — The activity logging functionality of protection or detection hardware/software (e.g., firewalls, anti-virus) shall be enabled, backed up, and reviewed.
  Target Maturity Score: 2.50
  KM Maturity Score: 1.00

Documentation Maturity Score: 1.00
Implementation Maturity Score: 1.00

- **DE.CM-4.1** — Anti-virus, spyware, and other malware programs shall be installed and updated.
  Target Maturity Score: 2.50
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

Overall Maturity Summary

- **Total Maturity Level:** 1.10
- **TLP Classification:** AMBER
- **CyberFundamentals Maturity Level:** BASIC

The radar graph visualization (not shown in text) illustrates the organization's maturity across all CyberFundamentals categories, comparing:

- **Target Maturity Score (green)**
- **Category Maturity Score (orange)**
- **Documentation Maturity Score (red)**
- **Implementation Maturity Score (blue)**

CyberFundamentals Maturity Level BASIC (Radar Summary)

Purpose:
This radar visualization provides a comparative view of the organization's maturity levels across all CyberFundamentals categories.

Axes represent:

- Each CyberFundamentals category (IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER).
- Maturity levels ranging from **0 to 5**, with:
  - **5 = Optimizing**
  - **4 = Managed**
  - **3 = Defined**
  - **2 = Repeatable**
  - **1 = Initial**
  - **0 = Non-existent**

Plotted Data:

- **Green line:** Target Maturity Score
- **Orange line:** Category Maturity Score
- **Grey line:** Documentation Maturity Score
- **Blue line:** Implementation Maturity Score

Observed Values (from chart and summary):

- **Asset Management (ID.AM):** Target 2.5 — Actual 1.0
- **Governance (ID.GV):** Target 2.5 — Actual 1.0
- **Risk Assessment (ID.RA):** Target 2.5 — Actual 1.0
- **Identity Management, Authentication and Access Control (PR.AC):** Target 2.5 — Actual 1.0
- **Awareness and Training (PR.AT):** Target 2.5 — Actual 1.0
- **Data Security (PR.DS):** Target 2.5 — Actual 1.0
- **Information Protection Processes and Procedures (PR.IP):** Target 2.5 — Actual 2.5
- **Maintenance (PR.MA):** Target 2.5 — Actual 1.0
- **Protective Technology (PR.PT):** Target 2.5 — Actual 1.0
- **Anomalies and Events (DE.AE):** Target 2.5 — Actual 1.0
- **Security Continuous Monitoring (DE.CM):** Target 2.5 — Actual 1.0
- **Response Planning (RS.RP):** Target 2.5 — Actual 1.0
- **Communications (RS.CO):** Target 2.5 — Actual 1.0
- **Improvements (RS.IM):** Target 2.5 — Actual 1.0
- **Recovery Planning (RC.RP):** Target 2.5 — Actual 1.0

Visual Analysis:

- Overall **target maturity**: 2.5
- Overall **achieved maturity**: approximately 1.1 (as confirmed in "Total Maturity Level" box).
- Strongest performance in **PR.IP (Information Protection Processes and Procedures)** with a 2.5 score.
- Lowest uniform maturity (1.0) across most other categories.

CyberFundamentals Maturity Level — BASIC (Radar Chart Interpretation)

Chart Title

CyberFundamentals Maturity Level BASIC

Legend

- **Green line:** Target Maturity Score
- **Orange line:** Category Maturity Score
- **Gray line:** Documentation Maturity Score
- **Blue line:** Implementation Maturity Score

Axes and Labeled Domains

Each axis corresponds to a **CyberFundamentals Category** as defined in the NIS2-aligned CyberFundamentals Framework.

IDENTIFY

- Asset Management (ID.AM)
- Governance (ID.GV)
- Risk Assessment (ID.RA)
- Identity Management, Authentication and Access Control (PR.AC)

PROTECT

- Awareness and Training (PR.AT)
- Data Security (PR.DS)
- Information Protection Processes and Procedures (PR.IP)
- Maintenance (PR.MA)
- Protective Technology (PR.PT)

DETECT

- Anomalies and Events (DE.AE)
- Security Continuous Monitoring (DE.CM)

RESPOND

- Response Planning (RS.RP)
- Communications (RS.CO)
- Improvements (RS.IM)

RECOVER

- Recovery Planning (RC.RP)

Maturity Level Scale

The radar chart uses a standardized CyberFundamentals scale from **0 to 5**:

- 5 – Optimizing
- 4 – Managed
- 3 – Defined
- 2 – Repeatable

- 1 – Initial
- 0 – Non-existent

Plotted Data Summary (derived from chart and BASIC Summary)

Category	Target Maturity	Category Maturity	Documentation Maturity	Implementation Maturity
Asset Management (ID.AM)	2.50	1.00	1.00	1.00
Governance (ID.GV)	2.50	1.00	1.00	1.00
Risk Assessment (ID.RA)	2.50	1.00	1.00	1.00
Identity Management & Access Control (PR.AC)	2.50	1.00	1.00	1.00
Awareness and Training (PR.AT)	2.50	1.00	1.00	1.00
Data Security (PR.DS)	2.50	1.00	1.00	1.00
Information Protection Processes and Procedures (PR.IP)	2.50	1.00	1.00	1.00
Maintenance (PR.MA)	2.50	1.00	1.00	1.00
Protective Technology (PR.PT)	2.50	1.00	1.00	1.00
Anomalies and Events (DE.AE)	2.50	1.00	1.00	1.00
Security Continuous Monitoring (DE.CM)	2.50	1.00	1.00	1.00
Response Planning (RS.RP)	2.50	1.00	1.00	1.00
Communications (RS.CO)	2.50	1.00	1.00	1.00
Improvements (RS.IM)	2.50	1.00	1.00	1.00
Recovery Planning (RC.RP)	2.50	1.00	1.00	1.00

Observed Pattern in the Radar Chart

- **Target Maturity (green line):** forms an outer circular band around **level 2.5**, indicating that the BASIC level aims for a "Repeatable" state of control implementation across all domains.
- **Category Maturity (orange line):** remains near the **1.0** level, indicating "Initial" maturity, meaning processes exist in some form but are informal and inconsistently applied.
- **Documentation Maturity (gray line)** and **Implementation Maturity (blue line)** nearly overlap, both hovering tightly around **1.0**, forming a small inner circle at the center of the radar graph.
- The graph shows a **notable depression** in the Maintenance (PR.MA) axis, but all categories generally remain at or below the **Initial level (1.0–1.1)**.

Analytical Interpretation (Strictly Based on Chart Data)

The **CyberFundamentals BASIC radar chart** illustrates that the organization's actual maturity remains significantly below the targeted threshold of 2.5 across all functions.

- The **target expectations** (green line) represent the required "Repeatable" maturity state for entities at BASIC assurance level.
- However, the **measured performance** (blue and gray lines) suggests that the organization's cybersecurity posture is still in the **"Initial" stage**, where procedures are mostly undocumented, ad hoc, and dependent on individual effort rather than defined processes.

The radar's **symmetry** (almost circular shape at level 1.0) shows consistent underperformance across all categories — indicating that the gap between documented controls and operational implementation is uniform.

This means:

- **Policies exist conceptually** but lack formalized documentation and procedural enforcement.
- **No category exceeds maturity level 1.1**, showing minimal variation among IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER functions.
- **Target maturity (2.5)** is not met in any domain, suggesting foundational work is still required to reach a repeatable, process-driven security baseline.

Interpretive Summary

The radar chart reflects a **low overall cyber maturity** profile for BASIC level assessment. It conveys that while the organization may understand the required cybersecurity functions conceptually, its actual **execution and documentation** remain at the **Initial stage (level 1)**.

Visually, the chart shows:

- The **Target (green)** ring at level 2.5 forming an external perimeter.
- The **Documentation (gray)** and **Implementation (blue)** lines overlapping near the center at level 1.0, representing early maturity.

This visual and numeric pattern indicates a **uniform capability gap** across all domains — a typical profile for organizations at the start of their CyberFundamentals Framework compliance journey.

_____-

IMPORTANT Details

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Subcategory: ID.AM-1: Physical devices and systems within the organization are inventoried
Requirement: BASIC_ID.AM-1.1: An inventory of assets associated with information and information processing facilities within the organization shall be documented, reviewed, and updated when changes occur.
Guidance: •   This inventory includes fixed and portable computers, tablets, mobile phones, Programmable Logic Controllers (PLCs), sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices.
•   This inventory must include all assets, whether or not they are connected to the organization's network.
•   The use of an IT asset management tool could be considered.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Requirement: ID.AM-1.2: The inventory of assets associated with information and information processing facilities shall reflect changes in the organization's context and include all information necessary for effective accountability.
Guidance: •   Inventory specifications include for example, manufacturer, device type, model, serial number, machine names and network addresses, physical location…
•   Accountability is the obligation to explain, justify, and take responsibility for one's actions, it implies answerability for the outcome of the task or process.
•   Changes include the decommissioning of material.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Requirement: ID.AM-1.3: When unauthorized hardware is detected, it shall be quarantined for possible exception handling, removed, or replaced, and the inventory shall be updated accordingly.
Guidance: •   Any unsupported hardware without an exception documentation, is designated as unauthorized.
•   Unauthorized hardware can be detected during inventory, requests for support by the user or other means.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Subcategory: ID.AM-2: Software platforms and applications within the organization are inventoried
Requirement: BASIC_ID.AM-2.1: An inventory that reflects what software platforms and applications are being used in the organization shall be documented, reviewed, and updated when changes occur.
Guidance: •   This inventory includes software programs, software platforms and databases, even if outsourced (SaaS).
•   Outsourcing arrangements should be part of the contractual agreements with the provider.
•   Information in the inventory should include for example: name, description, version, number of users, data processed, etc.
•   A distinction should be made between unsupported software and unauthorized software.
•   The use of an IT asset management tool could be considered.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

Requirement: ID.AM-2.2: The inventory of software platforms and applications associated with information and information processing shall reflect changes in the organization's context and include all information necessary for effective accountability.
Guidance: The inventory of software platforms and applications should include the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Requirement: ID.AM-2.3: Individuals who are responsible and who are accountable for administering software platforms and applications within the organization shall be identified.
Guidance: There are no additional guidelines.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Requirement: ID.AM-2.4: When unauthorized software is detected, it shall be quarantined for possible exception handling, removed, or replaced, and the inventory shall be updated accordingly.
Guidance: •   Any unsupported software without an exception documentation, is designated as unauthorized.
•   Unauthorized software can be detected during inventory, requests for support by the user or other means.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their

relative importance to organizational objectives and the organization's risk strategy.
Subcategory: ID.AM-3: Organizational communication and data flows are mapped
Requirement: BASIC_ID.AM-3.1: Information that the organization stores and uses shall be identified.
Guidance: •   Start by listing all the types of information your business stores or uses. Define "information type" in any useful way that makes sense to your business. You may want to have your employees make a list of all the information they use in their regular activities. List everything you can think of, but you do not need to be too specific. For example, you may keep customer names and email addresses, receipts for raw material, your banking information, or other proprietary information.
•   Consider mapping this information with the associated assets identified in the inventories of physical devices, systems, software platforms and applications used within the organization (see ID.AM-1 & ID.AM-2).
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Requirement: ID.AM-3.2: All connections within the organization's ICT/OT environment, and to other organization-internal platforms shall be mapped, documented, approved, and updated as appropriate.
Guidance: •   Connection information includes, for example, the interface characteristics, data characteristics, ports, protocols, addresses, description of the data, security requirements, and the nature of the connection.
•   Configuration management can be used as supporting asset.
•   This documentation should not be stored only on the network it represents.
•   Consider keeping a copy of this documentation in a safe offline environment (e.g. offline hard disk, paper hardcopy, …)
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their

relative importance to organizational objectives and the organization's risk strategy.
Subcategory: ID.AM-4: External information systems are catalogued
Requirement: ID.AM-4.1: The organization shall map, document, authorize and when changes occur, update, all external services and the connections made with them.
Guidance: •   Outsourcing of systems, software platforms and applications used within the organization is covered in ID.AM-1 & ID.AM-2
•   External information systems are systems or components of systems for which organizations typically have no direct supervision and authority over the application of security requirements and controls, or the determination of the effectiveness of implemented controls on those systems i.e., services that are run in cloud, SaaS, hosting or other external environments, API (Application Programming Interface)…
•   Mapping external services and the connections made to them and authorizing them in advance avoids wasting unnecessary resources investigating a supposedly non-authenticated connection to external systems.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Subcategory: ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
Requirement: BASIC_ID.AM-5.1: The organization's resources (hardware, devices, data, time, personnel, information, and software) shall be prioritized based on their classification, criticality, and business value.
Guidance: •   Determine organization's resources (e.g., hardware, devices, data, time, personnel, information, and software):
o   What would happen to my business if these resources were made public, damaged, lost…?
o   What would happen to my business when the integrity of resources is no longer guaranteed?
o   What would happen to my business if I/my customers couldn't access these resources? And rank these resources based on their classification, criticality, and business value.
•   Resources should include enterprise assets.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1

Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Guidance: •   Create a classification for sensitive information by first determining categories, e.g.
o   Public - freely accessible to all, even externally
o   Internal - accessible only to members of your organization
o   Confidential - accessible only to those whose duties require access.
•   Communicate these categories and identify what types of data fall into these categories (HR data, financial data, legal data, personal data, etc.).
•   Consider the use of the Traffic Light Protocol (TLP).
•   Data classification should apply to the three aspects: C-I-A.

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Key Measure: Key Measure
Subcategory: ID.AM-6: Cybersecurity roles, responsibilities, and authorities for the entire workforce and third-party stakeholders are established
Requirement: ID.AM-6.1: Information security and cybersecurity roles, responsibilities and authorities within the organization shall be documented, reviewed, authorized, and updated and alignment with organization-internal roles and external partners.
Guidance: It should be considered to:
•   Describe security roles, responsibilities, and authorities: who in your organization should be consulted, informed, and held accountable for all or part of your assets.
•   Provide security roles, responsibilities, and authority for all key functions in information/cyber security (legal, detection activities…).
•   Include information/cybersecurity roles and responsibilities for third-party providers (e.g., suppliers, customers, partners) with physical or logical access to the organization's ICT/OT environment.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
Subcategory: ID.BE-1: The organization's role in the supply chain is identified and communicated
Requirement: ID.BE-1.1: The organization's role in the supply chain shall be identified, documented, and communicated.
Guidance: •   The organisation should be able to clearly identify who is upstream and downstream of the organisation and which suppliers provide services, capabilities, products and items to the organisation.
•   The organisation should communicate its position to its upstream and downstream so that it is understood where they sit in terms of critical importance to the organisation's operations.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
Subcategory: ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated
Requirement: ID.BE-2.1: The organization's place in critical infrastructure and its industry sector shall be identified and communicated.
Guidance: The organisation covered by NIS legislation has a responsibility to know the other organisations in the same sector in order to work with them to achieve the objectives set by NIS for that particular sector.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and

prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
Subcategory: ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
Requirement: ID.BE-3.1: Priorities for organizational mission, objectives, and activities are established and communicated.
Guidance: Information protection needs should be determined, and the related processes revised as necessary.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
Subcategory: ID.BE-4: Dependencies and critical functions for delivery of critical services are established
Requirement: ID.BE-4.1: Dependencies and mission-critical functions for the delivery of critical services shall be identified, documented, and prioritized according to their criticality as part of the risk assessment process.
Guidance: Dependencies and business critical functions should include support services.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
Subcategory: ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)
Requirement: ID.BE-5.1: To support cyber resilience and secure the delivery of critical services, the necessary requirements are identified, documented and their implementation tested and approved.
Guidance: •   Consider implementing resiliency mechanisms to support normal and adverse operational situations (e.g., failsafe, load balancing, hot swap).
•   Consider aspects of business continuity management in e.g. Business Impact Analyse (BIA), Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP).

Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
Subcategory: ID.GV-1: Organizational cybersecurity policy is established and communicated
Requirement: BASIC_ID.GV-1.1: Policies and procedures for information security and cyber security shall be created, documented, reviewed, approved, and updated when changes occur.
Guidance: •   Policies and procedures used to identify acceptable practices and expectations for business operations, can be used to train new employees on your information security expectations, and can aid an investigation in case of an incident. These policies and procedures should be readily accessible to employees.
•   Policies and procedures for information- and cybersecurity should clearly describe your expectations for protecting the organization's information and systems, and how management expects the company's resources to be used and protected by all employees.
•   Policies and procedures should be reviewed and updated at least annually and every time there are changes in the organization or technology. Whenever the policies are changed, employees should be made aware of the changes.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
Requirement: ID.GV-1.2: An organization-wide information security and cybersecurity policy shall be established, documented, updated when changes occur, disseminated, and approved by senior management.
Guidance: The policy should include, for example:
•   The identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Guidance on role profiles along with their identified titles, missions, tasks, skills, knowledge, competences is available

in the "European Cybersecurity Skills Framework Role Profiles" by
ENISA. (https://www.enisa.europa.eu/publications/european-
cybersecurity-skills-framework-role-profiles)
•   The coordination among organizational entities responsible for
the different aspects of security (i.e., technical, physical,
personnel, cyber-physical, information, access control, media
protection, vulnerability management, maintenance, monitoring)
•   The coverage of the full life cycle of the ICT/OT systems.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Governance (ID.GV): The policies, procedures, and processes
to manage and monitor the organization's regulatory, legal, risk,
environmental, and operational requirements are understood and inform
the management of cybersecurity risk.
Subcategory: ID.GV-3: Legal and regulatory requirements regarding
cybersecurity, including privacy and civil liberties obligations, are
understood and managed
Requirement: BASIC_ID.GV-3.1: Legal and regulatory requirements
regarding information/cybersecurity, including privacy obligations,
shall be understood and implemented.
Guidance: There are no additional guidelines.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Governance (ID.GV): The policies, procedures, and processes
to manage and monitor the organization's regulatory, legal, risk,
environmental, and operational requirements are understood and inform
the management of cybersecurity risk.
Requirement: ID.GV-3.2: Legal and regulatory requirements regarding
information/cybersecurity, including privacy obligations, shall be
managed.
Guidance: •   There should be regular reviews to ensure the
continuous compliance with legal and regulatory requirements regarding
information/cybersecurity, including privacy obligations.
•   This requirement also applies to contractors and service
providers.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)

Category: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
Subcategory: ID.GV-4: Governance and risk management processes address cybersecurity risks
Requirement: BASIC_ID.GV-4.1: As part of the company's overall risk management, a comprehensive strategy to manage information security and cybersecurity risks shall be developed and updated when changes occur.
Guidance: This strategy should include determining and allocating the required resources to protect the organisation's business-critical assets.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
Requirement: ID.GV-4.2: Information security and cybersecurity risks shall be documented, formally approved, and updated when changes occur.
Guidance: Consider using Risk Management tools.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
Subcategory: ID.RA-1: Asset vulnerabilities are identified and documented
Requirement: BASIC_ID.RA-1.1: Threats and vulnerabilities shall be identified.
Guidance: •   A vulnerability refers to a weakness in the organization's hardware, software, or procedures. It is a gap through which a bad actor can gain access to the organization's assets. A vulnerability exposes an organization to threats.
•   A threat is a malicious or negative event that takes advantage of a vulnerability.
•   The risk is the potential for loss and damage when the threat does occur.
Documentation Score: 1

Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Risk Assessment (ID.RA): The organization understands the
cybersecurity risk to organizational operations (including mission,
functions, image, or reputation), organizational assets, and
individuals.
Requirement: ID.RA-1.2: A process shall be established to monitor,
identify, and document vulnerabilities of the organisation's business
critical systems in a continuous manner.
Guidance: •   Where safe and feasible, the use of vulnerability
scanning should be considered.
•   The organization should establish and maintain a testing program
appropriate to its size, complexity, and maturity.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Risk Assessment (ID.RA): The organization understands the
cybersecurity risk to organizational operations (including mission,
functions, image, or reputation), organizational assets, and
individuals.
Subcategory: ID.RA-2: Cyber threat intelligence is received from
information sharing forums and sources
Requirement: ID.RA-2.1: A threat and vulnerability awareness program
that includes a cross-organization information-sharing capability
shall be implemented.
Guidance: A threat and vulnerability awareness program should include
ongoing contact with security groups and associations to receive
security alerts and advisories. (Security groups and associations
include, for example, special interest groups, forums, professional
associations, news groups, and/or peer groups of security
professionals in similar organizations).This contact can include the
sharing of information about potential vulnerabilities and incidents.
This sharing capability should have an unclassified and classified
information sharing capability.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)

Category: Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
Subcategory: ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
Requirement: BASIC_ID.RA-5.1: The organization shall conduct risk assessments in which risk is determined by threats, vulnerabilities and impact on business processes and assets.
Guidance: •   Keep in mind that threats exploit vulnerabilities.
•   Identify the consequences that losses of confidentiality, integrity and availability may have on the assets and related business processes.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
Requirement: ID.RA-5.2: The organization shall conduct and document risk assessments in which risk is determined by threats, vulnerabilities, impact on business processes and assets, and the likelihood of their occurrence.
Guidance: •   Risk assessment should include threats from insiders and external parties.
•   Qualitative and/or quantitative risk analysis methods (MAPGOOD, ISO27005, CIS RAM, …) can be used together with software tooling.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
Subcategory: ID.RA-6: Risk responses are identified and prioritized
Requirement: ID.RA-6.1: A comprehensive strategy shall be developed and implemented to manage risks to the organization's critical systems, that includes the identification and prioritization of risk responses.
Guidance: •   Management and employees should be involved in information- and cybersecurity.

- It should be identified what the most important assets are, and how they are protected.
- It should be clear what impact will be if these assets are compromised.
- It should be established how the implementation of adequate mitigation measures will be organized.

Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
Subcategory: ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders
Requirement: ID.RM-1.1: A cyber risk management process that identifies key internal and external stakeholders and facilitates addressing risk-related issues and information shall be created, documented, reviewed, approved, and updated when changes occur.
Guidance: External stakeholders include customers, investors and shareholders, suppliers, government agencies and the wider community.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
Subcategory: ID.RM-2: Organizational risk tolerance is determined and clearly expressed
Requirement: ID.RM-2.1: The organization shall clearly determine it's risk appetite.
Guidance: Determination and expression of risk tolerance (risk appetite) should be in line with the policies on information security and cybersecurity, to facilitate demonstration of coherence between policies, risk tolerance and measures.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Risk Management Strategy (ID.RM): The organization's
priorities, constraints, risk tolerances, and assumptions are
established and used to support operational risk decisions.
Subcategory: ID.RM-3: The organization's determination of risk
tolerance is informed by its role in critical infrastructure and
sector specific risk analysis
Requirement: ID.RM-3.1: The organization's role in critical
infrastructure and its sector shall determine the organization's risk
appetite.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Supply Chain Risk Management (ID.SC):
The organization's priorities, constraints, risk tolerances, and
assumptions are established and used to support risk decisions
associated with managing supply chain risk. The organization has
established and implemented the processes to identify, assess and
manage supply chain risks.
Subcategory: ID.SC-2: Suppliers and third party partners of
information systems, components, and services are identified,
prioritized, and assessed using a cyber supply chain risk assessment
process
Requirement: ID.SC-2.1: The organization shall conduct cyber supply
chain risk assessments at least annually or when a change to the
organization's critical systems, operational environment, or supply
chain occurs; These assessments shall be documented, and the results
disseminated to relevant stakeholders including those responsible for
ICT/OT systems.
Guidance: This assessment should identify and prioritize potential
negative impacts to the organization from the risks associated with
the distributed and interconnected nature of ICT/OT product and
service supply chains.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Supply Chain Risk Management (ID.SC):

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

Subcategory: ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.

Requirement: ID.SC-3.1: Based on the results of the cyber supply chain risk assessment, a contractual framework for suppliers and external partners shall be established to address sharing of sensitive information and distributed and interconnected ICT/OT products and services.

Guidance: •   Entities not subject to the NIS legislation should consider business critical suppliers and third-party partners only.
•   Keep in mind that GDPR requirements need to be fulfilled when business information contains personal data (applicable on all levels), i.e. security measures need to be addressed in the contractual framework.

Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Supply Chain Risk Management (ID.SC):
The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

Subcategory: ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.

Requirement: ID.SC-4.1: The organization shall review assessments of suppliers' and third-party partner's compliance with contractual obligations by routinely reviewing audits, test results, and other evaluations.

Guidance: Entities not subject to the NIS legislation could limit themselves to business critical suppliers and third-party partners only.

Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)

Category: Supply Chain Risk Management (ID.SC):
The organization's priorities, constraints, risk tolerances, and
assumptions are established and used to support risk decisions
associated with managing supply chain risk. The organization has
established and implemented the processes to identify, assess and
manage supply chain risks.
Subcategory: ID.SC-5: Response and recovery planning and testing are
conducted with suppliers and third-party providers
Requirement: ID.SC-5.1: The organization shall identify and document
key personnel from suppliers and third-party partners to include them
as stakeholders in response and recovery planning activities.
Guidance: Entities not subject to the NIS legislation could limit
themselves to business critical suppliers and third-party partners
only.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Key Measure: Key Measure
Subcategory: PR.AC-1: Identities and credentials are issued, managed,
verified, revoked, and audited for authorized devices, users and
processes
Requirement: BASIC_PR.AC-1.1: Identities and credentials for
authorized devices and users shall be managed.

Guidance: Identities and credentials for authorized devices and users
could be managed through a password policy. A password policy is a set
of rules designed to enhance ICT/OT security by encouraging
organization's to:
(Not limitative list and measures to be considered as appropriate)
•   Change all default passwords.
•   Ensure that no one works with administrator privileges for daily
tasks.
•   Keep a limited and updated list of system administrator accounts.
•   Enforce password rules, e.g. passwords must be longer than a
state-of-the-art number of characters with a combination of character
types and changed periodically or when there is any suspicion of
compromise.
•   Use only individual accounts and never share passwords.
•   Immediately disable unused accounts
•   Rights and privileges are managed by user groups.
Documentation Score: 1
Implementation Score: 1

Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Requirement: PR.AC-1.2: Identities and credentials for authorized
devices and users shall be managed, where feasible through automated
mechanisms.
Guidance: •   Automated mechanisms can help to support the
management and auditing of information system credentials.
•   Consider strong user authentication, meaning an authentication
based on the use of at least two authentication factors from different
categories of either knowledge (something only the user knows),
possession (something only the user possesses) or inherence (something
the user is) that are independent, in that the breach of one does not
compromise the reliability of the others, and is designed in such a
way to protect the confidentiality of the authentication data.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Subcategory: PR.AC-2: Physical access to assets is managed and
protected
Requirement: BASIC_PR.AC-2.1: Physical access to the facility, servers
and network components shall be managed.
Guidance: •   Consider to strictly manage keys to access the
premises and alarm codes. The following rules should be considered:
o   Always retrieve an employee's keys or badges when they leave the
company permanently.
o   Change company alarm codes frequently.
o   Never give keys or alarm codes to external service providers
(cleaning agents, etc.), unless it is possible to trace these accesses
and restrict them technically to given time slots.
•   Consider to not leaving internal network access outlets
accessible in public areas. These public places can be waiting rooms,
corridors...
Documentation Score: 1

Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Requirement: PR.AC-2.2: The management of physical access shall include measures related to access in emergency situations.
Guidance: •   Physical access controls may include, for example: lists of authorized individuals, identity credentials, escort requirements, guards, fences, turnstiles, locks, monitoring of facility access, camera surveillance.
•   The following measures should be considered:
o   Implement a badge system and create different security zones.
o   Limit physical access to servers and network components to authorized personnel.
o   Log all access to servers and network components.
•   Visitor access records should be maintained, reviewed and acted upon as required.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Subcategory: PR.AC-3: Remote access is managed
Requirement: BASIC_PR.AC-3.1: The organisation's wireless access points shall be secured.
Guidance: Consider the following when wireless networking is used:
•   Change the administrative password upon installation of a wireless access points.
•   Set the wireless access point so that it does not broadcast its Service Set Identifier (SSID).
•   Set your router to use at least WiFi Protected Access (WPA-2 or WPA-3 where possible), with the Advanced Encryption Standard (AES) for encryption.
•   Ensure that wireless internet access to customers is separated from your business network.
•   Connecting to unknown or unsecured / guest wireless access points, should be avoided, and if unavoidable done through an encrypted virtual private network (VPN) capability.

• Manage all endpoint devices (fixed and mobile) according to the organization's security policies.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Key Measure: Key Measure
Requirement: BASIC_PR.AC-3.2: The organization's networks when accessed remotely shall be secured, including through multi-factor authentication (MFA).
Guidance: Enforce MFA (e.g. 2FA) on Internet-facing systems, such as email, remote desktop, and Virtual Private Network (VPNs).
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Key Measure: Key Measure
Requirement: PR.AC-3.3: Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization's critical systems environment shall be identified, documented and implemented.
Guidance: Consider the following:
• Remote access methods include, for example, wireless, broadband, Virtual Private Network (VPN) connections, mobile device connections, and communications through external networks.
• Login credentials should be in line with company's user authentication policies.
• Remote access for support activities or maintenance of organizational assets should be approved, logged, and performed in a manner that prevents unauthorized access.
• The user should be made aware of any remote connection to its device by a visual indication.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Key Measure: Key Measure
Subcategory: PR.AC-4: Access permissions and authorizations are
managed, incorporating the principles of least privilege and
separation of duties
Requirement: BASIC_PR.AC-4.1: Access permissions for users to the
organization's systems shall be defined and managed.
Guidance: The following should be considered:
•   Draw up and review regularly access lists per system (files,
servers, software, databases, etc.), possibly through analysis of the
Active Directory in Windows-based systems, with the objective of
determining who needs what kind of access (privileged or not), to
what, to perform their duties in the organization.
•   Set up a separate account for each user (including any
contractors needing access) and require that strong, unique passwords
be used for each account.
•   Ensure that all employees use computer accounts without
administrative privileges to perform typical work functions. This
includes separation of personal and admin accounts.
•   For guest accounts, consider using the minimal privileges (e.g.
internet access only) as required for your business needs.
•   Permission management should be documented in a procedure and
updated when appropriate.
•   Use 'Single Sign On' (SSO) when appropriate.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Key Measure: Key Measure
Requirement: BASIC_PR.AC-4.2: It shall be identified who should have
access to the organization's business's critical information and
technology and the means to get access.
Guidance: Means to get access may include: a key, password, code, or
administrative privilege.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Key Measure: Key Measure
Requirement: BASIC_PR.AC-4.3: Employee access to data and information
shall be limited to the systems and specific information they need to
do their jobs (the principle of Least Privilege).

Guidance: The principle of Least Privilege should be understood as the
principle that a security architecture should be designed so that each
employee is granted the minimum system resources and authorizations
that the employee needs to perform its function. Consider to:
•   Not allow any employee to have access to all the business's
information.
•   Limit the number of Internet accesses and interconnections with
partner networks to the strict necessary to be able to centralize and
homogenize the monitoring of exchanges more easily.
•   Ensure that when an employee leaves the business, all access to
the business's information or systems is blocked instantly.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Key Measure: Key Measure
Requirement: BASIC_PR.AC-4.4: Nobody shall have administrator
privileges for daily tasks.

Guidance: Consider the following:
•   Separate administrator accounts from user accounts.
•   Do not privilege user accounts to effectuate administration
tasks.
•   Create unique local administrator passwords and disable unused
accounts.
•   Consider prohibiting Internet browsing from administrative
accounts.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Requirement: PR.AC-4.5: Where feasible, automated mechanisms shall be implemented to support the management of user accounts on the organisation's critical systems, including disabling, monitoring, reporting and deleting user accounts.
Guidance: Consider separately identifying each person with access to the organization's critical systems with a username to remove generic and anonymous accounts and access.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Requirement: PR.AC-4.6: Separation of duties (SoD) shall be ensured in the management of access rights.
Guidance: Separation of duties includes, for example:
•   dividing operational functions and system support functions among different roles.
•   conducting system support functions with different individuals.
•   not allow a single individual to both initiate and approve a transaction (financial or otherwise).
•   ensuring that security personnel administering access control functions do not also administer audit functions.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Requirement: PR.AC-4.7: Priviliged users shall be managed and monitored.
Guidance: There are no additional guidelines.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Key Measure: Key Measure
Subcategory: PR.AC-5: Network integrity is protected (e.g., network
segregation, network segmentation)
Requirement: BASIC_PR.AC-5.1: Firewalls shall be installed and
activated on all the organization's networks.
Guidance: Consider the following:
•   Install and operate a firewall between your internal network and
the Internet. This may be a function of a (wireless) access
point/router, or it may be a function of a router provided by the
Internet Service Provider (ISP).
•   Ensure there is antivirus software installed on purchased
firewall solutions and ensure that the administrator's log-in and
administrative password is changed upon installation and regularly
thereafter.
•   Install, use, and update a software firewall on each computer
system (including smart phones and other networked devices).
•   Have firewalls on each of your computers and networks even if you
use a cloud service provider or a virtual private network (VPN).
Ensure that for telework home network and systems have hardware and
software firewalls installed, operational, and regularly updated.
•   Consider installing an Intrusion Detection / Prevention System
(IDPS). These devices analyze network traffic at a more detailed level
and can provide a greater level of protection.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Key Measure: Key Measure
Requirement: BASIC_PR.AC-5.2: Where appropriate, network integrity of
the organization's critical systems shall be protected by
incorporating network segmentation and segregation.
Guidance: •   Consider creating different security zones in the
network (e.g. Basic network segmentation through VLAN's or other
network access control mechanisms) and control/monitor the traffic
between these zones.

• When the network is "flat", the compromise of a vital network component can lead to the compromise of the entire network.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Key Measure: Key Measure
Requirement: PR.AC-5.3: Where appropriate, network integrity of the organization's critical systems shall be protected by
(1) Identifying, documenting, and controlling connections between system components.
(2) Limiting external connections to the organization's critical systems.
Guidance: Boundary protection mechanisms include, for example, routers, gateways, unidirectional gateways, data diodes, and firewalls separating system components into logically separate networks or subnetworks.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Key Measure: Key Measure
Requirement: PR.AC-5.4: The organization shall monitor and control connections and communications at the external boundary and at key internal boundaries within the organization's critical systems by implementing boundary protection devices where appropriate.
Guidance: Consider implementing the following recommendations:
• Separate your public WIFI network from your business network.
• Protect your business WIFI with state-of-the-art encryption.
• Implement a Network Access Control (NAC) solution.
• Encrypt connections to your corporate network.
• Divide your network according to security levels and apply firewall rules. Isolate your networks for server administration.
• Force VPN on public networks.
• Implement a closed policy for security gateways (deny all policy: only allow/open connections that have been explicitly pre-authorized).
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Subcategory: PR.AC-6: Identities are proofed and bound to credentials
and asserted in interactions
Requirement: PR.AC-6.1: The organization shall implement documented
procedures for verifying the identity of individuals before issuing
credentials that provide access to organization's systems.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Subcategory: PR.AC-7: Users, devices, and other assets are
authenticated (e.g., single-factor, multi-factor) commensurate with
the risk of the transaction (e.g., individuals' security and privacy
risks and other organizational risks)
Requirement: PR.AC-7.1: The organization shall perform a documented
risk assessment on organization's critical system transactions and
authenticate users, devices, and other assets (e.g., single-factor,
multi-factor) commensurate with the risk of the transaction (e.g.,
individuals' security and privacy risks and other organizational
risks).
Guidance: Consider a security-by-design approach for new systems; For
existing systems a separate risk assessment should be used.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Awareness and Training (PR.AT): The organization's personnel
and partners are provided cybersecurity awareness education and are
trained to perform their cybersecurity-related duties and

responsibilities consistent with related policies, procedures, and agreements.
Subcategory: PR.AT-1: All users are informed and trained
Requirement: BASIC_PR.AT-1.1: Employees shall be trained as appropriate.
Guidance: •   Employees include all users and managers of the ICT/OT systems, and they should be trained immediately when hired and regularly thereafter about the company's information security policies and what they will be expected to do to protect company's business information and technology.
•   Training should be continually updated and reinforced by awareness campaigns.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
Requirement: PR.AT-1.2: The organization shall incorporate insider threat recognition and reporting into security awareness training.
Guidance: Consider to:
•   Communicate and discuss regularly to ensure that everyone is aware of their responsibilities.
•   Develop an outreach program by gathering in a document the messages you want to convey to your staff (topics, audiences, objectives, etc.) and your communication rhythm on a calendar (weekly, monthly, one-time, etc.). Communicate continuously and in an engaging way, involving management, IT colleagues, the ICT service provider and HR and Communication managers.
•   Cover topics such as: recognition of fraud attempts, phishing, management of sensitive information, incidents, etc. The goal is for all employees to understand ways to protect company information.
•   Discuss with your management, your ICT colleagues, or your ICT service provider some practice scenarios (e.g. what to do if a virus alert is triggered, if a storm cuts off the power, if data is blocked, if an account is hacked, etc.), determine what behaviours to adopt, document and communicate them to all your staff. The central point of contact in the event of an incident should be known to all.
•   Organize a simulation of a scenario to test your knowledge. Consider performing the exercise for example at least once a year.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
Subcategory: PR.AT-2: Privileged users understand their roles and responsibilities
Requirement: PR.AT-2.1: Privileged users shall be qualified before privileges are granted, and these users shall be able to demonstrate the understanding of their roles, responsibilities, and authorities.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
Subcategory: PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
Requirement: PR.AT-3.1: The organization shall establish and enforce security requirements for business-critical third-party providers and users.
Guidance: Enforcement should include that 'third party stakeholder'-users (e.g. suppliers, customers, partners) can demonstrate the understanding of their roles and responsibilities.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
Requirement: PR.AT-3.2: Third-party providers shall be required to notify any personnel transfers, termination, or transition involving personnel with physical or logical access to organization's business critical system's components.

Guidance: Third-party providers include, for example, service providers, contractors, and other organizations providing system development, technology services, outsourced applications, or network and security management.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
Requirement: PR.AT-3.3:The organization shall monitor business critical service providers and users for security compliance.
Guidance: Third party audit results can be used as audit evidence.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
Subcategory: PR.AT-4: Senior executives understand their roles and responsibilities
Requirement: PR.AT-4.1: Senior executives shall demonstrate the understanding of their roles, responsibilities, and authorities.
Guidance: Guidance on role profiles along with their identified titles, missions, tasks, skills, knowledge, competences is available in the "European Cybersecurity Skills Framework Role Profiles" by ENISA. (https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles)
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

Subcategory: PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities
Requirement: PR.AT-5.1: The organization shall ensure that personnel responsible for the physical protection and security of the organization's critical systems and facilities are qualified through training before privileges are granted, and that they understand their responsibilities.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Subcategory: PR.DS-1: Data-at-rest is protected
Requirement: NO REQUIREMENT / This control is covered by other elements of the framework; no additional requirements are identified. Covered in PR.AC-4 / Guidance to be considered
Guidance: •   Consider using encryption techniques for data storage, data transmission or data transport (e.g., laptop, USB).
•   Consider encrypting end-user devices and removable media containing sensitive data (e.g. hard disks, laptops, mobile device, USB storage devices, …). This could be done by e.g. Windows BitLocker®, VeraCrypt, Apple FileVault®, Linux® dm-crypt,…
•   Consider encrypting sensitive data stored in the cloud.
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Subcategory: PR.DS-2: Data-in-transit is protected
Requirement: NO REQUIREMENT / This control is covered by other elements of the framework; no additional requirements are identified. Covered in PR.DS-1 / Guidance to be considered
Guidance: When the organization often sends sensitive documents or e-mails, it is recommended to encrypt those documents and/or e-mails with appropriate, supported, and authorized software tools.

Function: PROTECT (PR)

Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Subcategory: PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
Requirement: BASIC_PR.DS-3.1: Assets and media shall be disposed of safely.
Guidance: •   When eliminating tangible assets like business computers/laptops, servers, hard drive(s) and other storage media (USB drives, paper…), ensure that all   sensitive business or personal data are securely deleted (i.e. electronically "wiped") before they are removed and then physically destroyed (or re-commissioned). This is also known as "sanitization" and thus related to the requirement and guidance in PR.IP-6.
•   Consider installing a remote-wiping application on company laptops, tablets, cell phones, and other mobile devices.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Requirement: PR.DS-3.2: The organization shall enforce accountability for all its business-critical assets throughout the system lifecycle, including removal, transfers, and disposition.
Guidance: Accountability should include:
•   The authorization for business-critical assets to enter and exit the facility.
•   Monitoring and maintaining documentation related to the movements of business-critical assets.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Requirement: PR.DS-3.3: The organization shall ensure that the necessary measures are taken to deal with loss, misuse, damage, or theft of assets.
Guidance: This can be done by policies, processes & procedures (reporting), technical & organizational means (encryption, Access Control (AC), Mobile Device Management (MDM), monitoring, secure wipe, awareness, signed user agreement, guidelines & manuals, backups, inventory update …).

Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Subcategory: PR.DS-4: Adequate capacity to ensure availability is maintained
Requirement: PR.DS-4.1: Capacity planning shall ensure adequate resources for organization's critical system information processing, networking, telecommunications, and data storage.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Requirement: PR.DS-4.2: Audit data from the organization's critical systems shall be moved to an alternative system.
Guidance: Be aware that log services can become a bottleneck and hinder the correct functioning of the source systems.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Key Measure: Key Measure
Subcategory: PR.DS-5: Protections against data leaks are implemented
Requirement: PR.DS-5.1: The organization shall take appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorized access and activities, including data leakage, is detected.
Guidance: •   Consider implementing dedicated protection measures (restricted access rights, daily backups, data encryption, installation of firewalls, etc.) for the most sensitive data.
•   Consider frequent audit of the configuration of the central directory (Active Directory in Windows environment), with specific focus on the access to data of key persons in the company.
Documentation Score: 1

Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are
managed consistent with the organization's risk strategy to protect
the confidentiality, integrity, and availability of information.
Subcategory: PR.DS-6: Integrity checking mechanisms are used to verify
software, firmware, and information integrity
Requirement: PR.DS-6.1: The organization shall implement software,
firmware, and information integrity checks to detect unauthorized
changes to its critical system components during storage, transport,
start-up and when determined necessary.
Guidance: State-of-the-practice integrity-checking mechanisms (e.g.,
parity checks, cyclical redundancy checks, cryptographic hashes) and
associated tools can automatically monitor the integrity of
information systems and hosted applications.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are
managed consistent with the organization's risk strategy to protect
the confidentiality, integrity, and availability of information.
Subcategory: PR.DS-7: The development and testing environment(s) are
separate from the production environment
Requirement: NO REQUIREMENT / Guidance to be considered
Guidance: •   Any change one wants to make to the ICT/OT environment
should first be tested in an environment that is different and
separate from the production environment (operational environment)
before that change is effectively implemented . That way, the effect
of those changes can be analysed and adjustments can be made without
disrupting operational activities.
•   Consider adding and testing cybersecurity features as early as
during development (secure development lifecycle principles).

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP):
Security policies (that address purpose, scope, roles,
responsibilities, management commitment, and coordination among
organizational entities), processes, and procedures are maintained and
used to manage protection of information systems and assets.

Key Measure: Key Measure
Subcategory: PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
Requirement: PR.IP-1.1: The organization shall develop, document, and maintain a baseline configuration for the its business critical systems.
Guidance: •   This control includes the concept of least functionality.
•   Baseline configurations include for example, information about organization's business critical systems, current version numbers and patch information on operating systems and applications, configuration settings/parameters, network topology, and the logical placement of those components within the system architecture.
•   Network topology should include the nerve points of the IT/OT environment (external connections, servers hosting data and/or sensitive functions, DNS services security, etc.).
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Subcategory: PR.IP-2: A System Development Life Cycle to manage systems is implemented
Requirement: PR.IP-2.1: The system and application development life cycle shall include security considerations.
Guidance: •   System and application development life cycle should include the acquisition process of the organization's business critical systems and its components.
•   Vulnerability awareness and prevention training for (web application) developers, and advanced social engineering awareness training for high-profile roles should be considered.
•   When hosting internet facing applications the implementation of a web application firewall (WAF) should be considered.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Subcategory: PR.IP-3: Configuration change control processes are in place
Requirement: PR.IP-3.1: Changes shall be tested and validated before being implemented into operational systems.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Key Measure: Key Measure
Subcategory: PR.IP-4: Backups of information are conducted, maintained, and tested
Requirement: BASIC_PR.IP-4.1: Backups for organization's business critical data shall be conducted and stored on a system different from the device on which the original data resides.
Guidance: •   Organization's business critical system's data includes for example software, configurations and settings, documentation, system configuration data including computer configuration backups, application configuration backups, etc.
•   Consider a regular backup and put it offline periodically.
•   Recovery time and recovery point objectives should be considered.
•   Consider not storing the organization's data backup on the same network as the system on which the original data resides and provide an offline copy. Among other things, this prevents file encryption by hackers (risk of ransomware).
Documentation Score: 1

Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP):
Security policies (that address purpose, scope, roles,
responsibilities, management commitment, and coordination among
organizational entities), processes, and procedures are maintained and
used to manage protection of information systems and assets.

Requirement: PR.IP-4.2: The reliability and integrity of backups shall
be verified and tested on regular basis.
Guidance: This should include regularly testing of the backup restore
procedures.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP):
Security policies (that address purpose, scope, roles,
responsibilities, management commitment, and coordination among
organizational entities), processes, and procedures are maintained and
used to manage protection of information systems and assets.

Requirement: PR.IP-4.3: A separate alternate storage site for system backups shall be operated and the same security safeguards as the primary storage location shall be employed.
Guidance: An offline backup of your data is ideally stored in a separate physical location from the original data source and where feasible offsite for extra protection and security.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Subcategory: PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met
Requirement: PR.IP-5.1: The organization shall define, implement, and enforce policy and procedures regarding emergency and safety systems, fire protection systems, and environment controls for its critical systems.
Guidance: The below measures should be considered:
•   Protect unattended computer equipment with padlocks or a locker and key system.
•   Fire suppression mechanisms should take the organization's critical system environment into account (e.g., water sprinkler systems could be hazardous in specific environments).

Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP):
Security policies (that address purpose, scope, roles,
responsibilities, management commitment, and coordination among
organizational entities), processes, and procedures are maintained and
used to manage protection of information systems and assets.

Subcategory: PR.IP-6: Data is destroyed according to policy
Requirement: PR.IP-6.1: The organization shall ensure that its
critical system's data is destroyed according to policy.
Guidance: •   Disposal actions include media sanitization actions
(See PR.DS-3)
•   There are two primary types of media in common use:
o   Hard copy media (physical representations of information)
o   Electronic or soft copy media (the bits and bytes contained in
hard drives, random access memory (RAM), read-only memory (ROM),
disks, memory devices, phones, mobile computing devices, networking
equipment…)
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP):
Security policies (that address purpose, scope, roles,
responsibilities, management commitment, and coordination among

organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Subcategory: PR.IP-7: Protection processes are improved
Requirement: PR.IP-7.1: The organization shall incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into protection process updates (continuous improvement).
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Subcategory: PR.IP-8: Effectiveness of protection technologies is shared
Requirement: PR.IP-8.1: The organization shall collaborate and share information about its critical system's related security incidents and mitigation measures with designated partners.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Requirement: PR.IP-8.2: Communication of effectiveness of protection technologies shall be shared with appropriate parties.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Requirement: PR.IP-8.3: The organization shall implement, where feasible, automated mechanisms to assist in information collaboration.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Subcategory: PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
Requirement: PR.IP-9.1: Incident response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) shall be established, maintained, approved, and tested to determine the effectiveness of the plans, and the readiness to execute the plans.

Guidance: •   The incident response plan is the documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack.
•   Plans should incorporate recovery objectives, restoration priorities, metrics, contingency roles, personnel assignments and contact information.
•   Maintaining essential functions despite system disruption, and the eventual restoration of the organization's systems, should be addressed.
•   Consider defining incident types, resources and management support needed to effectively maintain and mature the incident response and contingency capabilities.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Subcategory: PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
Requirement: BASIC_PR.IP-11.1: Personnel having access to the organization's most critical information or technology shall be verified.
Guidance: •   The access to critical information or technology should be considered when recruiting, during employment and at termination.
•   Background verification checks should take into consideration applicable laws, regulations, and ethics in proportion to the business

requirements, the classification of the information to be accessed and the perceived risks.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Requirement: PR.IP-11.2: Develop and maintain a human resource information/cyber security process that is applicable when recruiting, during employment and at termination of employment.
Guidance: The human resource information/cyber security process should include access to critical information or technology; background verification checks; code of conduct; roles, authorities, and responsibilities…
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Subcategory: PR.IP-12: A vulnerability management plan is developed and implemented
Requirement: PR.IP-12.1: The organization shall establish and maintain a documented process that allows continuous review of vulnerabilities and strategies to mitigate them.
Guidance: •   Consider inventorying sources likely to report vulnerabilities in the identified components and distribute updates (software publisher websites, CERT website, ENISA website).
•   The organization should identify where its critical system's vulnerabilities may be exposed to adversaries.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
Key Measure: Key Measure
Subcategory: PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
Requirement: BASIC_PR.MA-1.1: Patches and security updates for Operating Systems and critical system components shall be installed.
Guidance: The following should be considered:
•   Limit yourself to only install those applications (operating systems, firmware, or plugins) that you need to run your business and patch/update them regularly.
•   You should only install a current and vendor-supported version of software you choose to use. It may be useful to assign a day each month to check for patches.
•   There are products which can scan your system and notify you when there is an update for an application you have installed. If you use one of these products, make sure it checks for updates for every application you use.
•   Install patches and security updates in a timely manner.
Documentation Score: 1

Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
Requirement: PR.MA-1.2: The organization shall plan, perform and document preventive maintenance and repairs on its critical system components according to approved processes and tools.
Guidance: Consider the below measures:
(1) Perform security updates on all software in a timely manner.
(2) Automate the update process and audit its effectiveness.
(3) Introduce an internal patching culture on desktops, mobile devices, servers, network components, etc. to ensure updates are tracked.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
Requirement: PR.MA-1.3: The organization shall enforce approval requirements, control, and monitoring of maintenance tools for use on the its critical systems.
Guidance: Maintenance tools can include, for example, hardware/software diagnostic test equipment, hardware/software packet sniffers and laptops.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
Requirement: PR.MA-1.4: The organization shall verify security controls following hardware maintenance or repairs, and take action as appropriate.
Guidance: No additional guidance on this topic
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
Subcategory: PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
Requirement: PR.MA-2.1: Remote maintenance shall only occur after prior approval, monitoring to avoid unauthorised access, and approval of the outcome of the maintenance activities as described in approved processes or procedures.
Guidance: No additional guidance on this topic
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
Requirement: PR.MA-2.2: The organization shall make sure that strong authenticators, record keeping, and session termination for remote maintenance is implemented.
Guidance: No additional guidance on this topic
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
Key Measure: Key Measure
Subcategory: PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
Requirement: BASIC_PR.PT-1.1: Logs shall be maintained, documented, and reviewed.
Guidance: •   Ensure the activity logging functionality of protection / detection hardware or software (e.g. firewalls, anti-virus) is enabled.
•   Logs should be backed up and saved for a predefined period.
•   The logs should be reviewed for any unusual or unwanted trends, such as a large use of social media websites or an unusual number of viruses consistently found on a particular computer. These trends may indicate a more serious problem or signal the need for stronger protections in a particular area.

Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions
are managed to ensure the security and resilience of systems and
assets, consistent with related policies, procedures, and agreements.
Requirement: PR.PT-1.2: The organization shall ensure that the log
records include an authoritative time source or internal clock time
stamp that are compared and synchronized to an authoritative time
source.
Guidance: Authoritative time sources include for example, an internal
Network Time Protocol (NTP) server, radio clock, atomic clock, GPS
time source.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions
are managed to ensure the security and resilience of systems and
assets, consistent with related policies, procedures, and agreements.
Subcategory: PR.PT-2: Removable media is protected and its use
restricted according to policy
Requirement: PR.PT-2.1: The usage restriction of portable storage
devices shall be ensured through an appropriate documented policy and
supporting safeguards.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions
are managed to ensure the security and resilience of systems and
assets, consistent with related policies, procedures, and agreements.
Requirement: PR.PT-2.2: The organisation should technically prohibit
the connection of removable media unless strictly necessary; in other
instances, the execution of autoruns from such media should be
disabled.
Guidance: No additional guidance on this topic.
Documentation Score: 1

Implementation Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions
are managed to ensure the security and resilience of systems and
assets, consistent with related policies, procedures, and agreements.
Subcategory: PR.PT-3: The principle of least functionality is
incorporated by configuring systems to provide only essential
capabilities
Requirement: PR.PT-3.1: The organization shall configure the business
critical systems to provide only essential capabilities.
Guidance: Consider applying the principle of least functionality to
access systems and assets (see also PR.AC-4).
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions
are managed to ensure the security and resilience of systems and
assets, consistent with related policies, procedures, and agreements.
Subcategory: PR.PT-4: Communications and control networks are
protected
Requirement: BASIC_PR.PT-4.1: Web and e-mail filters shall be
installed and used.
Guidance: •   E-mail filters should detect malicious e-mails, and
filtering should be configured based on the type of message
attachments so that files of the specified types are automatically
processed (e.g. deleted).
•   Web-filters should notify the user if a website may contain
malware and potentially preventing users from accessing that website.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Anomalies and Events (DE.AE): Anomalous activity is detected
and the potential impact of events is understood.
Subcategory: DE.AE-2: Detected events are analyzed to understand
attack targets and methods
Requirement: DE.AE-2.1: The organization shall review and analyze
detected events to understand attack targets and methods.
Guidance: No additional guidance on this topic.
Documentation Score: 1

Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Anomalies and Events (DE.AE): Anomalous activity is detected
and the potential impact of events is understood.
Key Measure: Key Measure
Subcategory: DE.AE-3: Event data are collected and correlated from
multiple sources and sensors
Requirement: BASIC_DE.AE-3.1: The activity logging functionality of
protection / detection hardware or software
(e.g. firewalls, anti-virus) shall be enabled, backed-up and reviewed.
Guidance: •   Logs should be backed up and saved for a predefined
period.
•   The logs should be reviewed for any unusual or unwanted trends,
such as a large use of social media websites or an unusual number of
viruses consistently found on a particular computer. These trends may
indicate a more serious problem or signal the need for stronger
protections in a particular area.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Anomalies and Events (DE.AE): Anomalous activity is detected
and the potential impact of events is understood.
Requirement: DE.AE-3.2: The organization shall ensure that event data
is compiled and correlated across its critical systems using various
sources such as event reports, audit monitoring, network monitoring,
physical access monitoring, and user/administrator reports.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Anomalies and Events (DE.AE): Anomalous activity is detected
and the potential impact of events is understood.
Subcategory: DE.AE-5: Incident alert thresholds are established
Requirement: DE.AE-5.1: The organization shall implement automated
mechanisms and system generated alerts to support event detection and
to assist in the identification of security alert thresholds.
Guidance: No additional guidance on this topic.

Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.
Requirement: DE.AE-5.2: The organization shall define incident alert thresholds.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Subcategory: DE.CM-1: The network is monitored to detect potential cybersecurity events
Requirement: BASIC_DE.CM-1.1: Firewalls shall be installed and operated on the network boundaries and completed with firewall protection on the endpoints.
Guidance: •   Endpoints include desktops, laptops, servers...
•   Consider, where feasible, including smart phones and other networked devices when installing and operating firewalls.
•   Consider limiting the number of interconnection gateways to the Internet.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Key Measure: Key Measure
Requirement: DE.CM-1.2: The organization shall monitor and identify unauthorized use of its business critical systems through the detection of unauthorized local connections, network connections and remote connections.

Guidance: •   Monitoring of network communications should happen at the external boundary of the organization's business critical systems and at key internal boundaries within the systems.
•   When hosting internet facing applications the implementation of a web application firewall (WAF) should be considered.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Subcategory: DE.CM-2: The physical environment is monitored to detect potential cybersecurity events
Requirement: DE.CM-2.1: The physical environment of the facility shall be monitored for potential information/cybersecurity events.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Subcategory: DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
Requirement: BASIC_DE.CM-3.1: End point and network protection tools to monitor end-user behavior for dangerous activity shall be implemented.
Guidance: Consider deploying an Intrusion Detection/Prevention system (IDS/IPS).
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Requirement: DE.CM-3.2: End point and network protection tools that monitor end-user behavior for dangerous activity shall be managed.
Guidance: Consider using a centralized log platform for the consolidation and exploitation of log files.

Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Requirement: DE.CM-3.3: Software usage and installation restrictions shall be enforced.
Guidance: Only authorized software should be used and user access rights should be limited to the specific data, resources and applications needed to complete a required task (least privilege principle).
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Key Measure: Key Measure
Subcategory: DE.CM-4: Malicious code is detected
Requirement: BASIC_DE.CM-4.1: Anti-virus, -spyware, and other -malware programs shall be installed and updated.
Guidance: •   Malware includes viruses, spyware, and ransomware and should be countered by installing, using, and regularly updating anti-virus and anti-spyware software on every device used in company's business (including computers, smart phones, tablets, and servers).
•   Anti-virus and anti-spyware software should automatically check for updates in "real-time" or at least daily followed by system scanning as appropriate.
•   It should be considered to provide the same malicious code protection mechanisms for home computers (e.g. teleworking) or personal devices that are used for professional work (BYOD).
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Subcategory: DE.CM-5: Unauthorized mobile code is detected

Requirement: DE.CM-5.1: The organization shall define acceptable and unacceptable mobile code and mobile code technologies; and authorize, monitor, and control the use of mobile code within the system.
Guidance: •   Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Mobile code technologies include for example Java applets, JavaScript, HTML5, WebGL, and VBScript.
•   Decisions regarding the use of mobile code in organizational systems should be based on the potential for the code to cause damage to the systems if used maliciously. Usage restrictions and implementation guidance should apply to the selection and use of mobile code installed.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Subcategory: DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events
Requirement: DE.CM-6.1: All external connections by vendors supporting IT/OT applications or infrastructure shall be secured and actively monitored to ensure that only permissible actions occur during the connection.
Guidance: This monitoring includes unauthorized personnel access, connections, devices, and software.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Requirement: DE.CM-6.2: External service providers' conformance with personnel security policies and procedures and contract security requirements shall be monitored relative to their cybersecurity risks.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Subcategory: DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
Requirement: DE.CM-7.1: The organization's business critical systems shall be monitored for unauthorized personnel access, connections, devices, access points, and software.
Guidance: •   Unauthorized personnel access includes access by external service providers.
•   System inventory discrepancies should be included in the monitoring.
•   Unauthorized configuration changes to organization's critical systems should be included in the monitoring.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Subcategory: DE.CM-8: Vulnerability scans are performed
Requirement: DE.CM-8.1: The organization shall monitor and scan for vulnerabilities in its critical systems and hosted applications ensuring that system functions are not adversely impacted by the scanning process.
Guidance: Consider the implementation of a continuous vulnerability scanning program; Including reporting and mitigation plans.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Requirement: DE.CM-8.2: The vulnerability scanning process shall include analysis, remediation, and information sharing.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
Subcategory: DE.DP-2: Detection activities comply with all applicable requirements
Requirement: DE.DP-2.1: The organization shall conduct detection activities in accordance with applicable federal and regional laws, industry regulations and standards, policies, and other applicable requirements.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
Subcategory: DE.DP-3: Detection processes are tested
Requirement: DE.DP-3.1: The organization shall validate that event detection processes are operating as intended.
Guidance: •   Validation includes testing.
•   Validation should be demonstrable.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
Subcategory: DE.DP-4: Event detection information is communicated
Requirement: DE.DP-4.1: The organization shall communicate event detection information to predefined parties.
Guidance: Event detection information includes for example, alerts on atypical account usage, unauthorized remote access, wireless connectivity, mobile device connection, altered configuration settings, contrasting system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, use of Voice over Internet Protocol (VoIP), and malware disclosure.
Documentation Score: 1

Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Detection Processes (DE.DP): Detection processes and
procedures are maintained and tested to ensure awareness of anomalous
events.
Subcategory: DE.DP-5: Detection processes are continuously improved
Requirement: DE.DP-5.1: Improvements derived from the monitoring,
measurement, assessment, testing, review, and lessons learned, shall
be incorporated into detection process revisions.
Guidance: •   This results in a continuous improvement of the
detection processes.
•   The use of independent teams to assess the detection process
could be considered.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Response Planning (RS.RP): Response processes and procedures
are executed and maintained, to ensure response to detected
cybersecurity incidents.
Subcategory: RS.RP-1: Response plan is executed during or after an
incident
Requirement: BASIC_RS.RP-1.1: An incident response process, including
roles, responsibilities, and authorities, shall be executed during or
after an information/cybersecurity event on the organization's
critical systems.
Guidance: •   The incident response process should include a
predetermined set of instructions or procedures to detect, respond to,
and limit consequences of a malicious cyber-attack.
•   The roles, responsibilities, and authorities in the incident
response plan should be specific on involved people, contact info,
different roles and responsibilities, and who makes the decision to
initiate recovery procedures as well as who will be the contact with
appropriate external stakeholders.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.
Guidance: It should be considered to determine the causes of an information/cybersecurity event and implement a corrective action in order that the event does not recur or occur elsewhere (an infection by malicious code on one machine did not have spread elsewhere in the network). The effectiveness of any corrective action taken should be reviewed. Corrective actions should be appropriate to the effects of the information/cybersecurity event encountered.
Internal Note: Requirements are covered in PR.IP-9

Function: RESPOND (RS)
Category: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
Subcategory: RS.CO-1: Personnel know their roles and order of operations when a response is needed
Requirement: RS.CO-1.1: The organization shall ensure that personnel understand their roles, objectives, restoration priorities, task sequences (order of operations) and assignment responsibilities for event response.
Guidance: Consider the use the CCB Incident Management Guide to guide you through this exercise and consider bringing in outside experts if needed. Test your plan regularly and adjust it after each incident.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
Subcategory: RS.CO-2: Incidents are reported consistent with established criteria
Requirement: RS.CO-2.1: The organization shall implement reporting on information/cybersecurity incidents on its critical systems in an organization-defined time frame to organization-defined personnel or roles.
Guidance: All users should have a single point of contact to report any incident and be encouraged to do so.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1

Subcategory Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
Subcategory: RS.CO-3: Information is shared consistent with response plans
Requirement: BASIC_RS.CO-3.1: Information/cybersecurity incident information shall be communicated and shared with the organization's employees in a format that they can understand.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
Requirement: RS.CO-3.2: The organization shall share information/cybersecurity incident information with relevant stakeholders as foreseen in the incident response plan.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: RESPOND (RS)
Category: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
Subcategory: RS.CO-4: Coordination with stakeholders occurs consistent with response plans
Requirement: RS.CO-4.1: The organization shall coordinate information/cybersecurity incident response actions with all predefined stakeholders.
Guidance: •   Stakeholders for incident response include for example, mission/business owners, organization's critical system owners, integrators, vendors, human resources offices, physical and personnel security offices, legal departments, operations personnel, and procurement offices.
•   Coordination with stakeholders occurs consistent with incident response plans.
Documentation Score: 1
Implementation Score: 1

Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Communications (RS.CO): Response activities are coordinated
with internal and external stakeholders (e.g. external support from
law enforcement agencies).
Subcategory: RS.CO-5: Voluntary information sharing occurs with
external stakeholders to achieve broader cybersecurity situational
awareness
Requirement: RS.CO-5.1: The organization shall share
information/cybersecurity event information voluntarily, as
appropriate, with external stakeholders, industry security groups,… to
achieve broader information/cybersecurity situational awareness.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Analysis (RS.AN): Analysis is conducted to ensure effective
response and support recovery activities.
Subcategory: RS.AN-1: Notifications from detection systems are
investigated
Requirement: RS.AN-1.1: The organization shall investigate
information/cybersecurity-related notifications generated from
detection systems.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1.75
Category Implementation Maturity Score: 1.5

Function: RESPOND (RS)
Category: Analysis (RS.AN): Analysis is conducted to ensure effective
response and support recovery activities.
Subcategory: RS.AN-2: The impact of the incident is understood
Requirement: RS.AN-2.1:Thorough investigation and result analysis
shall be the base for understanding the full implication of the
information/cybersecurity incident.
Guidance: •   Result analysis can involve the outcome of determining
the correlation between the information of the detected event and the

outcome of risk assessments. In this way, insight is gained into the impact of the event across the organization.
•   Consider including detection of unauthorized changes to its critical systems in its incident response capabilities.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
Subcategory: RS.AN-4: Incidents are categorized consistent with response plans
Requirement: RS.AN-4.1: Information/cybersecurity incidents shall be categorized according to the level of severity and impact consistent with the evaluation criteria included the incident response plan.
Guidance: •   It should be considered to determine the causes of an information/cybersecurity incident and implement a corrective action in order that the incident does not recur or occur elsewhere.
•   The effectiveness of any corrective action taken should be reviewed.
•   Corrective actions should be appropriate to the effects of the information/cybersecurity incident encountered.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
Key Measure: Key Measure
Subcategory: RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
Requirement: RS.AN-5.1: The organization shall implement vulnerability management processes and procedures that include processing, analyzing and remedying vulnerabilities from internal and external sources.
Guidance: Internal and external sources could be e.g. internal testing, security bulletins, or security researchers.
Documentation Score: 4
Implementation Score: 3
Subcategory Documentation Maturity Score: 4
Subcategory Implementation Maturity Score: 3

Function: RESPOND (RS)
Category: Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
Subcategory: RS.MI-1: Incidents are contained
Requirement: RS.MI-1.1: The organization shall implement an incident handling capability for information/cybersecurity incidents on its business critical systems that includes preparation, detection and analysis, containment, eradication, recovery and documented risk acceptance.
Guidance: A documented risk acceptance deals with risks that the organisation assesses as not dangerous to the organisation's business critical systems and where the risk owner formally accepts the risk (related with the risk appetite of the organization)
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
Subcategory: RS.IM-1: Response plans incorporate lessons learned
Requirement: BASIC_RS.IM-1.1:The organization shall conduct post-incident evaluations to analyse lessons learned from incident response and recovery, and consequently improve processes / procedures / technologies to enhance its cyber resilience.
Guidance: Consider bringing involved people together after each incident and reflect together on ways to improve what happened, how it happened, how we reacted, how it could have gone better, what should be done to prevent it from happening again, etc.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
Requirement: RS.IM-1.2:Lessons learned from incident handling shall be translated into updated or new incident handling procedures that shall be tested, approved and trained.

Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: RESPOND (RS)
Category: Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
Subcategory: RS.IM-2: Response and Recovery strategies are updated
Requirement: RS.IM-2.1:The organization shall update the response and recovery plans to address changes in its context.
Guidance: The organization's context relates to the organizational structure, its critical systems, attack vectors, new threats, improved technology, environment of operation, problems encountered during plan implementation/execution/testing and lessons learned.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: RECOVER (RC)
Category: Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
Subcategory: RC.RP-1: Recovery plan is executed during or after a cybersecurity incident
Requirement: BASIC_RC.RP-1.1: A recovery process for disasters and information/cybersecurity incidents shall be developed and executed as appropriate.
Guidance: A process should be developed for what immediate actions will be taken in case of a fire, medical emergency, burglary, natural disaster, or an information/cyber security incident.
This process should consider:
•   Roles and Responsibilities, including of who makes the decision to initiate recovery procedures and who will be the contact with appropriate external stakeholders.
•   What to do with company's information and information systems in case of an incident. This includes shutting down or locking computers, moving to a backup site, physically removing important documents, etc.
•   Who to call in case of an incident.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: RECOVER (RC)
Category: Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
Subcategory: RC.IM-1: Recovery plans incorporate lessons learned
Requirement: RC.IM-1.1: The organization shall incorporate lessons learned from incident recovery activities into updated or new system recovery procedures and, after testing, frame this with appropriate training.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: RECOVER (RC)
Category: Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).
Subcategory: RC.CO-1: Public relations are managed
Requirement: RC.CO-1.1: The organization shall centralize and coordinate how information is disseminated and manage how the organization is presented to the public.
Guidance: Public relations management may include, for example, managing media interactions, coordinating and logging all requests for interviews, handling and 'triaging' phone calls and e-mail requests, matching media requests with appropriate and available internal experts who are ready to be interviewed, screening all of information provided to the media, ensuring personnel are familiar with public relations and privacy policies.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: RECOVER (RC)
Category: Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).
Subcategory: RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

```
Requirement: RC.CO-3.1: The organization shall communicate recovery
activities to predefined stakeholders, executive and management teams.
Guidance: Communication of recovery activities to all relevant
stakeholders applies only to entities subject to the NIS legislation.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
```

IMPORTANT Summary

CyberFundamentals Framework — IMPORTANT Summary

CyberFundamentals Categories and Maturity Scores

IDENTIFY

- **Asset Management (ID.AM)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.03
  Implementation Maturity Score: 1.02
- **Business Environment (ID.BE)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Governance (ID.GV)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Risk Assessment (ID.RA)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Risk Management Strategy (ID.RM)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00

Documentation Maturity Score: 1.00
Implementation Maturity Score: 1.00

- **Supply Chain Risk Management (ID.SC)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

PROTECT

- **Identity Management, Authentication and Access Control (PR.AC)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Awareness and Training (PR.AT)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Data Security (PR.DS)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Information Protection Processes and Procedures (PR.IP)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Maintenance (PR.MA)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Protective Technology (PR.PT)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

DETECT

- **Anomalies and Events (DE.AE)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Security Continuous Monitoring (DE.CM)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Detection Processes (DE.DP)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

RESPOND

- **Response Planning (RS.RP)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.163
  Documentation Maturity Score: 1.175
  Implementation Maturity Score: 1.150
- **Communications (RS.CO)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Analysis (RS.AN)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Mitigation (RS.MI)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Improvements (RS.IM)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00

Documentation Maturity Score: 1.00
Implementation Maturity Score: 1.00

RECOVER

- **Recovery Planning (RC.RP)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Improvements (RC.IM)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Communications (RC.CO)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

Key Measures (KM) and Maturity Scores

Access Control and Security Measures

- **PR.AC-1.1** — Identities and credentials for authorized devices and users shall be managed.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-3.2** — The organization's networks, when accessed remotely, shall be secured through multi-factor authentication (MFA).
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-4.1** — Access permissions for users to the organization's systems shall be defined and managed.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **PR.AC-4.2** — Personnel who should have access to the organization's business-critical information and technology shall be identified and assigned access rights accordingly.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-4.3** — Employee access to data and information shall be limited to the systems and specific information they need to do their jobs (principle of Least Privilege).
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-4.4** — Nobody shall have administrator privileges for daily tasks.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-5.1** — Firewalls shall be installed and activated on all the organization's networks.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-5.2** — Where appropriate, network integrity of the organization's critical systems shall be protected by incorporating network segmentation and segregation.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.IP-4.1** — Backups for organization's business-critical data shall be conducted and stored on a system different from the device on which the original data resides.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.MA-1.1** — Patches and security updates for operating systems and critical system components shall be installed.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00

Documentation Maturity Score: 1.00
Implementation Maturity Score: 1.00

- **PR.PT-1.1** — Logs shall be maintained, documented, and reviewed.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **DE.AE-3.1** — The activity logging functionality of protection and detection hardware/software (e.g., firewalls, anti-virus) shall be enabled, backed up, and reviewed.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **DE.CM-4.1** — Anti-virus, spyware, and other malware programs shall be installed and updated.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

Extended and Management Measures

- **ID.AM-6.1** — Information security and cybersecurity roles, responsibilities, and authorities within the organization shall be documented, reviewed, authorized, and updated as aligned with organizational roles and external partners.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-3.3** — Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization's critical systems shall be identified, documented, and implemented.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-5.3** — Where appropriate, network integrity of the organization's critical systems shall be protected by:
  (1) Identifying, documenting, and controlling connections between system components.
  (2) Limiting external connections to the organization's critical systems.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00

Documentation Maturity Score: 1.00
Implementation Maturity Score: 1.00

- **PR.AC-5.4** — The organization shall monitor and control connections and communications at the external boundary and at key internal boundaries within the organization's critical systems by implementing boundary protection devices where appropriate.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **PR.DS-5.1** — The organization shall take appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points where unauthorized access and activities, including data leakage, is detected.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **PR.IP-1.1** — The organization shall develop, document, and maintain a baseline configuration for its business-critical systems.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **DE.CM-1.2** — The organization shall monitor and identify unauthorized use of its business-critical systems through detection of unauthorized local connections, network connections, and remote connections.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **RS.AN-5.1** — The organization shall implement vulnerability management processes and procedures that include processing, analyzing, and remedying vulnerabilities from internal and external sources.
  Target Maturity Score: 3.00
  KM Maturity Score: 3.50
  Documentation Maturity Score: 4.00
  Implementation Maturity Score: 3.00

Total Maturity Level

Overall Score: 1.03
TLP Classification: AMBER

_____

ESSENTIAL Details

```
Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices,
systems, and facilities that enable the organization to achieve
business purposes are identified and managed consistent with their
relative importance to organizational objectives and the
organization's risk strategy.
Subcategory: ID.AM-1: Physical devices and systems within the
organization are inventoried
Requirement: BASIC_ID.AM-1.1: An inventory of assets associated with
information and information processing facilities within the
organization shall be documented, reviewed, and updated when changes
occur.
Guidance: •     This inventory includes fixed and portable computers,
tablets, mobile phones, Programmable Logic Controllers (PLCs),
sensors, actuators, robots, machine tools, firmware, network switches,
routers, power supplies, and other networked components or devices.
•     This inventory must include all assets, whether or not they are
connected to the organization's network.
•     The use of an IT asset management tool could be considered.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1.0666666666666667
Category Implementation Maturity Score: 1.1666666666666667

---

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices,
systems, and facilities that enable the organization to achieve
business purposes are identified and managed consistent with their
relative importance to organizational objectives and the
organization's risk strategy.
Requirement: IMPORTANT_ID.AM-1.2: The inventory of assets associated
with information and information processing facilities shall reflect
changes in the  organization's context and include all information
necessary for effective accountability.
Guidance: •     Inventory specifications include for example,
manufacturer, device type, model, serial number, machine names and
network addresses, physical location…
```

- Accountability is the obligation to explain, justify, and take responsibility for one's actions, it implies answerability for the outcome of the task or process.
- Changes include the decommissioning of material.

Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Requirement: IMPORTANT_ID.AM-1.3: When unauthorized hardware is detected, it shall be quarantined for possible exception handling, removed, or replaced, and the inventory shall be updated accordingly.
Guidance: • Any unsupported hardware without an exception documentation, is designated as unauthorized.
- Unauthorized hardware can be detected during inventory, requests for support by the user or other means.

Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Requirement: ID.AM-1.4: Mechanisms for detecting the presence of unauthorized hardware and firmware components within the organization's network shall be identified.
Guidance: • Where safe and feasible, these mechanisms should be automated.
- There should be a process to address unauthorized assets on a frequently basis; The organization may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their

relative importance to organizational objectives and the organization's risk strategy.
Subcategory: ID.AM-2: Software platforms and applications within the organization are inventoried
Requirement: BASIC_ID.AM-2.1: An inventory that reflects what software platforms and applications are being used in the organization shall be documented, reviewed, and updated when changes occur.
Guidance: •   This inventory includes software programs, software platforms and databases, even if outsourced (SaaS).
•   Outsourcing arrangements should be part of the contractual agreements with the provider.
•   Information in the inventory should include for example: name, description, version, number of users, data processed, etc.
•   A distinction should be made between unsupported software and unauthorized software.
•   The use of an IT asset management tool could be considered.
Documentation Score: 3
Implementation Score: 1
Subcategory Documentation Maturity Score: 1.4
Subcategory Implementation Maturity Score: 2

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Requirement: IMPORTANT_ID.AM-2.2: The inventory of software platforms and applications associated with information and information processing shall reflect changes in the organization's context and include all information necessary for effective accountability.
Guidance: The inventory of software platforms and applications should include the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date.
Documentation Score: 1
Implementation Score: 3

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Requirement: IMPORTANT_ID.AM-2.3: Individuals who are responsible and who are accountable for administering software platforms and applications within the organization shall be identified.

Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 4

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Requirement: IMPORTANT_ID.AM-2.4: When unauthorized software is detected, it shall be quarantined for possible exception handling, removed, or replaced, and the inventory shall be updated accordingly.
Guidance: •   Any unsupported software without an exception documentation, is designated as unauthorized.
•   Unauthorized software can be detected during inventory, requests for support by the user or other means.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Requirement: ID.AM-2.5: Mechanisms for detecting the presence of unauthorized software within the organization's ICT/OT environment shall be identified.
Guidance: •   Where safe and feasible, these mechanisms should be automated.
•   There should be a process to regularly address unauthorised assets; The organization may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Subcategory: ID.AM-3: Organizational communication and data flows are mapped

Requirement: BASIC_ID.AM-3.1: Information that the organization stores and uses shall be identified.
Guidance: •   Start by listing all the types of information your business stores or uses. Define "information type" in any useful way that makes sense to your business. You may want to have your employees make a list of all the information they use in their regular activities. List everything you can think of, but you do not need to be too specific. For example, you may keep customer names and email addresses, receipts for raw material, your banking information, or other proprietary information.
•   Consider mapping this information with the associated assets identified in the inventories of physical devices, systems, software platforms and applications used within the organization (see ID.AM-1 & ID.AM-2).
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Requirement: IMPORTANT_ID.AM-3.2: All connections within the organization's ICT/OT environment, and to other organization-internal platforms shall be mapped, documented, approved, and updated as appropriate.
Guidance: •   Connection information includes, for example, the interface characteristics, data characteristics, ports, protocols, addresses, description of the data, security requirements, and the nature of the connection.
•   Configuration management can be used as supporting asset.
•   This documentation should not be stored only on the network it represents.
•   Consider keeping a copy of this documentation in a safe offline environment (e.g. offline hard disk, paper hardcopy, …)
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

Requirement: ID.AM-3.3: The information flows/data flows within the organization's ICT/OT environment, as well as to other organization-internal systems shall be mapped, documented, authorized, and updated when changes occur.
Guidance: •   With knowledge of the information/data flows within a system and between systems, it is possible to determine where information can and cannot go.
•   Consider:
o   Enforcing controls restricting connections to only authorized interfaces.
o   Heightening system monitoring activity whenever there is an indication of increased risk to organization's critical operations and assets.
o   Protecting the system from information leakage due to electromagnetic signals emanations.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Subcategory: ID.AM-4: External information systems are catalogued
Requirement: IMPORTANT_ID.AM-4.1: The organization shall map, document, authorize and when changes occur, update, all external services and the connections made with them.
Guidance: •   Outsourcing of systems, software platforms and applications used within the organization is covered in ID.AM-1 & ID.AM-2
•   External information systems are systems or components of systems for which organizations typically have no direct supervision and authority over the application of security requirements and controls, or the determination of the effectiveness of implemented controls on those systems i.e., services that are run in cloud, SaaS, hosting or other external environments, API (Application Programming Interface)…
•   Mapping external services and the connections made to them and authorizing them in advance avoids wasting unnecessary resources investigating a supposedly non-authenticated connection to external systems.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)

Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Requirement: ID.AM-4.2: The flow of information to/from external systems shall be mapped, documented, authorized, and update when changes occur.
Guidance: Consider requiring external service providers to identify and document the functions, ports, protocols, and services necessary for the connection services.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Subcategory: ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
Requirement: BASIC_ID.AM-5.1: The organization's resources (hardware, devices, data, time, personnel, information, and software) shall be prioritized based on their classification, criticality, and business value.
Guidance: •   Determine organization's resources (e.g., hardware, devices, data, time, personnel, information, and software):
o   What would happen to my business if these resources were made public, damaged, lost…?
o   What would happen to my business when the integrity of resources is no longer guaranteed?
o   What would happen to my business if I/my customers couldn't access these resources? And rank these resources based on their classification, criticality, and business value.
•   Resources should include enterprise assets.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

Guidance: •   Create a classification for sensitive information by first determining categories, e.g.
o   Public - freely accessible to all, even externally
o   Internal - accessible only to members of your organization
o   Confidential - accessible only to those whose duties require access.
•   Communicate these categories and identify what types of data fall into these categories (HR data, financial data, legal data, personal data, etc.).
•   Consider the use of the Traffic Light Protocol (TLP).
•   Data classification should apply to the three aspects: C-I-A.

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Guidance: Consider implementing an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider.

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
Key Measure: Key Measure
Subcategory: ID.AM-6: Cybersecurity roles, responsibilities, and authorities for the entire workforce and third-party stakeholders are established
Requirement: IMPORTANT_ID.AM-6.1: Information security and cybersecurity roles, responsibilities and authorities within the organization shall be documented, reviewed, authorized, and updated and alignment with organization-internal roles and external partners.
Key Measure
Guidance: It should be considered to:
•   Describe security roles, responsibilities, and authorities: who in your organization should be consulted, informed, and held accountable for all or part of your assets.
•   Provide security roles, responsibilities, and authority for all key functions in information/cyber security (legal, detection activities…).
•   Include information/cybersecurity roles and responsibilities for third-party providers (e.g., suppliers, customers, partners) with physical or logical access to the organization's ICT/OT environment.

Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Asset Management (ID.AM): The data, personnel, devices,
systems, and facilities that enable the organization to achieve
business purposes are identified and managed consistent with their
relative importance to organizational objectives and the
organization's risk strategy.
Requirement: ID.AM-6.2: The organization shall appoint an information
security officer.
Guidance: The information security officer should be responsible for
monitoring the implementation of the organization's information/cyber
security strategy and safeguards.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Business Environment (ID.BE): The organization's mission,
objectives, stakeholders, and activities are understood and
prioritized; this information is used to inform cybersecurity roles,
responsibilities, and risk management decisions.
Subcategory: ID.BE-1: The organization's role in the supply chain is
identified and communicated
Requirement: IMPORTANT_ID.BE-1.1: The organization's role in the
supply chain shall be identified, documented, and communicated.
Guidance: •   The organisation should be able to clearly identify
who is upstream and downstream of the organisation and which suppliers
provide services, capabilities, products and items to the
organisation.
•   The organisation should communicate its position to its upstream
and downstream so that it is understood where they sit in terms of
critical importance to the organisation's operations.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Business Environment (ID.BE): The organization's mission,
objectives, stakeholders, and activities are understood and

prioritized; this information is used to inform cybersecurity roles,
responsibilities, and risk management decisions.
Requirement: ID.BE-1.2: The organization shall protect its ICT/OT
environment from supply chain threats by applying security safeguards
as part of a documented comprehensive security strategy.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Business Environment (ID.BE): The organization's mission,
objectives, stakeholders, and activities are understood and
prioritized; this information is used to inform cybersecurity roles,
responsibilities, and risk management decisions.
Subcategory: ID.BE-2: The organization's place in critical
infrastructure and its industry sector is identified and communicated
Requirement: IMPORTANT_ID.BE-1.2: The organization's place in critical
infrastructure and its industry sector shall be identified and
communicated.
Guidance: The organisation covered by NIS legislation has a
responsibility to know the other organisations in the same sector in
order to work with them to achieve the objectives set by NIS for that
particular sector.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Business Environment (ID.BE): The organization's mission,
objectives, stakeholders, and activities are understood and
prioritized; this information is used to inform cybersecurity roles,
responsibilities, and risk management decisions.
Subcategory: ID.BE-3: Priorities for organizational mission,
objectives, and activities are established and communicated
Requirement: IMPORTANT_ID.BE-1.3: Priorities for organizational
mission, objectives, and activities are established and communicated.
Guidance: Information protection needs should be determined, and the
related processes revised as necessary.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)

Category: Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
Subcategory: ID.BE-4: Dependencies and critical functions for delivery of critical services are established
Requirement: IMPORTANT_ID.BE-1.4: Dependencies and mission-critical functions for the delivery of critical services shall be identified, documented, and prioritized according to their criticality as part of the risk assessment process.
Guidance: Dependencies and business critical functions should include support services.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
Subcategory: ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)
Requirement: IMPORTANT_ID.BE-5.1: To support cyber resilience and secure the delivery of critical services, the necessary requirements are identified, documented and their implementation tested and approved.
Guidance: •   Consider implementing resiliency mechanisms to support normal and adverse operational situations (e.g., failsafe, load balancing, hot swap).
•   Consider aspects of business continuity management in e.g. Business Impact Analyse (BIA), Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP).
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
Requirement: ID.BE-5.2: Information processing & supporting facilities shall implement redundancy to meet availability requirements, as defined by the organization and/or regulatory frameworks.

Guidance: •   Consider provisioning adequate data and network redundancy (e.g. redundant network devices, servers with load balancing, raid arrays, backup services, 2 separate datacentres, fail-over network connections, 2 ISP's…).
•   Consider protecting critical equipment/services from power outages and other failures due to utility interruptions (e.g. UPS & NO-break, frequent test, service contracts that include regular maintenance, redundant power cabling, 2 different power service providers...).
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
Requirement: ID.BE-5.3: Recovery time and recovery point objectives for the resumption of essential ICT/OT system processes shall be defined.
Guidance: •   Consider applying the 3-2-1 back-up rule to improve RPO and RTO (maintain at least 3 copies of your data, keep 2 of them at separate locations and one copy should be stored at an off-site location).
•   Consider implementing mechanisms such as hot swap, load balancing and failsafe to increase resilience.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
Subcategory: ID.GV-1: Organizational cybersecurity policy is established and communicated
Requirement: BASIC_ID.GV-1.1: Policies and procedures for information security and cyber security shall be created, documented, reviewed, approved, and updated when changes occur.
Guidance: •   Policies and procedures used to identify acceptable practices and expectations for business operations, can be used to train new employees on your information security expectations, and can aid an investigation in case of an incident. These policies and procedures should be readily accessible to employees.
•   Policies and procedures for information- and cybersecurity should clearly describe your expectations for protecting the organization's information and systems, and how management expects the company's resources to be used and protected by all employees.

• Policies and procedures should be reviewed and updated at least annually and every time there are changes in the organization or technology. Whenever the policies are changed, employees should be made aware of the changes.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
Requirement: IMPORTANT_ID.GV-1.2: An organization-wide information security and cybersecurity policy shall be established, documented, updated when changes occur, disseminated, and approved by senior management.
Guidance: The policy should include, for example:
• The identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Guidance on role profiles along with their identified titles, missions, tasks, skills, knowledge, competences is available in the "European Cybersecurity Skills Framework Role Profiles" by ENISA. (https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles)
• The coordination among organizational entities responsible for the different aspects of security (i.e., technical, physical, personnel, cyber-physical, information, access control, media protection, vulnerability management, maintenance, monitoring)
• The coverage of the full life cycle of the ICT/OT systems.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
Subcategory: ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
Requirement: BASIC_ID.GV-3.1: Legal and regulatory requirements regarding information/cybersecurity, including privacy obligations, shall be understood and implemented.
Guidance: There are no additional guidelines.

Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Governance (ID.GV): The policies, procedures, and processes
to manage and monitor the organization's regulatory, legal, risk,
environmental, and operational requirements are understood and inform
the management of cybersecurity risk.
Requirement: IMPORTANT_ID.GV-3.2: Legal and regulatory requirements
regarding information/cybersecurity, including privacy obligations,
shall be managed.
Guidance: •   There should be regular reviews to ensure the
continuous compliance with legal and regulatory requirements regarding
information/cybersecurity, including privacy obligations.
•   This requirement also applies to contractors and service
providers.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Governance (ID.GV): The policies, procedures, and processes
to manage and monitor the organization's regulatory, legal, risk,
environmental, and operational requirements are understood and inform
the management of cybersecurity risk.
Subcategory: ID.GV-4: Governance and risk management processes address
cybersecurity risks
Requirement: BASIC_ID.GV-4.1: As part of the company's overall risk
management, a comprehensive strategy to manage information security
and cybersecurity risks shall be developed and updated when changes
occur.
Guidance: This strategy should include determining and allocating the
required resources to protect the organisation's business-critical
assets.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Governance (ID.GV): The policies, procedures, and processes
to manage and monitor the organization's regulatory, legal, risk,
environmental, and operational requirements are understood and inform
the management of cybersecurity risk.

Requirement: IMPORTANT_ID.GV-4.2: Information security and cybersecurity risks shall be documented, formally approved, and updated when changes occur.
Guidance: Consider using Risk Management tools.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
Subcategory: ID.RA-1: Asset vulnerabilities are identified and documented
Requirement: BASIC_ID.RA-1.1: Threats and vulnerabilities shall be identified.
Guidance: •   A vulnerability refers to a weakness in the organization's hardware, software, or procedures. It is a gap through which a bad actor can gain access to the organization's assets. A vulnerability exposes an organization to threats.
•   A threat is a malicious or negative event that takes advantage of a vulnerability.
•   The risk is the potential for loss and damage when the threat does occur.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
Requirement: IMPORTANT_ID.RA-1.2: A process shall be established to monitor, identify, and document vulnerabilities of the organisation's business critical systems in a continuous manner.
Guidance: •   Where safe and feasible, the use of vulnerability scanning should be considered.
•   The organization should establish and maintain a testing program appropriate to its size, complexity, and maturity.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
Requirement: ID.RA-1.3: To ensure that organization's operations are not adversely impacted by the testing process, performance/load testing and penetration testing on the organization's systems shall be conducted with care.
Guidance: Consider validating security measures after each penetration test.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
Subcategory: ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources
Requirement: IMPORTANT_ID.RA-2.1: A threat and vulnerability awareness program that includes a cross-organization information-sharing capability shall be implemented.
Guidance: A threat and vulnerability awareness program should include ongoing contact with security groups and associations to receive security alerts and advisories. (Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations).This contact can include the sharing of information about potential vulnerabilities and incidents. This sharing capability should have an unclassified and classified information sharing capability.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
Requirement: ID.RA-2.2: It shall be identified where automated mechanisms can be implemented to make security alert and advisory information available to relevant organization stakeholders.
Guidance: No additional guidance on this topic.
Documentation Score: 1

Implementation Score: 1

Function: IDENTIFY (ID)
Category: Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
Subcategory: ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
Requirement: BASIC_ID.RA-5.1: The organization shall conduct risk assessments in which risk is determined by threats, vulnerabilities and impact on business processes and assets.
Guidance: •   Keep in mind that threats exploit vulnerabilities.
•   Identify the consequences that losses of confidentiality, integrity and availability may have on the assets and related business processes.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
Requirement: IMPORTANT_ID.RA-5.2: The organization shall conduct and document risk assessments in which risk is determined by threats, vulnerabilities, impact on business processes and assets, and the likelihood of their occurrence.
Guidance: •   Risk assessment should include threats from insiders and external parties.
•   Qualitative and/or quantitative risk analysis methods (MAPGOOD, ISO27005, CIS RAM, …) can be used together with software tooling.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
Requirement: ID.RA-5.3: Risk assessment results shall be disseminated to relevant stakeholders.
Guidance: No additional guidance on this topic.

Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Risk Assessment (ID.RA): The organization understands the
cybersecurity risk to organizational operations (including mission,
functions, image, or reputation), organizational assets, and
individuals.
Subcategory: ID.RA-6: Risk responses are identified and prioritized
Requirement: IMPORTANT_ID.RA-6.1: A comprehensive strategy shall be
developed and implemented to manage risks to the organization's
critical systems, that includes the identification and prioritization
of risk responses.
Guidance: •   Management and employees should be involved in
information- and cybersecurity.
•   It should be identified what the most important assets are, and
how they are protected.
•   It should be clear what impact will be if these assets are
compromised.
•   It should be established how the implementation of adequate
mitigation measures will be organized.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Risk Management Strategy (ID.RM): The organization's
priorities, constraints, risk tolerances, and assumptions are
established and used to support operational risk decisions.
Subcategory: ID.RM-1: Risk management processes are established,
managed, and agreed to by organizational stakeholders
Requirement: IMPORTANT_ID.RM-1.1: A cyber risk management process that
identifies key internal and external stakeholders and facilitates
addressing risk-related issues and information shall be created,
documented, reviewed, approved, and updated when changes occur.
Guidance: External stakeholders include customers, investors and
shareholders, suppliers, government agencies and the wider community.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: IDENTIFY (ID)

Category: Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
Subcategory: ID.RM-2: Organizational risk tolerance is determined and clearly expressed
Requirement: IMPORTANT_ID.RM-2.1: The organization shall clearly determine it's risk appetite.
Guidance: Determination and expression of risk tolerance (risk appetite) should be in line with the policies on information security and cybersecurity, to facilitate demonstration of coherence between policies, risk tolerance and measures.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
Subcategory: ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
Requirement: IMPORTANT_ID.RM-3.1: The organization's role in critical infrastructure and its sector shall determine the organization's risk appetite.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Supply Chain Risk Management (ID.SC):
The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.
Subcategory: ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
Requirement: ID.SC-1.1: The organization shall document, review, approve, update when changes occur, and implement a cyber supply chain risk management process that supports the identification, assessment, and mitigation of the risks associated with the distributed and interconnected nature of ICT/OT product and service supply chains.
Guidance: No additional guidance on this topic.

Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Supply Chain Risk Management (ID.SC):
The organization's priorities, constraints, risk tolerances, and
assumptions are established and used to support risk decisions
associated with managing supply chain risk. The organization has
established and implemented the processes to identify, assess and
manage supply chain risks.
Subcategory: ID.SC-2: Suppliers and third party partners of
information systems, components, and services are identified,
prioritized, and assessed using a cyber supply chain risk assessment
process
Requirement: IMPORTANT_ID.SC-2.1: The organization shall conduct cyber
supply chain risk assessments at least annually or when a change to
the organization's critical systems, operational environment, or
supply chain occurs; These assessments shall be documented, and the
results disseminated to relevant stakeholders including those
responsible for ICT/OT systems.
Guidance: This assessment should identify and prioritize potential
negative impacts to the organization from the risks associated with
the distributed and interconnected nature of ICT/OT product and
service supply chains.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Supply Chain Risk Management (ID.SC):
The organization's priorities, constraints, risk tolerances, and
assumptions are established and used to support risk decisions
associated with managing supply chain risk. The organization has
established and implemented the processes to identify, assess and
manage supply chain risks.
Requirement: ID.SC-2.2: A documented list of all the organization's
suppliers, vendors and partners who may be involved in a major
incident shall be established, kept up-to-date and made available
online and offline.
Guidance: This list should include suppliers, vendors and partners
contact information and the services they provide, so they can be
contacted for assistance in the event of an outage or service
degradation.

Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Supply Chain Risk Management (ID.SC):
The organization's priorities, constraints, risk tolerances, and
assumptions are established and used to support risk decisions
associated with managing supply chain risk. The organization has
established and implemented the processes to identify, assess and
manage supply chain risks.
Subcategory: ID.SC-3: Contracts with suppliers and third-party
partners are used to implement appropriate measures designed to meet
the objectives of an organization's cybersecurity program and Cyber
Supply Chain Risk Management Plan.
Requirement: IMPORTANT_ID.SC-3.1: Based on the results of the cyber
supply chain risk assessment, a contractual framework for suppliers
and external partners shall be established to address sharing of
sensitive information and distributed and interconnected ICT/OT
products and services.
Guidance: •   Entities not subject to the NIS legislation should
consider business critical suppliers and third-party partners only.
•   Keep in mind that GDPR requirements need to be fulfilled when
business information contains personal data (applicable on all
levels), i.e. security measures need to be addressed in the
contractual framework.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Supply Chain Risk Management (ID.SC):
The organization's priorities, constraints, risk tolerances, and
assumptions are established and used to support risk decisions
associated with managing supply chain risk. The organization has
established and implemented the processes to identify, assess and
manage supply chain risks.
Key Measure: Key Measure
Requirement: ID.SC-3.2: Contractual information security and
cybersecurity' requirements for suppliers and third-party partners
shall be implemented to ensure a verifiable flaw remediation process,
and to ensure the correction of flaws identified during 'information
security and cybersecurity' testing and evaluation.
Guidance: •   Information systems containing software (or firmware)
affected by recently announced software flaws (and potential
vulnerabilities resulting from those flaws) should be identified.
•   Newly released security relevant patches, service packs, and hot
fixes should be installed, and these patches, service packs, and hot

fixes are tested for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling are also addressed expeditiously. Flaw remediation should be incorporated into configuration management as an emergency change.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Supply Chain Risk Management (ID.SC):
The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.
Key Measure: Key Measure
Requirement: ID.SC-3.3: The organization shall establish contractual requirements permitting the organization to review the 'information security and cybersecurity' programs implemented by suppliers and third-party partners.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Supply Chain Risk Management (ID.SC):
The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.
Subcategory: ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
Requirement: IMPORTANT_ID.SC-4.1: The organization shall review assessments of suppliers' and third-party partner's compliance with contractual obligations by routinely reviewing audits, test results, and other evaluations.
Guidance: Entities not subject to the NIS legislation could limit themselves to business critical suppliers and third-party partners only.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Supply Chain Risk Management (ID.SC):
The organization's priorities, constraints, risk tolerances, and
assumptions are established and used to support risk decisions
associated with managing supply chain risk. The organization has
established and implemented the processes to identify, assess and
manage supply chain risks.
Requirement: ID.SC-4.2: The organization shall review assessments of
suppliers' and third-party partner's compliance with contractual
obligations by routinely reviewing third-party independent audits,
test results, and other evaluations.
Guidance: The depth of the review should depend on the criticality of
delivered products and services.
Documentation Score: 1
Implementation Score: 1

Function: IDENTIFY (ID)
Category: Supply Chain Risk Management (ID.SC):
The organization's priorities, constraints, risk tolerances, and
assumptions are established and used to support risk decisions
associated with managing supply chain risk. The organization has
established and implemented the processes to identify, assess and
manage supply chain risks.
Subcategory: ID.SC-5: Response and recovery planning and testing are
conducted with suppliers and third-party providers
Requirement: IMPORTANT_ID.SC-5.1: The organization shall identify and
document key personnel from suppliers and third-party partners to
include them as stakeholders in response and recovery planning
activities.
Guidance: Entities not subject to the NIS legislation could limit
themselves to business critical suppliers and third-party partners
only.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: IDENTIFY (ID)
Category: Supply Chain Risk Management (ID.SC):
The organization's priorities, constraints, risk tolerances, and
assumptions are established and used to support risk decisions
associated with managing supply chain risk. The organization has
established and implemented the processes to identify, assess and
manage supply chain risks.
Requirement: ID.SC-5.2: The organization shall identify and document
key personnel from suppliers and third-party partners to include them

as stakeholders in testing and execution of the response and recovery plans.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Key Measure: Key Measure
Subcategory: PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
Requirement: BASIC_PR.AC-1.1: Identities and credentials for authorized devices and users shall be managed.

Guidance: Identities and credentials for authorized devices and users could be managed through a password policy. A password policy is a set of rules designed to enhance ICT/OT security by encouraging organization's to:
(Not limitative list and measures to be considered as appropriate)
•   Change all default passwords.
•   Ensure that no one works with administrator privileges for daily tasks.
•   Keep a limited and updated list of system administrator accounts.
•   Enforce password rules, e.g. passwords must be longer than a state-of-the-art number of characters with a combination of character types and changed periodically or when there is any suspicion of compromise.
•   Use only individual accounts and never share passwords.
•   Immediately disable unused accounts
•   Rights and privileges are managed by user groups.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Requirement: IMPORTANT_PR.AC-1.2: Identities and credentials for authorized devices and users shall be managed, where feasible through automated mechanisms.
Guidance: •   Automated mechanisms can help to support the management and auditing of information system credentials.
•   Consider strong user authentication, meaning an authentication based on the use of at least two authentication factors from different categories of either knowledge (something only the user knows), possession (something only the user possesses) or inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way to protect the confidentiality of the authentication data.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Requirement: PR.AC-1.3: System credentials shall be deactivated after a specified period of inactivity unless it would compromise the safe operation of (critical) processes.
Guidance: •   To guarantee the safe operation, service accounts should be used for running processes and services.
•   Consider the use of a formal access procedure for external parties.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Requirement: PR.AC-1.4: For transactions within the organization's critical systems, the organization shall implement:
•   multi-factor end-user authentication (MFA or "strong authentication").
•   certificate-based authentication for system-to-system communications
Guidance: Consider the use of SSO (Single Sign On) in combination with MFA for the organization's internal and external critical systems.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Requirement: PR.AC-1.5: The organization's critical systems shall be
monitored for atypical use of system credentials. Credentials
associated with significant risk shall be disabled.
Guidance: •   Consider limiting the number of failed login attempts
by implementing automatic lockout.
•   The locked account won't be accessible until it has been reset or
the account lockout duration elapses.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Subcategory: PR.AC-2: Physical access to assets is managed and
protected
Requirement: BASIC_PR.AC-2.1: Physical access to the facility, servers
and network components shall be managed.
Guidance: •   Consider to strictly manage keys to access the
premises and alarm codes. The following rules should be considered:
o   Always retrieve an employee's keys or badges when they leave the
company permanently.
o   Change company alarm codes frequently.
o   Never give keys or alarm codes to external service providers
(cleaning agents, etc.), unless it is possible to trace these accesses
and restrict them technically to given time slots.
•   Consider to not leaving internal network access outlets
accessible in public areas. These public places can be waiting rooms,
corridors...
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and

is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Requirement: IMPORTANT_PR.AC-2.2: The management of physical access shall include measures related to access in emergency situations.
Guidance: •	Physical access controls may include, for example: lists of authorized individuals, identity credentials, escort requirements, guards, fences, turnstiles, locks, monitoring of facility access, camera surveillance.
•	The following measures should be considered:
o	Implement a badge system and create different security zones.
o	Limit physical access to servers and network components to authorized personnel.
o	Log all access to servers and network components.
•	Visitor access records should be maintained, reviewed and acted upon as required.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Requirement: PR.AC-2.3: Physical access to critical zones shall be controlled in addition to the physical access to the facility.
Guidance: E.g. production, R&D, organization's critical systems equipment (server rooms…)
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Requirement: PR.AC-2.4: Assets related to critical zones shall be physically protected.
Guidance: •	Consider protecting power equipment, power cabling, network cabling, and network access interfaces from accidental damage, disruption, and physical tampering.
•	Consider implementing redundant and physically separated power systems for organization's critical operations.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Subcategory: PR.AC-3: Remote access is managed
Requirement: BASIC_PR.AC-3.1: The organisation's wireless access
points shall be secured.
Guidance: Consider the following when wireless networking is used:
•   Change the administrative password upon installation of a
wireless access points.
•   Set the wireless access point so that it does not broadcast its
Service Set Identifier (SSID).
•   Set your router to use at least WiFi Protected Access (WPA-2 or
WPA-3 where possible), with the Advanced Encryption Standard (AES) for
encryption.
•   Ensure that wireless internet access to customers is separated
from your business network.
•   Connecting to unknown or unsecured / guest wireless access
points, should be avoided, and if unavoidable done through an
encrypted virtual private network (VPN) capability.
•   Manage all endpoint devices (fixed and mobile) according to the
organization's security policies.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Key Measure: Key Measure
Requirement: BASIC_PR.AC-3.2: The organization's networks when
accessed remotely shall be secured, including through multi-factor
authentication (MFA).
Guidance: Enforce MFA (e.g. 2FA) on Internet-facing systems, such as
email, remote desktop, and Virtual Private Network (VPNs).
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated

facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Key Measure: Key Measure
Requirement: IMPORTANT_PR.AC-3.3: Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization's critical systems environment shall be identified, documented and implemented.
Guidance: Consider the following:
•   Remote access methods include, for example, wireless, broadband, Virtual Private Network (VPN) connections, mobile device connections, and communications through external networks.
•   Login credentials should be in line with company's user authentication policies.
•   Remote access for support activities or maintenance of organizational assets should be approved, logged, and performed in a manner that prevents unauthorized access.
•   The user should be made aware of any remote connection to its device by a visual indication.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Requirement: R.AC-3.4: Remote access to the organization's critical systems shall be monitored and cryptographic mechanisms shall be implemented where determined necessary.
Guidance: This should include that only authorized use of privileged functions from remote access is allowed.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Requirement: R.AC-3.5: The security for connections with external systems shall be verified and framed by documented agreements.
Guidance: Access from pre-defined IP addresses could be considered.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Key Measure: Key Measure
Subcategory: PR.AC-4: Access permissions and authorizations are
managed, incorporating the principles of least privilege and
separation of duties
Requirement: BASIC_PR.AC-4.1: Access permissions for users to the
organization's systems shall be defined and managed.
Guidance: The following should be considered:
•   Draw up and review regularly access lists per system (files,
servers, software, databases, etc.), possibly through analysis of the
Active Directory in Windows-based systems, with the objective of
determining who needs what kind of access (privileged or not), to
what, to perform their duties in the organization.
•   Set up a separate account for each user (including any
contractors needing access) and require that strong, unique passwords
be used for each account.
•   Ensure that all employees use computer accounts without
administrative privileges to perform typical work functions. This
includes separation of personal and admin accounts.
•   For guest accounts, consider using the minimal privileges (e.g.
internet access only) as required for your business needs.
•   Permission management should be documented in a procedure and
updated when appropriate.
•   Use 'Single Sign On' (SSO) when appropriate.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Key Measure: Key Measure
Requirement: BASIC_PR.AC-4.2: It shall be identified who should have
access to the organization's business's critical information and
technology and the means to get access.
Guidance: Means to get access may include: a key, password, code, or
administrative privilege.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Key Measure: Key Measure
Requirement: BASIC_PR.AC-4.3: Employee access to data and information
shall be limited to the systems and specific information they need to
do their jobs (the principle of Least Privilege).

Guidance: The principle of Least Privilege should be understood as the
principle that a security architecture should be designed so that each
employee is granted the minimum system resources and authorizations
that the employee needs to perform its function. Consider to:
•   Not allow any employee to have access to all the business's
information.
•   Limit the number of Internet accesses and interconnections with
partner networks to the strict necessary to be able to centralize and
homogenize the monitoring of exchanges more easily.
•   Ensure that when an employee leaves the business, all access to
the business's information or systems is blocked instantly.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Key Measure: Key Measure
Requirement: BASIC_PR.AC-4.4: Nobody shall have administrator
privileges for daily tasks.

Guidance: Consider the following:
•   Separate administrator accounts from user accounts.
•   Do not privilege user accounts to effectuate administration
tasks.
•   Create unique local administrator passwords and disable unused
accounts.
•   Consider prohibiting Internet browsing from administrative
accounts.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Requirement: IMPORTANT_PR.AC-4.5: Where feasible, automated mechanisms
shall be implemented to support the management of user accounts on the
organisation's critical systems, including disabling, monitoring,
reporting and deleting user accounts.
Guidance: Consider separately identifying each person with access to
the organization's critical systems with a username to remove generic
and anonymous accounts and access.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Requirement: IMPORTANT_PR.AC-4.6: Separation of duties (SoD) shall be
ensured in the management of access rights.
Guidance: Separation of duties includes, for example:
•   dividing operational functions and system support functions among
different roles.
•   conducting system support functions with different individuals.
•   not allow a single individual to both initiate and approve a
transaction (financial or otherwise).
•   ensuring that security personnel administering access control
functions do not also administer audit functions.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Requirement: IMPORTANT_PR.AC-4.7: Priviliged users shall be managed
and monitored.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Requirement: PR.AC-4.8: Account usage restrictions for specific time
periods and locations shall be taken into account in the
organization's security access policy and applied accordingly.
Guidance: Specific restrictions can include, for example, restricting
usage to certain days of the week, time of day, or specific durations
of time.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Requirement: PR.AC-4.9: Priviliged users shall be managed, monitored
and audited.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control
(PR.AC): Access to physical and logical assets and associated
facilities is limited to authorized users, processes, and devices, and
is managed consistent with the assessed risk of unauthorized access to
authorized activities and transactions.
Key Measure: Key Measure
Subcategory: PR.AC-5: Network integrity is protected (e.g., network
segregation, network segmentation)
Requirement: BASIC_PR.AC-5.1: Firewalls shall be installed and
activated on all the organization's networks.
Guidance: Consider the following:
•   Install and operate a firewall between your internal network and
the Internet. This may be a function of a (wireless) access
point/router, or it may be a function of a router provided by the
Internet Service Provider (ISP).
•   Ensure there is antivirus software installed on purchased
firewall solutions and ensure that the administrator's log-in and

administrative password is changed upon installation and regularly thereafter.
•   Install, use, and update a software firewall on each computer system (including smart phones and other networked devices).
•   Have firewalls on each of your computers and networks even if you use a cloud service provider or a virtual private network (VPN). Ensure that for telework home network and systems have hardware and software firewalls installed, operational, and regularly updated.
•   Consider installing an Intrusion Detection / Prevention System (IDPS). These devices analyze network traffic at a more detailed level and can provide a greater level of protection.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Key Measure: Key Measure
Requirement: BASIC_PR.AC-5.2: Where appropriate, network integrity of the organization's critical systems shall be protected by incorporating network segmentation and segregation.
Guidance: •   Consider creating different security zones in the network (e.g. Basic network segmentation through VLAN's or other network access control mechanisms) and control/monitor the traffic between these zones.
•   When the network is "flat", the compromise of a vital network component can lead to the compromise of the entire network.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Key Measure: Key Measure
Requirement: IMPORTANT_PR.AC-5.3: Where appropriate, network integrity of the organization's critical systems shall be protected by
(1) Identifying, documenting, and controlling connections between system components.
(2) Limiting external connections to the organization's critical systems.

Guidance: Boundary protection mechanisms include, for example, routers, gateways, unidirectional gateways, data diodes, and firewalls separating system components into logically separate networks or subnetworks.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Key Measure: Key Measure
Requirement: IMPORTANT_PR.AC-5.4: The organization shall monitor and control connections and communications at the external boundary and at key internal boundaries within the organization's critical systems by implementing boundary protection devices where appropriate.
Guidance: Consider implementing the following recommendations:
• 	Separate your public WIFI network from your business network.
• 	Protect your business WIFI with state-of-the-art encryption.
• 	Implement a Network Access Control (NAC) solution.
• 	Encrypt connections to your corporate network.
• 	Divide your network according to security levels and apply firewall rules. Isolate your networks for server administration.
• 	Force VPN on public networks.
• 	Implement a closed policy for security gateways (deny all policy: only allow/open connections that have been explicitly pre-authorized).
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Requirement: PR.AC-5.5: The organization shall implement, where feasible, authenticated proxy servers for defined communications traffic between the organization's critical systems and external networks.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)

Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Requirement: PR.AC-5.6: The organization shall ensure that the organization's critical systems fail safely when a border protection device fails operationally.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Subcategory: PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions
Requirement: IMPORTANT_PR.AC-6.1: The organization shall implement documented procedures for verifying the identity of individuals before issuing credentials that provide access to organization's systems.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Requirement: PR.AC-6.2: The organization shall ensure the use of unique credentials bound to each verified user, device, and process interacting with the organization's critical systems; make sure that they are authenticated, and that the unique identifiers are captured when performing system interactions.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)

Category: Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Key Measure: Key Measure
Subcategory: PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
Requirement: IMPORTANT_PR.AC-7.1: The organization shall perform a documented risk assessment on organization's critical system transactions and authenticate users, devices, and other assets (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
Guidance: Consider a security-by-design approach for new systems; For existing systems a separate risk assessment should be used.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
Subcategory: PR.AT-1: All users are informed and trained
Requirement: BASIC_PR.AT-1.1: Employees shall be trained as appropriate.
Guidance: •   Employees include all users and managers of the ICT/OT systems, and they should be trained immediately when hired and regularly thereafter about the company's information security policies and what they will be expected to do to protect company's business information and technology.
•   Training should be continually updated and reinforced by awareness campaigns.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
Requirement: IMPORTANT_PR.AT-1.2: The organization shall incorporate insider threat recognition and reporting into security awareness training.
Guidance: Consider to:
• Communicate and discuss regularly to ensure that everyone is aware of their responsibilities.
• Develop an outreach program by gathering in a document the messages you want to convey to your staff (topics, audiences, objectives, etc.) and your communication rhythm on a calendar (weekly, monthly, one-time, etc.). Communicate continuously and in an engaging way, involving management, IT colleagues, the ICT service provider and HR and Communication managers.
• Cover topics such as: recognition of fraud attempts, phishing, management of sensitive information, incidents, etc. The goal is for all employees to understand ways to protect company information.
• Discuss with your management, your ICT colleagues, or your ICT service provider some practice scenarios (e.g. what to do if a virus alert is triggered, if a storm cuts off the power, if data is blocked, if an account is hacked, etc.), determine what behaviours to adopt, document and communicate them to all your staff. The central point of contact in the event of an incident should be known to all.
• Organize a simulation of a scenario to test your knowledge. Consider performing the exercise for example at least once a year.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
Requirement: PR.AT-1.3: The organization shall implement an evaluation method to measure the effectiveness of the awareness trainings.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and

responsibilities consistent with related policies, procedures, and agreements.
Subcategory: PR.AT-2: Privileged users understand their roles and responsibilities
Requirement: IMPORTANT_PR.AT-2.1: Privileged users shall be qualified before privileges are granted, and these users shall be able to demonstrate the understanding of their roles, responsibilities, and authorities.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
Subcategory: PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
Requirement: IMPORTANT_PR.AT-3.1: The organization shall establish and enforce security requirements for business-critical third-party providers and users.
Guidance: Enforcement should include that 'third party stakeholder'-users (e.g. suppliers, customers, partners) can demonstrate the understanding of their roles and responsibilities.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
Requirement: IMPORTANT_PR.AT-3.2: Third-party providers shall be required to notify any personnel transfers, termination, or transition involving personnel with physical or logical access to organization's business critical system's components.
Guidance: Third-party providers include, for example, service providers, contractors, and other organizations providing system development, technology services, outsourced applications, or network and security management.
Documentation Score: 1

Implementation Score: 1

Function: PROTECT (PR)
Category: Awareness and Training (PR.AT): The organization's personnel
and partners are provided cybersecurity awareness education and are
trained to perform their cybersecurity-related duties and
responsibilities consistent with related policies, procedures, and
agreements.
Requirement: IMPORTANT_PR.AT-3.3: The organization shall monitor
business critical service providers and users for security compliance.
Guidance: Third party audit results can be used as audit evidence.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Awareness and Training (PR.AT): The organization's personnel
and partners are provided cybersecurity awareness education and are
trained to perform their cybersecurity-related duties and
responsibilities consistent with related policies, procedures, and
agreements.
Requirement: PR.AT-3.4: The organization shall audit business-critical
external service providers for security compliance.
Guidance: Third party audit results can be used as audit evidence.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Awareness and Training (PR.AT): The organization's personnel
and partners are provided cybersecurity awareness education and are
trained to perform their cybersecurity-related duties and
responsibilities consistent with related policies, procedures, and
agreements.
Subcategory: PR.AT-4: Senior executives understand their roles and
responsibilities
Requirement: IMPORTANT_PR.AT-4.1: Senior executives shall demonstrate
the understanding of their roles, responsibilities, and authorities.
Guidance: Guidance on role profiles along with their identified
titles, missions, tasks, skills, knowledge, competences is available
in the "European Cybersecurity Skills Framework Role Profiles" by
ENISA. (https://www.enisa.europa.eu/publications/european-
cybersecurity-skills-framework-role-profiles)
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
Subcategory: PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities
Requirement: IMPORTANT_PR.AT-5.1: The organization shall ensure that personnel responsible for the physical protection and security of the organization's critical systems and facilities are qualified through training before privileges are granted, and that they understand their responsibilities.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Subcategory: PR.DS-1: Data-at-rest is protected
Requirement: PR.DS-1.1: The organization shall protect its critical system information determined to be critical/ sensitive while at rest.
Guidance: •   Consider using encryption techniques for data storage, data transmission or data transport (e.g., laptop, USB).
•   Consider encrypting end-user devices and removable media containing sensitive data (e.g. hard disks, laptops, mobile device, USB storage devices, …). This could be done by e.g. Windows BitLocker®, VeraCrypt, Apple FileVault®, Linux® dm-crypt,…
•   Consider encrypting sensitive data stored in the cloud.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Guidance: The below measures should be considered:

•   Implement dedicated safeguards to prevent unauthorized access, distortion, or modification of system data and audit records (e.g. restricted access rights, daily backups, data encryption, firewall installation).
•   Encrypt hard drives, external media, stored files, configuration files and data stored in the cloud.

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Subcategory: PR.DS-2: Data-in-transit is protected
Requirement: PR.DS-2.1: The organization shall protect its critical system information determined to be critical when in transit.
Guidance: When the organization often sends sensitive documents or e-mails, it is recommended to encrypt those documents and/or e-mails with appropriate, supported, and authorized software tools.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Guidance: If you send sensitive documents or emails, you may want to consider encrypting those documents and/or emails with appropriate, supported, and authorized software tools.

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Subcategory: PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
Requirement: BASIC_PR.DS-3.1: Assets and media shall be disposed of safely.
Guidance: •   When eliminating tangible assets like business computers/laptops, servers, hard drive(s) and other storage media (USB drives, paper…), ensure that all   sensitive business or personal data are securely deleted (i.e. electronically "wiped") before they are removed and then physically destroyed (or re-commissioned). This is also known as "sanitization" and thus related to the requirement and guidance in PR.IP-6.

- Consider installing a remote-wiping application on company laptops, tablets, cell phones, and other mobile devices.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Requirement: IMPORTANT_PR.DS-3.2: The organization shall enforce accountability for all its business-critical assets throughout the system lifecycle, including removal, transfers, and disposition.
Guidance: Accountability should include:
- The authorization for business-critical assets to enter and exit the facility.
- Monitoring and maintaining documentation related to the movements of business-critical assets.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Requirement: IMPORTANT_PR.DS-3.3: The organization shall ensure that the necessary measures are taken to deal with loss, misuse, damage, or theft of assets.
Guidance: This can be done by policies, processes & procedures (reporting), technical & organizational means (encryption, Access Control (AC), Mobile Device Management (MDM), monitoring, secure wipe, awareness, signed user agreement, guidelines & manuals, backups, inventory update …).
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Requirement: PR.DS-3.4: The organization shall ensure that disposal actions are approved, tracked, documented, and verified.
Guidance: Disposal actions include media sanitization actions (See PR.IP-6)
Documentation Score: 1

Implementation Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are
managed consistent with the organization's risk strategy to protect
the confidentiality, integrity, and availability of information.
Subcategory: PR.DS-4: Adequate capacity to ensure availability is
maintained
Requirement: IMPORTANT_PR.DS-4.1: Capacity planning shall ensure
adequate resources for organization's critical system information
processing, networking, telecommunications, and data storage.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are
managed consistent with the organization's risk strategy to protect
the confidentiality, integrity, and availability of information.
Requirement: IMPORTANT_PR.DS-4.2: Audit data from the organization's
critical systems shall be moved to an alternative system.
Guidance: Be aware that log services can become a bottleneck and
hinder the correct functioning of the source systems.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are
managed consistent with the organization's risk strategy to protect
the confidentiality, integrity, and availability of information.
Requirement: PR.DS-4.3: The organization's critical systems shall be
protected against denial-of-service attacks or at least the effect of
such attacks will be limited.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are
managed consistent with the organization's risk strategy to protect
the confidentiality, integrity, and availability of information.
Key Measure: Key Measure

Subcategory: PR.DS-5: Protections against data leaks are implemented
Requirement: IMPORTANT_PR.DS-5.1: The organization shall take appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorized access and activities, including data leakage, is detected.
Guidance: •   Consider implementing dedicated protection measures (restricted access rights, daily backups, data encryption, installation of firewalls, etc.) for the most sensitive data.
•   Consider frequent audit of the configuration of the central directory (Active Directory in Windows environment), with specific focus on the access to data of key persons in the company.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Subcategory: PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
Requirement: IMPORTANT_PR.DS-6.1: The organization shall implement software, firmware, and information integrity checks to detect unauthorized changes to its critical system components during storage, transport, start-up and when determined necessary.
Guidance: State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Requirement: PR.DS-6.2: The organization shall implement automated tools where feasible to provide notification upon discovering discrepancies during integrity verification.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Requirement: PR.DS-6.3: The organization shall implement automatic response capability with pre-defined security safeguards when integrity violations are discovered.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Subcategory: PR.DS-7: The development and testing environment(s) are separate from the production environment
Requirement: PR.DS-7.1: The development and test environment(s) shall be isolated from the production environment.
Guidance: •   Any change one wants to make to the ICT/OT environment should first be tested in an environment that is different and separate from the production environment (operational environment) before that change is effectively implemented . That way, the effect of those changes can be analysed and adjustments can be made without disrupting operational activities.
•   Consider adding and testing cybersecurity features as early as during development (secure development lifecycle principles).
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Guidance: •   Any change one wants to make to the ICT/OT environment should first be tested in an environment that is different and separate from the production environment (operational environment) before that change is effectively implemented . That way, the effect of those changes can be analysed and adjustments can be made without disrupting operational activities.
•   Consider adding and testing cybersecurity features as early as during development (secure development lifecycle principles).

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Subcategory: PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity
Requirement: PR.DS-8.1: The organization shall implement hardware integrity checks to detect unauthorized tampering to its critical system's hardware.
Guidance: State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
Requirement: PR.DS-8.2: The organization shall incorporate the detection of unauthorized tampering to its critical system's hardware into the organization incident response capability.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Key Measure: Key Measure
Subcategory: PR.IP-1: A baseline configuration of information
technology/industrial control systems is created and maintained
incorporating security principles (e.g. concept of least
functionality)
Requirement: IMPORTANT_PR.IP-1.1: The organization shall develop,
document, and maintain a baseline configuration for the its business
critical systems.
Guidance: •   This control includes the concept of least
functionality.
•   Baseline configurations include for example, information about
organization's business critical systems, current version numbers and
patch information on operating systems and applications, configuration
settings/parameters, network topology, and the logical placement of
those components within the system architecture.
•   Network topology should include the nerve points of the IT/OT
environment (external connections, servers hosting data and/or
sensitive functions, DNS services security, etc.).
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP):
Security policies (that address purpose, scope, roles,
responsibilities, management commitment, and coordination among
organizational entities), processes, and procedures are maintained and
used to manage protection of information systems and assets.

Requirement: PR.IP-1.2: The organization shall configure its business-critical systems to provide only essential capabilities; Therefore the baseline configuration shall be reviewed, and unnecessary capabilities disabled.
Guidance: •   Configuration of a system to provide only organization-defined mission essential capabilities is known as the "concept of least functionality".
•   Capabilities include functions, ports, protocols, software, and/or services.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Subcategory: PR.IP-2: A System Development Life Cycle to manage systems is implemented
Requirement: IMPORTANT_PR.IP-2.1: The system and application development life cycle shall include security considerations.
Guidance: •   System and application development life cycle should include the acquisition process of the organization's business critical systems and its components.
•   Vulnerability awareness and prevention training for (web application) developers, and advanced social engineering awareness training for high-profile roles should be considered.
•   When hosting internet facing applications the implementation of a web application firewall (WAF) should be considered.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP):
Security policies (that address purpose, scope, roles,
responsibilities, management commitment, and coordination among
organizational entities), processes, and procedures are maintained and
used to manage protection of information systems and assets.

Requirement: PR.IP-2.2: The development process for critical systems
and system components shall cover the full design cycle and shall
provide a description of the functional properties of security
controls, and design and implementation information for security-
relevant system interfaces.
Guidance: The development cycle includes:
•   All development phases: specification , design, development,
implementation.
•   Configuration management for planned and unplanned changes and
change control during the development.
•   Flaw tracking & resolution.
•   Security testing.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP):
Security policies (that address purpose, scope, roles,
responsibilities, management commitment, and coordination among
organizational entities), processes, and procedures are maintained and
used to manage protection of information systems and assets.

Subcategory: PR.IP-3: Configuration change control processes are in place
Requirement: IMPORTANT_PR.IP-3.1: Changes shall be tested and validated before being implemented into operational systems.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Requirement: PR.IP-3.2: For planned changes to the organization's critical systems, a security impact analysis shall be performed in a separate test environment before implementation in an operational environment.
Guidance: No additional guidance on this topic.
Documentation Score: 1

Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP):
Security policies (that address purpose, scope, roles,
responsibilities, management commitment, and coordination among
organizational entities), processes, and procedures are maintained and
used to manage protection of information systems and assets.

Key Measure: Key Measure
Subcategory: PR.IP-4: Backups of information are conducted,
maintained, and tested
Requirement: BASIC_PR.IP-4.1: Backups for organization's business
critical data shall be conducted and stored on a system different from
the device on which the original data resides
Guidance: •   Organization's business critical system's data
includes for example software, configurations and settings,
documentation, system configuration data including computer
configuration backups, application configuration backups, etc.
•   Consider a regular backup and put it offline periodically.
•   Recovery time and recovery point objectives should be considered.
•   Consider not storing the organization's data backup on the same
network as the system on which the original data resides and provide
an offline copy. Among other things, this prevents file encryption by
hackers (risk of ransomware).
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP):
Security policies (that address purpose, scope, roles,

responsibilities, management commitment, and coordination among
organizational entities), processes, and procedures are maintained and
used to manage protection of information systems and assets.

Requirement: IMPORTANT_PR.IP-4.2: The reliability and integrity of
backups shall be verified and tested on regular basis.
Guidance: This should include regularly testing of the backup restore
procedures.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP):
Security policies (that address purpose, scope, roles,
responsibilities, management commitment, and coordination among
organizational entities), processes, and procedures are maintained and
used to manage protection of information systems and assets.

Requirement: IMPORTANT_PR.IP-4.3: A separate alternate storage site for system backups shall be operated and the same security safeguards as the primary storage location shall be employed.
Guidance: An offline backup of your data is ideally stored in a separate physical location from the original data source and where feasible offsite for extra protection and security.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Requirement: PR.IP-4.4: Backup verification shall be coordinated with the functions in the organization that are responsible for related plans.
Guidance: •   Related plans include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Cyber Incident response plans.
•   Restoration of backup data during contingency plan testing should be provided.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among

organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Requirement: PR.IP-4.5: Critical system backup shall be separated from critical information backup.
Guidance: Seperation of critical system backup from critical information backup should lead to a shorter recovery time.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Subcategory: PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met

Requirement: IMPORTANT_PR.IP-5.1: The organization shall define, implement, and enforce policy and procedures regarding emergency and safety systems, fire protection systems, and environment controls for its critical systems.
Guidance: The below measures should be considered:
• Protect unattended computer equipment with padlocks or a locker and key system.
• Fire suppression mechanisms should take the organization's critical system environment into account (e.g., water sprinkler systems could be hazardous in specific environments).
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Requirement: PR.IP-5.2: The organization shall implement fire detection devices that activate and notify key personnel automatically in the event of a fire.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among

organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Subcategory: PR.IP-6: Data is destroyed according to policy
Requirement: IMPORTANT_PR.IP-6.1: The organization shall ensure that its critical system's data is destroyed according to policy.
Guidance: •   Disposal actions include media sanitization actions (See PR.DS-3)
•   There are two primary types of media in common use:
o   Hard copy media (physical representations of information)
o   Electronic or soft copy media (the bits and bytes contained in hard drives, random access memory (RAM), read-only memory (ROM), disks, memory devices, phones, mobile computing devices, networking equipment…)
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Requirement: PR.IP-6.2: Sanitation processes shall be documented and tested.
Guidance: •   Sanitation processes include procedures and equipment.
•   Consider applying non-destructive sanitization techniques to portable storage devices.
•   Consider sanitation procedures in proportion to confidentiality requirements.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Subcategory: PR.IP-7: Protection processes are improved
Requirement: IMPORTANT_PR.IP-7.1: The organization shall incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into protection process updates (continuous improvement).
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Requirement: PR.IP-7.2: The organization shall implement independent teams to assess the protection process(es).
Guidance: Independent teams, for example, may include internal or external impartial personnel.
Impartiality implies that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, or management of the organization's critical system under assessment or to the determination of security control effectiveness.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Requirement: PR.IP-7.3: The organization shall ensure that the security plan for its critical systems facilitates the review, testing, and continual improvement of the security protection processes.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Subcategory: PR.IP-8: Effectiveness of protection technologies is shared
Requirement: IMPORTANT_PR.IP-8.1: The organization shall collaborate and share information about its critical system's related security incidents and mitigation measures with designated partners.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Information Protection Processes and Procedures (PR.IP):
Security policies (that address purpose, scope, roles,
responsibilities, management commitment, and coordination among
organizational entities), processes, and procedures are maintained and
used to manage protection of information systems and assets.

Requirement: IMPORTANT_PR.IP-8.2: Communication of effectiveness of
protection technologies shall be shared with appropriate parties.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP):
Security policies (that address purpose, scope, roles,
responsibilities, management commitment, and coordination among
organizational entities), processes, and procedures are maintained and
used to manage protection of information systems and assets.

Requirement: IMPORTANT_PR.IP-8.3: The organization shall implement,
where feasible, automated mechanisms to assist in information
collaboration.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP):
Security policies (that address purpose, scope, roles,
responsibilities, management commitment, and coordination among
organizational entities), processes, and procedures are maintained and
used to manage protection of information systems and assets.

Subcategory: PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

Requirement: IMPORTANT_PR.IP-9.1: Incident response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) shall be established, maintained, approved, and tested to determine the effectiveness of the plans, and the readiness to execute the plans.

Guidance: •   The incident response plan is the documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack.
•   Plans should incorporate recovery objectives, restoration priorities, metrics, contingency roles, personnel assignments and contact information.
•   Maintaining essential functions despite system disruption, and the eventual restoration of the organization's systems, should be addressed.
•   Consider defining incident types, resources and management support needed to effectively maintain and mature the incident response and contingency capabilities.

Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Requirement: PR.IP-9.2: The organization shall coordinate the
development and the testing of incident response plans and recovery
plans with stakeholders responsible for related plans.
Guidance: Related plans include, for example, Business Continuity
Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis
Communications Plans, Critical Infrastructure Plans, Cyber incident
response plans, and Occupant Emergency Plans.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP):
Security policies (that address purpose, scope, roles,
responsibilities, management commitment, and coordination among
organizational entities), processes, and procedures are maintained and
used to manage protection of information systems and assets.

Subcategory: PR.IP-11: Cybersecurity is included in human resources
practices (e.g., deprovisioning, personnel screening)
Requirement: BASIC_PR.IP-11.1: Personnel having access to the
organization's most critical information or technology shall be
verified.
Guidance: •   The access to critical information or technology
should be considered when recruiting, during employment and at
termination.
•   Background verification checks should take into consideration
applicable laws, regulations, and ethics in proportion to the business
requirements, the classification of the information to be accessed and
the perceived risks.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP):
Security policies (that address purpose, scope, roles,
responsibilities, management commitment, and coordination among
organizational entities), processes, and procedures are maintained and
used to manage protection of information systems and assets.

Requirement: IMPORTANT_PR.IP-11.2: Develop and maintain a human
resource information/cyber security process that is applicable when
recruiting, during employment and at termination of employment.
Guidance: The human resource information/cyber security process should
include access to critical information or technology; background
verification checks; code of conduct; roles, authorities, and
responsibilities…
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Information Protection Processes and Procedures (PR.IP):
Security policies (that address purpose, scope, roles,
responsibilities, management commitment, and coordination among
organizational entities), processes, and procedures are maintained and
used to manage protection of information systems and assets.

Subcategory: PR.IP-12: A vulnerability management plan is developed
and implemented
Requirement: IMPORTANT_PR.IP-12.1: The organization shall establish
and maintain a documented process that allows continuous review of
vulnerabilities and strategies to mitigate them.
Guidance: •   Consider inventorying sources likely to report
vulnerabilities in the identified components and distribute updates
(software publisher websites, CERT website, ENISA website).

• The organization should identify where its critical system's vulnerabilities may be exposed to adversaries.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
Key Measure: Key Measure
Subcategory: PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
Requirement: BASIC_PR.MA-1.1: Patches and security updates for Operating Systems and critical system components shall be installed.
Guidance: The following should be considered:
• Limit yourself to only install those applications (operating systems, firmware, or plugins) that you need to run your business and patch/update them regularly.
• You should only install a current and vendor-supported version of software you choose to use. It may be useful to assign a day each month to check for patches.
• There are products which can scan your system and notify you when there is an update for an application you have installed. If you use one of these products, make sure it checks for updates for every application you use.
• Install patches and security updates in a timely manner.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
Requirement: IMPORTANT_PR.MA-1.2: The organization shall plan, perform and document preventive maintenance and repairs on its critical system components according to approved processes and tools.
Guidance: Consider the below measures:
(1) Perform security updates on all software in a timely manner.
(2) Automate the update process and audit its effectiveness.
(3) Introduce an internal patching culture on desktops, mobile devices, servers, network components, etc. to ensure updates are tracked.

Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
Requirement: IMPORTANT_PR.MA-1.3: The organization shall enforce approval requirements, control, and monitoring of maintenance tools for use on the its critical systems.
Guidance: Maintenance tools can include, for example, hardware/software diagnostic test equipment, hardware/software packet sniffers and laptops.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
Requirement: IMPORTANT_PR.MA-1.4: The organization shall verify security controls following hardware maintenance or repairs, and take action as appropriate.
Guidance: No additional guidance on this topic
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
Key Measure: Key Measure
Requirement: PR.MA-1.5: The organization shall prevent the unauthorized removal of maintenance equipment containing organization's critical system information.
Guidance: This requirement maily focuses mainly on OT/ICS environments.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

Key Measure: Key Measure
Requirement: PR.MA-1.6: Maintenance tools and portable storage devices
shall be inspected when brought into the facility and shall be
protected by anti-malware solutions so that they are scanned for
malicious code before they are used on organization's systems.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Maintenance (PR.MA): Maintenance and repairs of industrial
control and information system components are performed consistent
with policies and procedures.
Key Measure: Key Measure
Requirement: PR.MA-1.7: The organization shall verify security
controls following hardware and software maintenance or
repairs/patching and take action as appropriate.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Maintenance (PR.MA): Maintenance and repairs of industrial
control and information system components are performed consistent
with policies and procedures.
Subcategory: PR.MA-2: Remote maintenance of organizational assets is
approved, logged, and performed in a manner that prevents unauthorized
access
Requirement: IMPORTANT_PR.MA-2.1: Remote maintenance shall only occur
after prior approval, monitoring to avoid unauthorised access, and
approval of the outcome of the maintenance activities as described in
approved processes or procedures.
Guidance: No additional guidance on this topic
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Maintenance (PR.MA): Maintenance and repairs of industrial
control and information system components are performed consistent
with policies and procedures.
Requirement: IMPORTANT_PR.MA-2.2: The organization shall make sure
that strong authenticators, record keeping, and session termination
for remote maintenance is implemented.
Guidance: No additional guidance on this topic

Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Maintenance (PR.MA): Maintenance and repairs of industrial
control and information system components are performed consistent
with policies and procedures.
Requirement: PR.MA-2.3: The organization shall require that diagnostic
services pertaining to remote maintenance be performed from a system
that implements a security capability comparable to the capability
implemented on the equivalent organization's critical system.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions
are managed to ensure the security and resilience of systems and
assets, consistent with related policies, procedures, and agreements.
Key Measure: Key Measure
Subcategory: PR.PT-1: Audit/log records are determined, documented,
implemented, and reviewed in accordance with policy
Requirement: BASIC_PR.PT-1.1: Logs shall be maintained, documented,
and reviewed.
Guidance: •   Ensure the activity logging functionality of
protection / detection hardware or software (e.g. firewalls, anti-
virus) is enabled.
•   Logs should be backed up and saved for a predefined period.
•   The logs should be reviewed for any unusual or unwanted trends,
such as a large use of social media websites or an unusual number of
viruses consistently found on a particular computer. These trends may
indicate a more serious problem or signal the need for stronger
protections in a particular area.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions
are managed to ensure the security and resilience of systems and
assets, consistent with related policies, procedures, and agreements.
Requirement: IMPORTANT_PR.PT-1.2: The organization shall ensure that
the log records include an authoritative time source or internal clock

time stamp that are compared and synchronized to an authoritative
time source.
Guidance: Authoritative time sources include for example, an internal
Network Time Protocol (NTP) server, radio clock, atomic clock, GPS
time source.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions
are managed to ensure the security and resilience of systems and
assets, consistent with related policies, procedures, and agreements.
Requirement: PR.PT-1.3: The organization shall ensure that audit
processing failures on the organization's systems generate alerts and
trigger defined responses.
Guidance: The use of System Logging Protocol (Syslog) servers can be
considered.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions
are managed to ensure the security and resilience of systems and
assets, consistent with related policies, procedures, and agreements.
Requirement: PR.PT-1.4: The organization shall enable authorized
individuals to extend audit capabilities when required by events.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions
are managed to ensure the security and resilience of systems and
assets, consistent with related policies, procedures, and agreements.
Subcategory: PR.PT-2: Removable media is protected and its use
restricted according to policy
Requirement: IMPORTANT_PR.PT-2.1: The usage restriction of portable
storage devices shall be ensured through an appropriate documented
policy and supporting safeguards.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
Requirement: IMPORTANT_PR.PT-2.2: The organisation should technically prohibit the connection of removable media unless strictly necessary; in other instances, the execution of autoruns from such media should be disabled.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
Key Measure: Key Measure
Requirement: PR.PT-2.3: Portable storage devices containing system data shall be controlled and protected while in transit and in storage.
Guidance: Protection and control should include the scanning of all portable storage devices for malicious code before they are used on organization's systems.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
Subcategory: PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
Requirement: IMPORTANT_PR.PT-3.1: The organization shall configure the business critical systems to provide only essential capabilities.
Guidance: Consider applying the principle of least functionality to access systems and assets (see also PR.AC-4).
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)

Category: Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
Requirement: PR.PT-3.2: The organization shall disable defined functions, ports, protocols, and services within its critical systems that it deems unnecessary.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
Requirement: PR.PT-3.3: The organization shall implement technical safeguards to enforce a deny-all, permit-by-exception policy to only allow the execution of authorized software programs.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
Subcategory: PR.PT-4: Communications and control networks are protected
Requirement: BASIC_PR.PT-4.1: Web and e-mail filters shall be installed and used.
Guidance: •   E-mail filters should detect malicious e-mails, and filtering should be configured based on the type of message attachments so that files of the specified types are automatically processed (e.g. deleted).
•   Web-filters should notify the user if a website may contain malware and potentially preventing users from accessing that website.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Requirement: PR.PT-4.2: The organization shall control the information flows/data flows within its critical systems and between interconnected systems.
Guidance: Consider the following:
• Information flow may be supported, for example, by labelling or colouring physical connectors as an aid to manual hook-up.
• Inspection of message content may enforce information flow policy. For example, a message containing a command to an actuator may not be permitted to flow between the control network and any other network.
• Physical addresses (e.g., a serial port) may be implicitly or explicitly associated with labels or attributes (e.g., hardware I/O address). Manual methods are typically static. Label or attribute policy mechanisms may be implemented in hardware, firmware, and software that controls or has device access, such as device drivers and communications controllers.
Documentation Score: 1
Implementation Score: 1

Function: PROTECT (PR)
Category: Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
Requirement: PR.PT-4.3: The organization shall manage the interface for external communication services by establishing a traffic flow policy, protecting the confidentiality and integrity of the information being transmitted; This includes the review and documenting of each exception to the traffic flow policy.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.
Key Measure: Key Measure
Subcategory: DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed
Requirement: DE.AE-1.1: The organization shall ensure that a baseline of network operations and expected data flows for its critical systems is developed, documented and maintained to track events.
Guidance: • Consider enabling local logging on all your systems and network devices and keep them for a certain period, for example up to 6 months.
• Ensure that your logs contain enough information (source, date, user, timestamp, etc.) and that you have enough storage space for their generation.
• Consider centralizing your logs.

• 	Consider deploying a Security Information and Event Management tool (SIEM) that will facilitate the correlation and analysis of your data.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.
Subcategory: DE.AE-2: Detected events are analyzed to understand attack targets and methods
Requirement: IMPORTANT_DE.AE-2.1: The organization shall review and analyze detected events to understand attack targets and methods.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.
Requirement: DE.AE-2.2: The organization shall implement automated mechanisms where feasible to review and analyze detected events.
Guidance: Consider to review your logs regularly to identify anomalies or abnormal events.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.
Key Measure: Key Measure
Subcategory: DE.AE-3: Event data are collected and correlated from multiple sources and sensors
Requirement: BASIC_DE.AE-3.1: The activity logging functionality of protection / detection hardware or software
(e.g. firewalls, anti-virus) shall be enabled, backed-up and reviewed.
Guidance: • 	Logs should be backed up and saved for a predefined period.
• 	The logs should be reviewed for any unusual or unwanted trends, such as a large use of social media websites or an unusual number of

viruses consistently found on a particular computer. These trends may indicate a more serious problem or signal the need for stronger protections in a particular area.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.
Requirement: IMPORTANT_DE.AE-3.2: The organization shall ensure that event data is compiled and correlated across its critical systems using various sources such as event reports, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.
Requirement: DE.AE-3.3: The organization shall integrate analysis of events where feasible with the analysis of vulnerability scanning information; performance data; its critical system's monitoring, and facility monitoring to further enhance the ability to identify inappropriate or unusual activity.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.
Subcategory: DE.AE-4: Impact of events is determined
Requirement: DE.AE-4.1: Negative impacts to organization's operations, assets, and individuals resulting from detected events shall be determined and correlated with risk assessment outcomes.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Anomalies and Events (DE.AE): Anomalous activity is detected
and the potential impact of events is understood.
Subcategory: DE.AE-5: Incident alert thresholds are established
Requirement: IMPORTANT_DE.AE-5.1: The organization shall implement
automated mechanisms and system generated alerts to support event
detection and to assist in the identification of security alert
thresholds.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Anomalies and Events (DE.AE): Anomalous activity is detected
and the potential impact of events is understood.
Requirement: IMPORTANT_DE.AE-5.2: The organization shall define
incident alert thresholds.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information
system and assets are monitored to identify cybersecurity events and
verify the effectiveness of protective measures.
Subcategory: DE.CM-1: The network is monitored to detect potential
cybersecurity events
Requirement: BASIC_DE.CM-1.1: Firewalls shall be installed and
operated on the network boundaries and completed with firewall
protection on the endpoints.
Guidance: •   Endpoints include desktops, laptops, servers...
•   Consider, where feasible, including smart phones and other
networked devices when installing and operating firewalls.
•   Consider limiting the number of interconnection gateways to the
Internet.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: DETECT (DE)

Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Key Measure: Key Measure
Requirement: IMPORTANT_DE.CM-1.2: The organization shall monitor and identify unauthorized use of its business critical systems through the detection of unauthorized local connections, network connections and remote connections.
Guidance: •   Monitoring of network communications should happen at the external boundary of the organization's business critical systems and at key internal boundaries within the systems.
•   When hosting internet facing applications the implementation of a web application firewall (WAF) should be considered.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Requirement: DE.CM-1.3: The organization shall conduct ongoing security status monitoring of its network to detect defined information/cybersecurity events and indicators of potential information/cybersecurity events.
Guidance: Security status monitoring should include:
•   The generation of system alerts when indications of compromise or potential compromise occur.
•   Detection and reporting of atypical usage of organization's critical systems.
•   The establishment of audit records for defined information/cybersecurity events.
•   Boosting system monitoring activity whenever there is an indication of increased risk.
•   Physical environment, personnel, and service provider.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Subcategory: DE.CM-2: The physical environment is monitored to detect potential cybersecurity events
Requirement: IMPORTANT_DE.CM-2.1: The physical environment of the facility shall be monitored for potential information/cybersecurity events.
Guidance: No additional guidance on this topic.
Documentation Score: 1

Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Requirement: DE.CM-2.2: The physical access to organization's critical systems and devices shall be, on top of the physical access monitoring to the facility, increased through physical intrusion alarms, surveillance equipment, independent surveillance teams.
Guidance: It is recommended to log all visitors.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Subcategory: DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
Requirement: BASIC_DE.CM-3.1: End point and network protection tools to monitor end-user behavior for dangerous activity shall be implemented.
Guidance: Consider deploying an Intrusion Detection/Prevention system (IDS/IPS).
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Requirement: IMPORTANT_DE.CM-3.2: End point and network protection tools that monitor end-user behavior for dangerous activity shall be managed.
Guidance: Consider using a centralized log platform for the consolidation and exploitation of log files.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Guidance: Consider to actively investigate the alerts generated because of suspicious activities and take the appropriate actions to remediate the threat, e.g. through the deployment of a security operations centre (SOC).

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Requirement: IMPORTANT_DE.CM-3.3: Software usage and installation restrictions shall be enforced.
Guidance: Only authorized software should be used and user access rights should be limited to the specific data, resources and applications needed to complete a required task (least privilege principle).
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Key Measure: Key Measure
Subcategory: DE.CM-4: Malicious code is detected
Requirement: BASIC_DE.CM-4.1: Anti-virus, -spyware, and other -malware programs shall be installed and updated.
Guidance: •   Malware includes viruses, spyware, and ransomware and should be countered by installing, using, and regularly updating anti-virus and anti-spyware software on every device used in company's business (including computers, smart phones, tablets, and servers).
•   Anti-virus and anti-spyware software should automatically check for updates in "real-time" or at least daily followed by system scanning as appropriate.
•   It should be considered to provide the same malicious code protection mechanisms for home computers (e.g. teleworking) or personal devices that are used for professional work (BYOD).
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)

Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Requirement: DE.CM-4.2: The organisation shall set up a system to detect false positives while detecting and eradicating malicious code.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Subcategory: DE.CM-5: Unauthorized mobile code is detected
Requirement: IMPORTANT_DE.CM-5.1: The organization shall define acceptable and unacceptable mobile code and mobile code technologies; and authorize, monitor, and control the use of mobile code within the system.
Guidance: •   Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Mobile code technologies include for example Java applets, JavaScript, HTML5, WebGL, and VBScript.
•   Decisions regarding the use of mobile code in organizational systems should be based on the potential for the code to cause damage to the systems if used maliciously. Usage restrictions and implementation guidance should apply to the selection and use of mobile code installed.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Subcategory: DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events
Requirement: IMPORTANT_DE.CM-6.1: All external connections by vendors supporting IT/OT applications or infrastructure shall be secured and actively monitored to ensure that only permissible actions occur during the connection.
Guidance: This monitoring includes unauthorized personnel access, connections, devices, and software.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1

Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Requirement: IMPORTANT_DE.CM-6.2: External service providers' conformance with personnel security policies and procedures and contract security requirements shall be monitored relative to their cybersecurity risks.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Subcategory: DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
Requirement: IMPORTANT_DE.CM-7.1: The organization's business critical systems shall be monitored for unauthorized personnel access, connections, devices, access points, and software.
Guidance: •   Unauthorized personnel access includes access by external service providers.
•   System inventory discrepancies should be included in the monitoring.
•   Unauthorized configuration changes to organization's critical systems should be included in the monitoring.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Requirement: DE.CM-7.2: Unauthorized configuration changes to organization's systems shall be monitored and addressed with the appropriate mitigation actions.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information
system and assets are monitored to identify cybersecurity events and
verify the effectiveness of protective measures.
Subcategory: DE.CM-8: Vulnerability scans are performed
Requirement: IMPORTANT_DE.CM-8.1: The organization shall monitor and
scan for vulnerabilities in its critical systems and hosted
applications ensuring that system functions are not adversely impacted
by the scanning process.
Guidance: Consider the implementation of a continuous vulnerability
scanning program; Including reporting and mitigation plans.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Security Continuous Monitoring (DE.CM): The information
system and assets are monitored to identify cybersecurity events and
verify the effectiveness of protective measures.
Requirement: IMPORTANT_DE.CM-8.2: The vulnerability scanning process
shall include analysis, remediation, and information sharing.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: DETECT (DE)
Category: Detection Processes (DE.DP): Detection processes and
procedures are maintained and tested to ensure awareness of anomalous
events.
Subcategory: DE.DP-2: Detection activities comply with all applicable
requirements
Requirement: IMPORTANT_DE.DP-2.1: The organization shall conduct
detection activities in accordance with applicable federal and
regional laws, industry regulations and standards, policies, and other
applicable requirements.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: DETECT (DE)

Category: Detection Processes (DE.DP): Detection processes and
procedures are maintained and tested to ensure awareness of anomalous
events.
Subcategory: DE.DP-3: Detection processes are tested
Requirement: IMPORTANT_DE.DP-3.1: The organization shall validate that
event detection processes are operating as intended.
Guidance: •   Validation includes testing.
•   Validation should be demonstrable.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Detection Processes (DE.DP): Detection processes and
procedures are maintained and tested to ensure awareness of anomalous
events.
Subcategory: DE.DP-4: Event detection information is communicated
Requirement: IMPORTANT_DE.DP-4.1: The organization shall communicate
event detection information to predefined parties.
Guidance: Event detection information includes for example, alerts on
atypical account usage, unauthorized remote access, wireless
connectivity, mobile device connection, altered configuration
settings, contrasting system component inventory, use of maintenance
tools and nonlocal maintenance, physical access, temperature and
humidity, equipment delivery and removal, communications at the
information system boundaries, use of mobile code, use of Voice over
Internet Protocol (VoIP), and malware disclosure.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Detection Processes (DE.DP): Detection processes and
procedures are maintained and tested to ensure awareness of anomalous
events.
Subcategory: DE.DP-5: Detection processes are continuously improved
Requirement: IMPORTANT_DE.DP-5.1: Improvements derived from the
monitoring, measurement, assessment, testing, review, and lessons
learned, shall be incorporated into detection process revisions.
Guidance: •   This results in a continuous improvement of the
detection processes.
•   The use of independent teams to assess the detection process
could be considered.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1

Subcategory Implementation Maturity Score: 1

Function: DETECT (DE)
Category: Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
Requirement: DE.DP-5.2: The organization shall conduct specialized assessments including in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, performance/load testing, and verification and validation testing on the organization's critical systems.
Guidance: These activities can be outsourced, preferably to accredited organizations.
Documentation Score: 1
Implementation Score: 1

Function: RESPOND (RS)
Category: Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.
Subcategory: RS.RP-1: Response plan is executed during or after an incident
Requirement: BASIC_RS.RP-1.1: An incident response process, including roles, responsibilities, and authorities, shall be executed during or after an information/cybersecurity event on the organization's critical systems.
Guidance: •   The incident response process should include a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack.
•   The roles, responsibilities, and authorities in the incident response plan should be specific on involved people, contact info, different roles and responsibilities, and who makes the decision to initiate recovery procedures as well as who will be the contact with appropriate external stakeholders.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

Guidance: It should be considered to determine the causes of an information/cybersecurity event and implement a corrective action in order that the event does not recur or occur elsewhere (an infection by malicious code on one machine did not have spread elsewhere in the network). The effectiveness of any corrective action taken should be reviewed. Corrective actions should be appropriate to the effects of the information/cybersecurity event encountered.
Internal Note: Requirements are covered in PR.IP-9

Function: RESPOND (RS)
Category: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
Subcategory: RS.CO-1: Personnel know their roles and order of operations when a response is needed
Requirement: IMPORTANT_RS.CO-1.1: The organization shall ensure that personnel understand their roles, objectives, restoration priorities, task sequences (order of operations) and assignment responsibilities for event response.
Guidance: Consider the use the CCB Incident Management Guide to guide you through this exercise and consider bringing in outside experts if needed. Test your plan regularly and adjust it after each incident.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
Subcategory: RS.CO-2: Incidents are reported consistent with established criteria
Requirement: IMPORTANT_RS.CO-2.1: The organization shall implement reporting on information/cybersecurity incidents on its critical systems in an organization-defined time frame to organization-defined personnel or roles.
Guidance: All users should have a single point of contact to report any incident and be encouraged to do so.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
Requirement: RS.CO-2.2: Events shall be reported consistent with established criteria.
Guidance: Criteria to report should be included in the incident response plan.
Documentation Score: 1
Implementation Score: 1

Function: RESPOND (RS)
Category: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
Subcategory: RS.CO-3: Information is shared consistent with response plans
Requirement: BASIC_RS.CO-3.1: Information/cybersecurity incident information shall be communicated and shared with the organization's employees in a format that they can understand.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
Requirement: IMPORTANT_RS.CO-3.2: The organization shall share information/cybersecurity incident information with relevant stakeholders as foreseen in the incident response plan.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: RESPOND (RS)
Category: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
Subcategory: RS.CO-4: Coordination with stakeholders occurs consistent with response plans
Requirement: IMPORTANT_RS.CO-4.1: The organization shall coordinate information/cybersecurity incident response actions with all predefined stakeholders.

Guidance: •   Stakeholders for incident response include for example, mission/business owners, organization's critical system owners, integrators, vendors, human resources offices, physical and personnel security offices, legal departments, operations personnel, and procurement offices.
•   Coordination with stakeholders occurs consistent with incident response plans.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
Subcategory: RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
Requirement: IMPORTANT_RS.CO-5.1: The organization shall share information/cybersecurity event information voluntarily, as appropriate, with external stakeholders, industry security groups,… to achieve broader information/cybersecurity situational awareness.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
Subcategory: RS.AN-1: Notifications from detection systems are investigated
Requirement: IMPORTANT_RS.AN-1.1: The organization shall investigate information/cybersecurity-related notifications generated from detection systems.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: RESPOND (RS)

Category: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
Requirement: RS.AN-1.2: The organization shall implement automated mechanisms to assist in the investigation and analysis of information/cybersecurity-related notifications.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: RESPOND (RS)
Category: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
Subcategory: RS.AN-2: The impact of the incident is understood
Requirement: IMPORTANT_RS.AN-2.1: Thorough investigation and result analysis shall be the base for understanding the full implication of the information/cybersecurity incident.
Guidance: •   Result analysis can involve the outcome of determining the correlation between the information of the detected event and the outcome of risk assessments. In this way, insight is gained into the impact of the event across the organization.
•   Consider including detection of unauthorized changes to its critical systems in its incident response capabilities.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
Requirement: RS.AN-2.2: The organization shall implement automated mechanisms to support incident impact analysis.
Guidance: Implementation could vary from a ticketing system to a Security Information and Event Management (SIEM).
Documentation Score: 1
Implementation Score: 1

Function: RESPOND (RS)
Category: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
Subcategory: RS.AN-3: Forensics are performed
Requirement: RS.AN-3.1: The organization shall provide on-demand audit review, analysis, and reporting for after-the-fact investigations of information/cybersecurity incidents.
Guidance: No additional guidance on this topic.
Documentation Score: 1

Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
Requirement: RS.AN-3.2: The organization shall conduct forensic analysis on collected information/cybersecurity event information to determine root cause.
Guidance: Consider to determine the root cause of an incident. If necessary, use forensics analysis on collected information/cybersecurity event information to achieve this.
Documentation Score: 1
Implementation Score: 1

Function: RESPOND (RS)
Category: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
Subcategory: RS.AN-4: Incidents are categorized consistent with response plans
Requirement: IMPORTANT_RS.AN-4.1: Information/cybersecurity incidents shall be categorized according to the level of severity and impact consistent with the evaluation criteria included the incident response plan.
Guidance: •   It should be considered to determine the causes of an information/cybersecurity incident and implement a corrective action in order that the incident does not recur or occur elsewhere.
•   The effectiveness of any corrective action taken should be reviewed.
•   Corrective actions should be appropriate to the effects of the information/cybersecurity incident encountered.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
Key Measure: Key Measure
Subcategory: RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)

Requirement: IMPORTANT_RS.AN-5.1: The organization shall implement vulnerability management processes and procedures that include processing, analyzing and remedying vulnerabilities from internal and external sources.
Guidance: Internal and external sources could be e.g. internal testing, security bulletins, or security researchers.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
Requirement: RS.AN-5.2: The organization shall implement automated mechanisms to disseminate and track remediation efforts for vulnerability information, captured from internal and external sources, to key stakeholders.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: RESPOND (RS)
Category: Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
Subcategory: RS.MI-1: Incidents are contained
Requirement: IMPORTANT_RS.MI-1.1: The organization shall implement an incident handling capability for information/cybersecurity incidents on its business critical systems that includes preparation, detection and analysis, containment, eradication, recovery and documented risk acceptance.
Guidance: A documented risk acceptance deals with risks that the organisation assesses as not dangerous to the organisation's business critical systems and where the risk owner formally accepts the risk (related with the risk appetite of the organization)
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Subcategory: RS.IM-1: Response plans incorporate lessons learned
Requirement: BASIC_RS.IM-1.1: The organization shall conduct post-incident evaluations to analyse lessons learned from incident response and recovery, and consequently improve processes / procedures / technologies to enhance its cyber resilience.
Guidance: Consider bringing involved people together after each incident and reflect together on ways to improve what happened, how it happened, how we reacted, how it could have gone better, what should be done to prevent it from happening again, etc.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: RESPOND (RS)
Category: Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
Requirement: IMPORTANT_RS.IM-1.2: Lessons learned from incident handling shall be translated into updated or new incident handling procedures that shall be tested, approved and trained.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: RESPOND (RS)
Category: Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
Subcategory: RS.IM-2: Response and Recovery strategies are updated
Requirement: IMPORTANT_RS.IM-2.1: The organization shall update the response and recovery plans to address changes in its context.
Guidance: The organization's context relates to the organizational structure, its critical systems, attack vectors, new threats, improved technology, environment of operation, problems encountered during plan implementation/execution/testing and lessons learned.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

Function: RECOVER (RC)

Category: Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
Subcategory: RC.RP-1: Recovery plan is executed during or after a cybersecurity incident
Requirement: BASIC_RC.RP-1.1: A recovery process for disasters and information/cybersecurity incidents shall be developed and executed as appropriate.
Guidance: A process should be developed for what immediate actions will be taken in case of a fire, medical emergency, burglary, natural disaster, or an information/cyber security incident.
This process should consider:
•   Roles and Responsibilities, including of who makes the decision to initiate recovery procedures and who will be the contact with appropriate external stakeholders.
•   What to do with company's information and information systems in case of an incident. This includes shutting down or locking computers, moving to a backup site, physically removing important documents, etc.
•   Who to call in case of an incident.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: RECOVER (RC)
Category: Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
Requirement: RC.RP-1.2: The essential organization's functions and services shall be continued with little or no loss of operational continuity and continuity shall be sustained until full system restoration.
Guidance: No additional guidance on this topic.
Documentation Score: 1
Implementation Score: 1

Function: RECOVER (RC)
Category: Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
Subcategory: RC.IM-1: Recovery plans incorporate lessons learned
Requirement: IMPORTANT_RC.IM-1.1: The organization shall incorporate lessons learned from incident recovery activities into updated or new system recovery procedures and, after testing, frame this with appropriate training.
Guidance: No additional guidance on this topic.
Documentation Score: 1

Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: RECOVER (RC)
Category: Communications (RC.CO): Restoration activities are
coordinated with internal and external parties (e.g. coordinating
centers, Internet Service Providers, owners of attacking systems,
victims, other CSIRTs, and vendors).
Subcategory: RC.CO-1: Public relations are managed
Requirement: IMPORTANT_RC.CO-1.1: The organization shall centralize
and coordinate how information is disseminated and manage how the
organization is presented to the public.
Guidance: Public relations management may include, for example,
managing media interactions, coordinating and logging all requests for
interviews, handling and 'triaging' phone calls and e-mail requests,
matching media requests with appropriate and available internal
experts who are ready to be interviewed, screening all of information
provided to the media, ensuring personnel are familiar with public
relations and privacy policies.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1
Category Documentation Maturity Score: 1
Category Implementation Maturity Score: 1

Function: RECOVER (RC)
Category: Communications (RC.CO): Restoration activities are
coordinated with internal and external parties (e.g. coordinating
centers, Internet Service Providers, owners of attacking systems,
victims, other CSIRTs, and vendors).
Requirement: RC.CO-1.2: A Public Relations Officer shall be assigned.
Guidance: The Public Relations Officer should consider the use of pre-
define external contacts
(e.g. press, regulators, interest groups).
Documentation Score: 1
Implementation Score: 1

Function: RECOVER (RC)
Category: Communications (RC.CO): Restoration activities are
coordinated with internal and external parties (e.g. coordinating
centers, Internet Service Providers, owners of attacking systems,
victims, other CSIRTs, and vendors).

```
Subcategory: RC.CO-2: Reputation is repaired after an incident
Requirement: RC.CO-2.1: The organization shall implement a crisis
response strategy to protect the organization from the negative
consequences of a crisis and help restore its reputation.
Guidance: Crisis response strategies include, for example, actions to
shape attributions of the crisis, change perceptions of the
organization in crisis, and reduce the negative effect generated by
the crisis.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

---

Function: RECOVER (RC)
Category: Communications (RC.CO): Restoration activities are
coordinated with internal and external parties (e.g.  coordinating
centers, Internet Service Providers, owners of attacking systems,
victims, other CSIRTs, and vendors).
Subcategory: RC.CO-3: Recovery activities are communicated to internal
and external stakeholders as well as executive and management teams
Requirement: IMPORTANT_RC.CO-3.1: The organization shall communicate
recovery activities to predefined stakeholders, executive and
management teams.
Guidance: Communication of recovery activities to all relevant
stakeholders applies only to entities subject to the NIS legislation.
Documentation Score: 1
Implementation Score: 1
Subcategory Documentation Maturity Score: 1
Subcategory Implementation Maturity Score: 1

---
```

CyberFundamentals Framework — ESSENTIAL Summary

CyberFundamentals Categories and Maturity Scores
IDENTIFY

- **Asset Management (ID.AM)**
  Target Maturity Score: 3.50
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Business Environment (ID.BE)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.12

Documentation Maturity Score: 1.07
Implementation Maturity Score: 1.17

- **Governance (ID.GV)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Risk Assessment (ID.RA)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Risk Management Strategy (ID.RM)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Supply Chain Risk Management (ID.SC)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

PROTECT

- **Identity Management, Authentication and Access Control (PR.AC)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Awareness and Training (PR.AT)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Data Security (PR.DS)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **Information Protection Processes and Procedures (PR.IP)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Maintenance (PR.MA)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Protective Technology (PR.PT)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

DETECT

- **Anomalies and Events (DE.AE)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Security Continuous Monitoring (DE.CM)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Detection Processes (DE.DP)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

RESPOND

- **Response Planning (RS.RP)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **Communications (RS.CO)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Analysis (RS.AN)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Mitigation (RS.MI)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Improvements (RS.IM)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

RECOVER

- **Recovery Planning (RC.RP)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Improvements (RC.IM)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **Communications (RC.CO)**
  Target Maturity Score: 3.00
  Category Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

Key Measures (KM)

Access and Identity Controls

- **PR.AC-1.1** — Identities and credentials for authorized devices and users shall be managed.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-3.2** — The organization's networks when accessed remotely shall be secured, including through multi-factor authentication (MFA).
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-4.1** — Access permissions for users to the organization's systems shall be defined and managed.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-4.2** — It shall be identified who should have access to the organization's business-critical information and technology and the means to get access.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-4.3** — Employee access to data and information shall be limited to the systems and specific information they need to do their jobs (principle of Least Privilege).
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-4.4** — Nobody shall have administrator privileges for daily tasks.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-5.1** — Firewalls shall be installed and activated on all the organization's networks.
  Target Maturity Score: 3.00

KM Maturity Score: 1.00
Documentation Maturity Score: 1.00
Implementation Maturity Score: 1.00

- **PR.AC-5.2** — Where appropriate, network integrity of the organization's critical systems shall be protected by incorporating network segmentation and segregation.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **PR.IP-4.1** — Backups for organization's business critical data shall be conducted and stored on a system different from the device on which the original data resides.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **PR.MA-1.1** — Patches and security updates for operating systems and critical system components shall be installed.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **PR.PT-1.1** — Logs shall be maintained, documented, and reviewed.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **DE.AE-3.1** — The activity logging functionality of protection and detection hardware or software (e.g., firewalls, anti-virus) shall be enabled, backed up, and reviewed.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **DE.CM-4.1** — Anti-virus, spyware, and other malware programs shall be installed and updated.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

Governance, Processes, and Supply Chain Controls

- **ID.AM-6.1** — Information security and cybersecurity roles, responsibilities, and authorities within the organization shall be documented, reviewed, authorized, and updated in alignment with organizational internal roles and external partners.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **PR.AC-3.3** — Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization's critical systems shall be identified, documented, and implemented.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **PR.AC-5.3** — Where appropriate, network integrity of the organization's critical systems shall be protected by:
  (a) Identifying, documenting, and controlling connections between system components.
  (b) Limiting external connections to the organization's critical systems.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **PR.AC-5.4** — The organization shall monitor and control connections and communications at the external boundary and at key internal boundaries within the organization's critical systems by implementing boundary protection devices where appropriate.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **PR.DS-5.1** — The organization shall take appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorized access and activities, including data leakage, is detected.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **PR.IP-1.1** — The organization shall develop, document, and maintain a baseline configuration for its business-critical systems.

Target Maturity Score: 3.00
KM Maturity Score: 1.00
Documentation Maturity Score: 1.00
Implementation Maturity Score: 1.00

- **DE.CM-1.2** — The organization shall monitor and identify unauthorized use of its business-critical systems through the detection of unauthorized local connections, network connections, and remote connections.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **RS.AN-5.1** — The organization shall implement vulnerability management processes and procedures that include processing, analyzing, and remedying vulnerabilities from internal and external sources.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

Supply Chain and Maintenance Measures

- **ID.SC-3.2** — Contractual information security and cybersecurity requirements for suppliers and third-party partners shall be implemented to ensure a verifiable flaw remediation process, and to ensure correction of flaws identified during information security and cybersecurity review and evaluation.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **ID.SC-3.3** — The organization shall establish contractual requirements permitting the organization to supervise the information security and cybersecurity programs implemented by suppliers and third-party partners.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00
- **PR.AC-7.1** — The organization shall perform a documented risk assessment on its critical systems and authenticate users, devices, and other assets (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individual's security and privacy risk and other organizational risks).
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00

Documentation Maturity Score: 1.00
Implementation Maturity Score: 1.00

- **PR.MA-1.3** — The organization shall prevent the unauthorized removal of maintenance equipment containing organization's critical system information.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **PR.MA-1.5** — Maintenance tools and portable storage devices shall be inspected when brought into the facility and shall be protected by anti-malware solutions so that they are scanned for malicious code before they are used on organization's systems.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **PR.MA-1.6** — The organization shall verify security controls following hardware and software maintenance or repairs/patching and take actions as appropriate.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **PR.PT-2.3** — Portable storage devices containing system data shall be controlled and protected while in transit and in storage.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

- **DE.AE-1.3** — The organization shall ensure that a baseline of network operations and expected data flows for its critical systems is developed, documented, and maintained to track events.
  Target Maturity Score: 3.00
  KM Maturity Score: 1.00
  Documentation Maturity Score: 1.00
  Implementation Maturity Score: 1.00

Total Maturity Level

Overall Score: 1.01
TLP Classification: AMBER

CyberFundamentals Maturity Level ESSENTIAL

Legend:

- Green: Target Maturity Score
- Orange: Category Maturity Score
- Grey: Documentation Maturity Score
- Blue: Implementation Maturity Score

Maturity Level Scale:

5 – Optimizing

4 – Managed

3 – Defined

2 – Repeatable

1 – Initial

0 – Non-existent

Graphical Radar Representation (summary of metrics shown in source):
Each category (ID, PR, DE, RS, RC) plotted with visible concentric levels (0–5), showing close proximity of actual Documentation and Implementation scores (~1.0–1.2) vs. Target (3.0–3.5).

CyberFundamentals Maturity Level — ESSENTIAL (Radar Chart Interpretation)

Chart Title

CyberFundamentals Maturity Level ESSENTIAL

Legend

- **Green line:** Target Maturity Score
- **Orange line:** Category Maturity Score
- **Gray line:** Documentation Maturity Score
- **Blue line:** Implementation Maturity Score

Axes and Labeled Domains

Each axis on the radar chart represents one **CyberFundamentals Category** within the NIS2-aligned framework.
The categories and their corresponding functional domains are:

IDENTIFY

- Asset Management (ID.AM)
- Business Environment (ID.BE)
- Governance (ID.GV)

- Risk Assessment (ID.RA)
- Risk Management Strategy (ID.RM)
- Supply Chain Risk Management (ID.SC)

PROTECT
- Identity Management, Authentication and Access Control (PR.AC)
- Awareness and Training (PR.AT)
- Data Security (PR.DS)
- Information Protection Processes and Procedures (PR.IP)
- Maintenance (PR.MA)
- Protective Technology (PR.PT)

DETECT
- Anomalies and Events (DE.AE)
- Security Continuous Monitoring (DE.CM)
- Detection Processes (DE.DP)

RESPOND
- Response Planning (RS.RP)
- Communications (RS.CO)
- Analysis (RS.AN)
- Mitigation (RS.MI)
- Improvements (RS.IM)

RECOVER
- Recovery Planning (RC.RP)
- Improvements (RC.IM)
- Communications (RC.CO)

Maturity Level Scale

The radar chart uses a numeric maturity scale from **0 to 5**, with labeled reference points:

- 5 – Optimizing
- 4 – Managed
- 3 – Defined
- 2 – Repeatable
- 1 – Initial
- 0 – Non-existent

Each ring represents an incremental maturity level step.

Plotted Data Summary (from the chart and ESSENTIAL Summary sheet)

Category	Target Maturity	Category Maturity	Documentation Maturity	Implementation Maturity
Asset Management (ID.AM)	3.50	1.00	1.00	1.00
Business Environment (ID.BE)	3.00	1.12	1.07	1.17
Governance (ID.GV)	3.00	1.00	1.00	1.00
Risk Assessment (ID.RA)	3.00	1.00	1.00	1.00
Risk Management Strategy (ID.RM)	3.00	1.00	1.00	1.00
Supply Chain Risk Management (ID.SC)	3.00	1.00	1.00	1.00
Identity Management, Authentication & Access Control (PR.AC)	3.00	1.00	1.00	1.00
Awareness and Training (PR.AT)	3.00	1.00	1.00	1.00
Data Security (PR.DS)	3.00	1.00	1.00	1.00
Information Protection Processes and Procedures (PR.IP)	3.00	1.00	1.00	1.00
Maintenance (PR.MA)	3.00	1.00	1.00	1.00
Protective Technology (PR.PT)	3.00	1.00	1.00	1.00
Anomalies and Events (DE.AE)	3.00	1.00	1.00	1.00
Security Continuous Monitoring (DE.CM)	3.00	1.00	1.00	1.00
Detection Processes (DE.DP)	3.00	1.00	1.00	1.00
Response Planning (RS.RP)	3.00	1.00	1.00	1.00
Communications (RS.CO)	3.00	1.00	1.00	1.00
Analysis (RS.AN)	3.00	1.00	1.00	1.00
Mitigation (RS.MI)	3.00	1.00	1.00	1.00
Improvements (RS.IM)	3.00	1.00	1.00	1.00
Recovery Planning (RC.RP)	3.00	1.00	1.00	1.00
Improvements (RC.IM)	3.00	1.00	1.00	1.00
Communications (RC.CO)	3.00	1.00	1.00	1.00

Observed Distribution Pattern (Chart Interpretation)

- The **Target Maturity Scores** (green) consistently range between **3.0 and 3.5**, reflecting the expected "Defined" to "Managed" level under the ESSENTIAL tier of the CyberFundamentals Framework.

- The **Category Maturity Scores** (orange) remain at approximately **1.0–1.1** across all domains, corresponding to an "Initial" stage of capability maturity.
- Both **Documentation** (gray) and **Implementation** (blue) maturity lines closely overlap at around **1.0**, forming a nearly circular plot in the innermost band of the radar chart.

This alignment indicates **minimal divergence** between policy documentation and its execution — both equally underdeveloped relative to targets.

Interpretive Analysis (based strictly on chart and data)

The radar visualization depicts an organization that has **defined target expectations** (3.0–3.5) across all NIS2-aligned functional areas but exhibits **uniformly low practical maturity (≈1.0)** in both documentation and implementation.
 This consistent gap suggests that the foundational elements (policy documentation, control execution, and process validation) are **largely at an initial stage of development** across all functional domains.

In visual terms:

- The **target layer (green)** forms an outer ring around level 3–3.5.
- The **actual maturity lines (gray and blue)** form an almost perfect inner circle around level 1.
- No domain extends beyond 1.2, confirming that no single function exceeds the "Initial" phase of maturity.

The **TLP classification** for this summary remains **AMBER**, reflecting that core elements exist but require significant development to align with the ESSENTIAL-level cybersecurity expectations of the CyberFundamentals Framework.