CyFun®

BASIC

# CyberFundamentals 2023

Version 2023-03-01

# TABLE OF CONTENTS

# INTRODUCTION

The **CyberFundamentals Framework** is a set of concrete measures to:

- protect data,
- significantly reduce the risk of the most common cyberattacks,
- increase an organisation's cyber resilience.

The requirements and guidance are complemented with the relevant insights included in the NIST/CSF framework, ISO 27001/ISO 27002, IEC 62443 and the CIS Critical security Controls (ETSI TR 103 305-1).

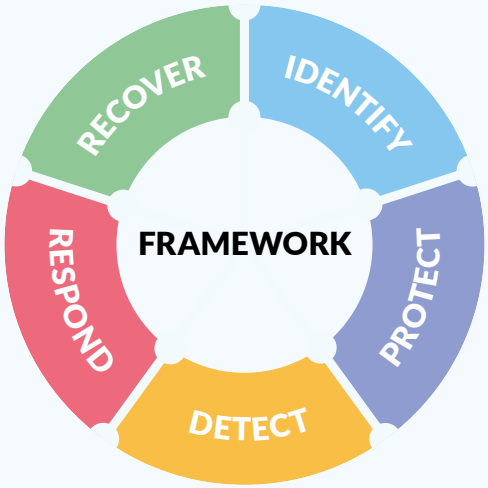
The coding of the requirements corresponds with the codes used in the NIST CSF Framework. Since not all NIST CSF requirements are applicable, some codes that do exist in the NIST CSF framework may be missing.

The framework and the proportional approach of the assurance levels are validated by practitioners in the field using anonymised real-world cyberattack information provided by the federal Cyber Emergency Response Team (CERT.be - the operational service of the Centre for Cybersecurity Belgium).

The **CyberFundamentals Framework** is built around five core functions: identify, protect, detect, respond and recover. Regardless of the organisation and industry, these functions make it possible to promote communication around cybersecurity among technical practitioners and stakeholders alike, so that cyber-related risks can be incorporated into the overall risk management strategy of the organisation.

### Identify

Being aware of important cyber threats to your most valuable assets. Essentially, you can't protect what you don't know exists. This function helps develop an organisational understanding of how to manage cybersecurity risks related to systems, people, assets, data, and capabilities.




### Protect

The Protect function focuses on developing and implementing the safeguards necessary to mitigate or contain a cyber risk.

### Detect

The purpose of the Detect function is to ensure the timely detection of cybersecurity events.

### Respond

The Respond function is all about the controls that help respond to cybersecurity incidents. The Respond function supports the ability to contain the impact of a potential cybersecurity incident.

### Recover

The Recover function focuses on those safeguards that help maintain resilience and restore services that have been affected by a cybersecurity incident.

---

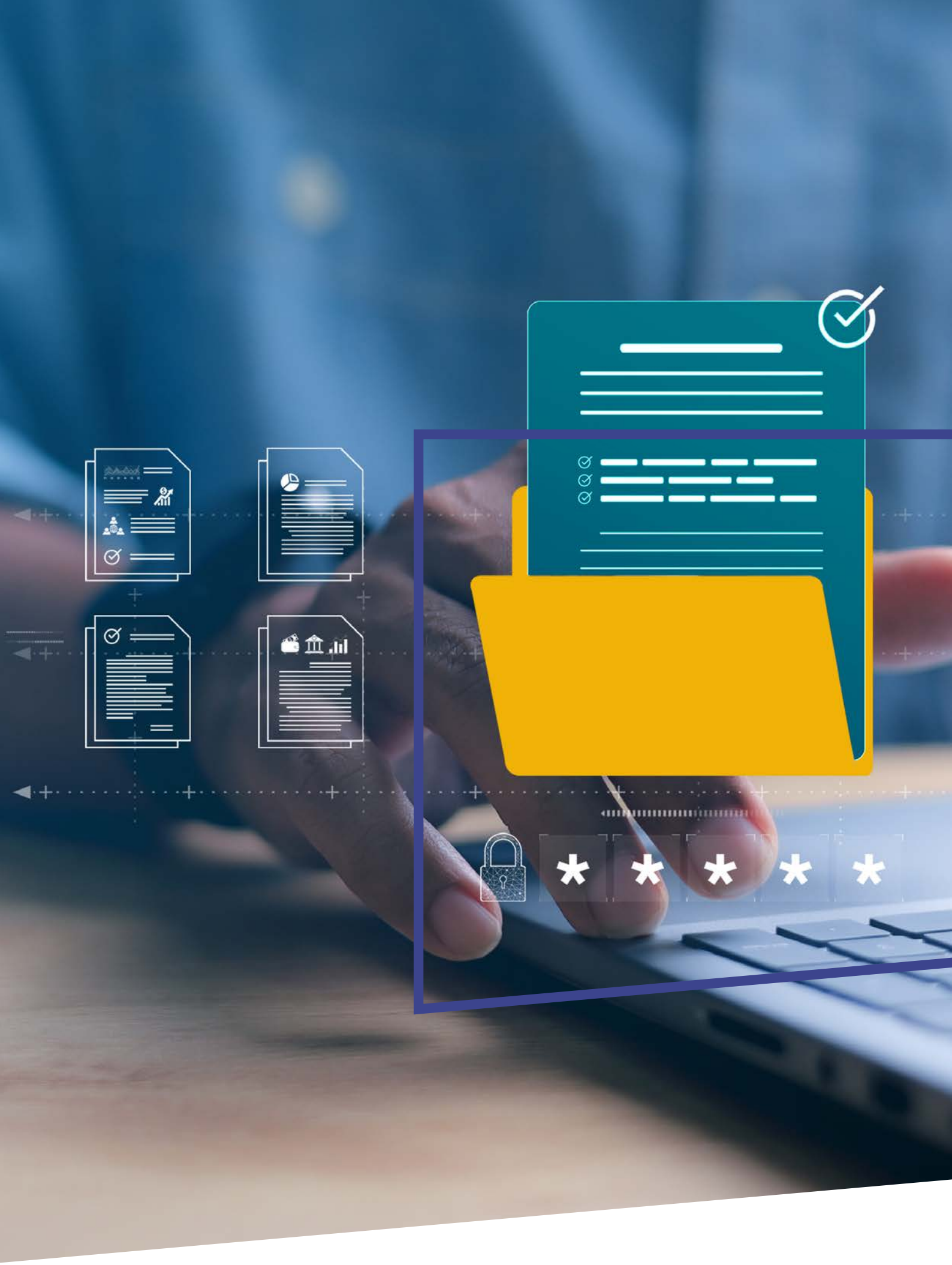
To respond to the severity of the threat an organisation is exposed to, and in addition to the starting level ***Small***, three assurance levels are also provided: ***Basic, Important and Essential***.

The **starting level *Small*** allows an organisation to make an initial assessment. It is intended for micro-organisations or organisations with limited technical knowledge.

The **assurance level *Basic*** contains the standard information security measures for all enterprises. These provide an effective security value that includes technology and processes that are generally already available. Where justified, the measures are tailored and refined.

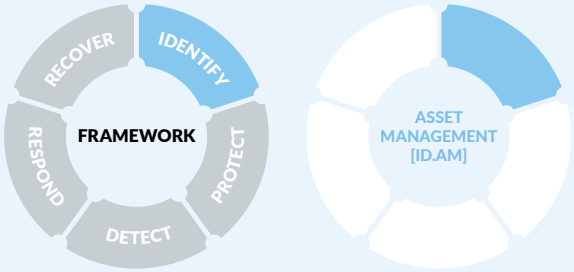
Several controls require particular attention; These measures are labelled as **key measure** .

The framework is a living document and will continue to be updated and improved in response to the feedback received from stakeholders, the evolving risk of specific cybersecurity threats, the availability of technical solutions and the insights achieved over time.



# IDENTIFY

# Identify




The data, personnel, devices, systems, and facilities that enable the organisation to achieve business purposes are identified and managed consistent with their relative importance to organisational objectives and the organisation's risk strategy.

## ID.AM-1 Physical devices and systems used within the organisation are inventoried.

An inventory of assets associated with information and information processing facilities within the organisation 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 organisation's network.
- The use of an IT asset management tool could be considered.

## ID.AM-2 Software platforms and applications used within the organisation are inventoried.

An inventory that reflects what software platforms and applications are being used in the organisation 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 unauthorised software.
- The use of an IT asset management tool could be considered.

## ID.AM-3 Organisational communication and data flows are mapped.

Information that the organisation 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 organisation (see ID.AM-1 & ID.AM-2).

## ID.AM-4 External information systems are catalogued.

No requirements are identified for the assurance level 'Basic', but guidelines are provided to increase information security.

### Guidance

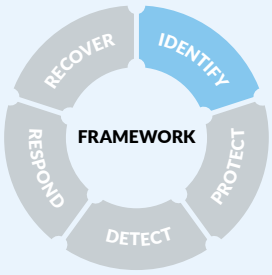
Outsourcing of systems, software platforms and applications used within the organisation is covered in ID.AM-1 & ID.AM-2.

## ID.AM-5 Resources are prioritised based on their classification, criticality, and business value.

The organisation's resources (hardware, devices, data, time, personnel, information, and software) shall be prioritised based on their classification, criticality, and business value.

### Guidance

- Determine the organisation's resources (e.g. hardware, devices, data, time, personnel, information, and software):
  - What would happen to my business if these resources were made public, damaged or lost...?
  - What would happen to my business when the integrity of resources is no longer guaranteed?
  - What would happen to my business if I/my customers couldn't access these resources? You should also rank these resources based on their classification, criticality, and business value.
- Resources should include enterprise assets.





The policies and procedures to manage and monitor the organisation's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

## ID.GV-1 Organisational cybersecurity policy is established and communicated.

**Policies and procedures for information security and cybersecurity 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 with regard to your information security expectations, and can aid an investigation in the event of an incident. These policies and procedures should be readily accessible to employees.
- Policies and procedures for information security and cybersecurity should clearly describe your expectations for protecting the organisation'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 organisation or technology. Whenever the policies are changed, employees should be made aware of the changes.

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

Legal and regulatory requirements regarding information/cybersecurity, including privacy obligations, shall be understood and implemented.

### Guidance

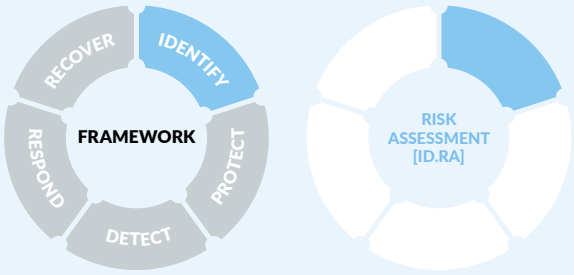
There are no additional guidelines.

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

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.




The organisation understands the cybersecurity risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals.

## ID.RA-1 Asset vulnerabilities are identified and documented.

Threats and vulnerabilities shall be identified.

### Guidance

- A vulnerability refers to a weakness in the organisation's hardware, software, or procedures. It is a gap through which a bad actor can gain access to the organisation's assets. A vulnerability exposes an organisation 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.

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

The organisation shall conduct risk assessments in which risk is determined by threats, vulnerabilities and impact on business processes and assets.

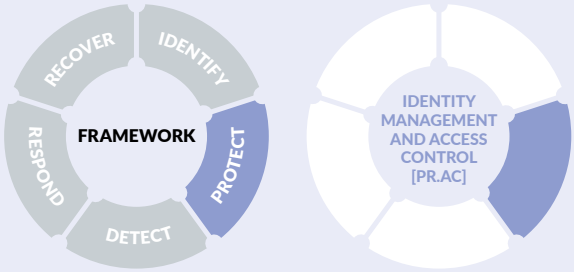
### Guidance

- 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.


Username
Password
Remember me
Protected
Balance:
5.367.50 $

# PROTECT

# Protect




Access to physical and logical assets and associated facilities is limited to authorised users, processes, and devices, and is managed consistent with the assessed risk of unauthorised access to authorised activities and transactions.

## PR.AC-1 Identities and credentials are issued, managed, verified, revoked, and audited for authorised devices, users, and processes.

Identities and credentials for authorised devices and users shall be managed.

### Guidance

Identities and credentials for authorised devices and users could be managed by means of a password policy. A password policy is a set of rules designed to enhance ICT/OT security by encouraging organisations to: (This list is not exhaustive and measures should be considered, as appropriate)

- Change all default passwords.
- Ensure that no-one works with administrator privileges when performing 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 whenever 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.

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

**Physical access to the facility, servers and network components shall be managed.**

### Guidance

- Consider strictly managing keys to access the premises and alarm codes. The following rules should be considered:
  - Always retrieve an employee's keys or badges when they leave the company permanently.
  - Change company alarm codes frequently.
  - Never give keys or alarm codes to external service providers (cleaning agents, etc.), unless it is possible to trace these accesses and technically restrict them to given time slots.
- Consider not leaving internal network access outlets accessible in public areas. These public places include waiting rooms, corridors, for example.

## PR.AC-3 Remote access is managed.

**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 Wi-Fi 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, connection should be made using an encrypted virtual private network (VPN) capability.
- Manage all endpoint devices (fixed and mobile) in accordance with the organisation's security policies.

**When accessed remotely, the organisation's networks shall be secured, including through the use of multi-factor authentication (MFA).**

### Guidance

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

## PR.AC-4 Access permissions and authorisations are managed, incorporating the principles of least privilege and separation of duties.

**Access permissions for users to the organisation'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), and to what, in order to perform their duties in the organisation.
- Set up a separate account for each user (including any contractors needing access) and require strong, unique passwords to be used for each account.
- Ensure that all employees use computer accounts without administrative privileges to perform typical work functions. This includes the separation of personal and admin accounts.
- For guest accounts, consider using 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.

**It shall be identified who should have access to the organisation's business-critical information and technology and is given the means to obtain access.**

### Guidance

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

**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 authorisations they need to perform their job role. Consider:

- Not allowing any employee to have access to all the business's information.
- Limiting the number of Internet accesses and interconnections with partner networks to those that are strictly necessary to be able to centralise and homogenise the monitoring of exchanges more easily.
- Ensuring that when an employee leaves the business, all access to the business's information or systems is blocked instantly.

**Nobody shall have administrator privileges for daily tasks.**

### Guidance

Consider the following:

- Separate administrator accounts from user accounts.
- Do not privilege user accounts to perform administration tasks.
- Create unique local administrator passwords and disable unused accounts.
- Consider prohibiting Internet browsing from administrative accounts.

## PR.AC-5 Network integrity (network segregation, network segmentation... ) is protected.

**Firewalls shall be installed and activated on all the organisation's networks.**

### Guidance

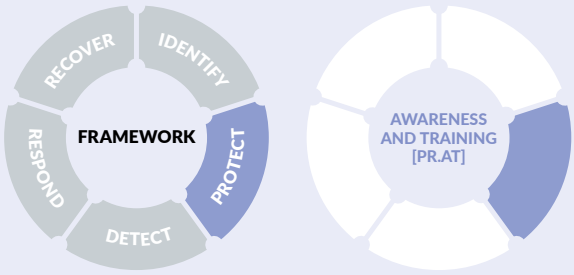
Consider the following:

- 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 that anti-virus software has been 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 teleworking purposes, home networks and systems have hardware and software firewalls installed that are operational, and regularly updated.
- Consider installing an Intrusion Detection / Prevention System (IDPS). These devices analyse network traffic at a more detailed level and can provide a greater level of protection.

**Where appropriate, the network integrity of the organisation'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.



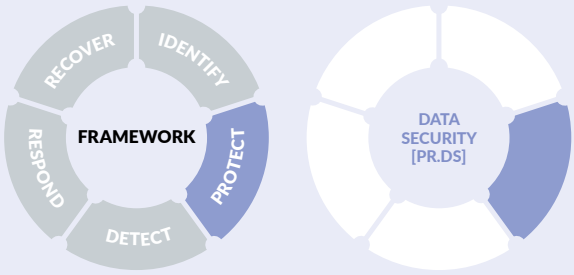

The organisation's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

## PR.AT-1 All users are informed and trained.

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 on the subject of 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.




Information and records (data) are managed consistent with the organisation's risk strategy to protect the confidentiality, integrity, and availability of information.

## PR.DS-1 Data-at-rest is protected.

**This control is covered by other elements of the framework; no additional requirements are identified.**

### 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 using solutions such as Windows BitLocker®, VeraCrypt, Apple FileVault®, Linux® dm-crypt,...
- Consider encrypting sensitive data stored in the cloud.

## PR.DS-2 Data-in-transit is protected.

**This control is covered by other elements of the framework; no additional requirements are identified.**

### Guidance

If the organisation frequently sends sensitive documents or e-mails, it is recommended to encrypt those documents and/or e-mails using software tools that are appropriate, supported, and authorised.

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

Assets and media shall be disposed of safely.

### Guidance

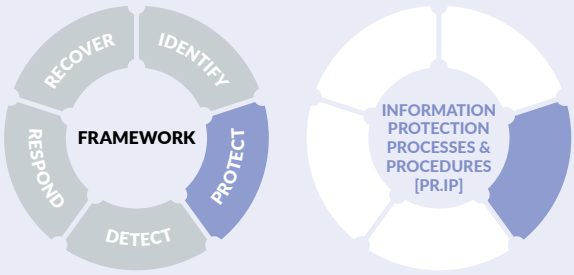
- When eliminating tangible assets like business computers/laptops, servers, hard drive(s) and other storage media (USB drives, paper...), ensure that all sensitive business or personal data are securely deleted (i.e. electronically "wiped") before they are removed and then physically destroyed (or re-commissioned). This is also known as "sanitisation" and therefore relates 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.

## PR.DS-7 The development and testing environment(s) are separate from the production environment.

No requirements are identified for the assurance level 'Basic', but guidelines are provided to increase information security.

### 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 life cycle principles).




Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organisational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

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

Backups for organisation's business-critical data shall be conducted and stored on a system different from the device on which the original data resides.

### Guidance

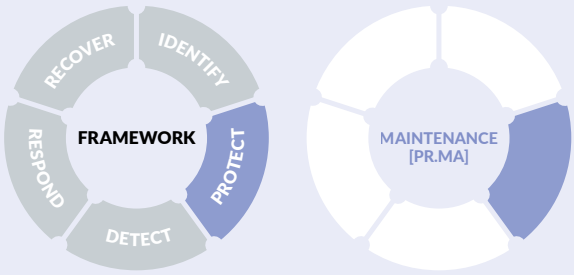
- The organisation's business critical system's data includes for example software, configurations and settings, documentation, system configuration data including computer configuration backups, application configuration backups, etc.
- Consider a regular backup and put it offline periodically.
- Recovery time and recovery point objectives should be considered.
- Consider not storing the organisation'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).

## PR.IP-11 Cybersecurity is included in human resources practices (deprovisioning, personnel screening...).

Personnel having access to the organisation'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 upon 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.




Maintenance and repair of industrial control and information system components are performed consistent with policies and procedures.

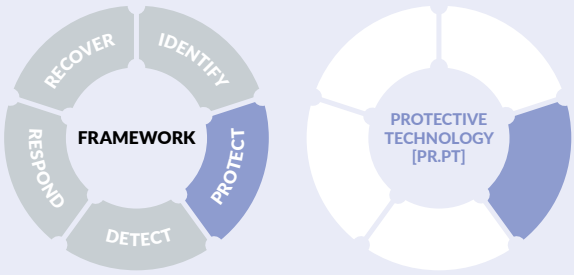
## PR.MA-1 Maintenance and repair of organisational assets are performed and logged, with approved and controlled tools.

**Patches and security updates for Operating Systems and critical system components shall be installed.**

### Guidance

The following should be considered:

- 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 that 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.




Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

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

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.

## PR.PT-4 Communications and control networks are protected.

Web and e-mail filters shall be installed and used.

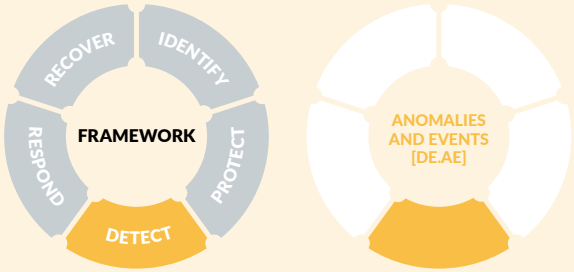
### Guidance

- 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.


WARNING!
SYSTEM WARNING

# DETECT

# Detect



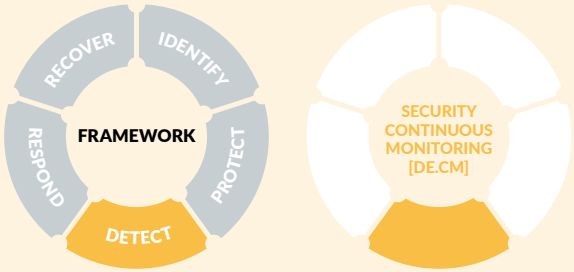

Anomalous activity is detected, and the potential impact of events is understood.

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

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 to identify 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.


The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

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

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 smartphones and other networked devices when installing and operating firewalls.
- Consider limiting the number of interconnection gateways to the Internet.

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

**Endpoint and network protection tools to monitor end-user behaviour for dangerous activity shall be implemented.**

### Guidance

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

## DE.CM-4 Malicious code is detected.

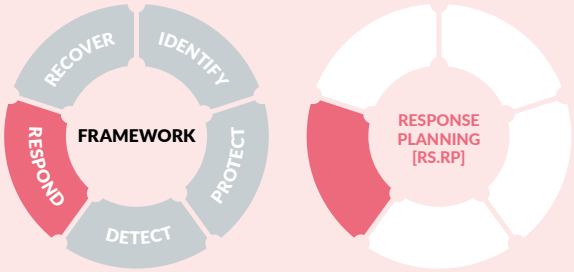
**Anti-virus, anti-spyware, and other -malware programs shall be installed and updated.**

### 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.
- Organisations should consider providing the same malicious code protection mechanisms for home computers (e.g. for teleworking purposes) or for personal devices that are used to perform work of a professional nature (BYOD).

# RESPOND

# Respond



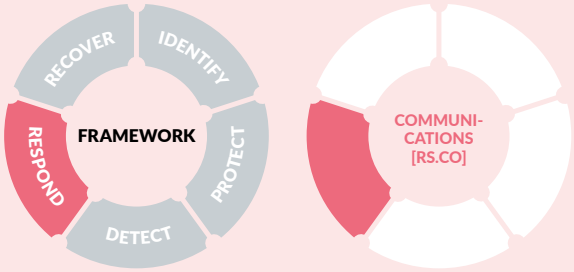

Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

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

An incident response process, including roles, responsibilities, and authorities, shall be executed during or after an information/cybersecurity event on the organisation'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 cyberattack.
- The roles, responsibilities, and authorities in the incident response plan should be specific with regard to the people involved, contact information, different roles and responsibilities, and with regard to who makes the decision to initiate recovery procedures as well as who will be the contact for appropriate external stakeholders.



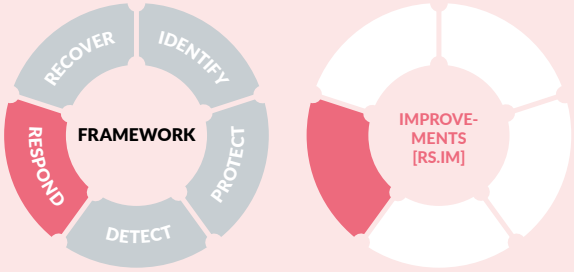

Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

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

Information/cybersecurity incident information shall be communicated and shared with the organisation's employees in a format that they can understand.

### Guidance

There are no additional guidelines.



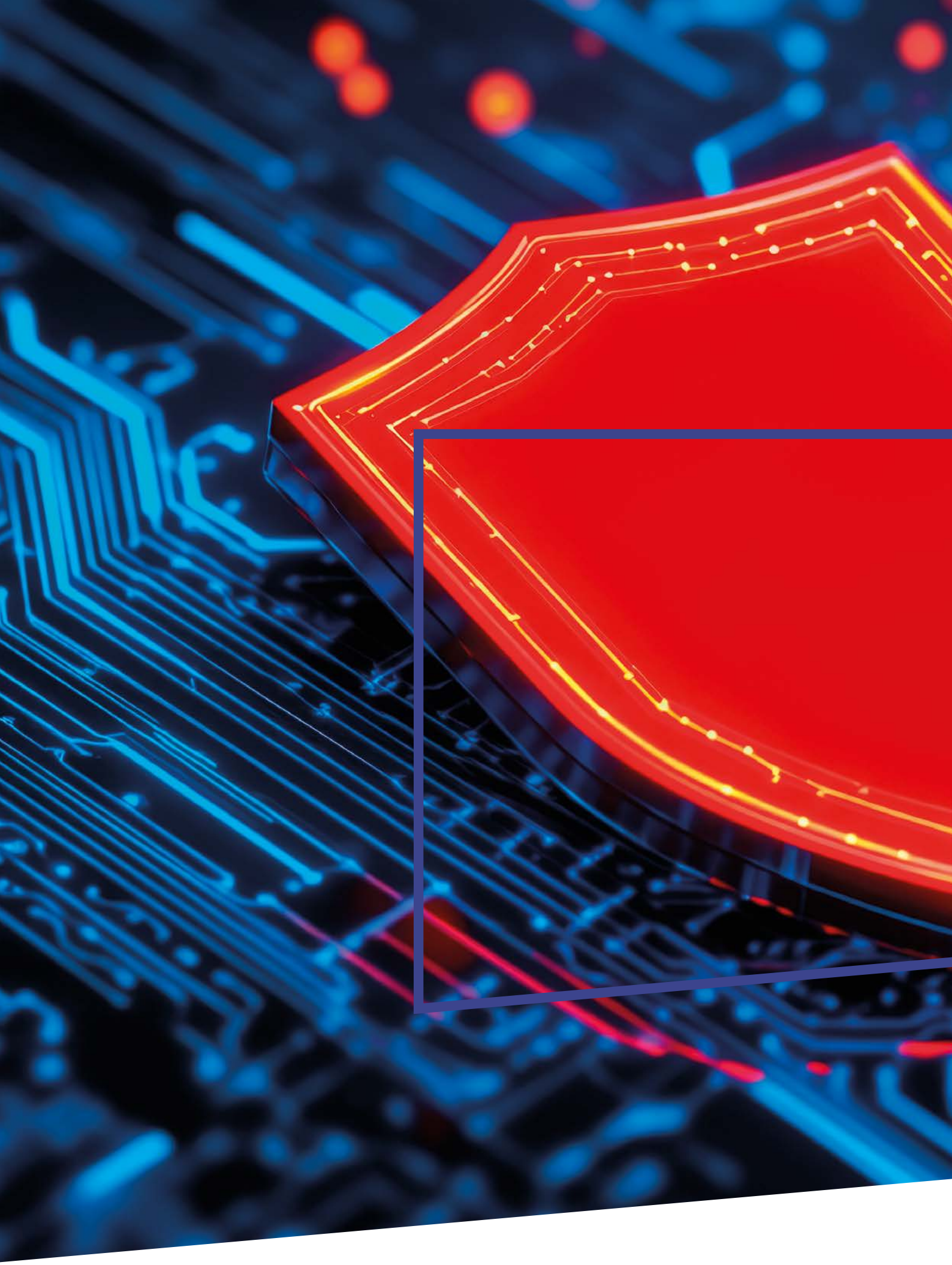

Organisational response activities are improved by incorporating lessons learned from current and previous detection/response activities

## RS.IM-1 Response plans incorporate lessons learned.

The organisation 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.

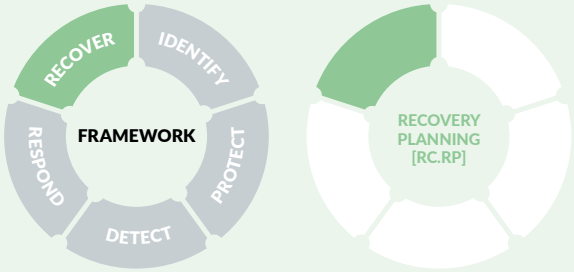
### Guidance

After each incident, consider bringing the persons involved together 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.



# RECOVER

# Recover




Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

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

**A recovery process for disasters and information/cybersecurity incidents shall be developed and executed as appropriate.**

### Guidance

A process should be developed to determine what immediate actions will be taken in the event of a fire, medical emergency, burglary, natural disaster, or an information/cybersecurity 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 the 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 the event of an incident.

# ANNEX

# ANNEX A : LIST OF KEY MEASURES FOR THE ASSURANCE LEVEL 'BASIC'

## PROTECT

**PR.AC-1 Identities and credentials are issued, managed, verified, revoked, and audited for authorised devices, users, and processes.**

(1) Identities and credentials for authorised devices and users shall be managed.

**PR.AC-3 Remote access is managed.**

(2) When accessed remotely, the organisation's networks shall be secured, including through the use of multi-factor authentication (MFA).

**PR.AC-4 Access permissions and authorisations are managed, incorporating the principles of least privilege and separation of duties.**

(3) Access permissions for users to the organisation's systems shall be defined and managed.

(4) It shall be identified who should have access to the organisation's business-critical information and technology and is given the means to obtain access.

(5) Employee access to data and information shall be limited to the systems and specific information they need to do their jobs.

(6) Nobody shall have administrator privileges for daily tasks.

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

(7) Firewalls shall be installed and activated on all the organisation's networks.

(8) Where appropriate, the network integrity of the organisation's critical systems shall be protected by incorporating network segmentation and segregation.

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

(9) Backups for organisation's business-critical data shall be conducted and stored on a system different from the device on which the original data resides.

**PR.MA-1** Maintenance and repair of organisational assets are performed and logged, with approved and controlled tools.

(10) Patches and security updates for Operating Systems and critical system components shall be installed.

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

(11) Logs shall be maintained, documented, and reviewed.

## DETECT

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

(12) The activity logging functionality of protection / detection hardware or software (e.g. firewalls, anti-virus) shall be enabled, backed up and reviewed.

**DE.CM-4** Malicious code is detected.

(13) Anti-virus, anti-spyware, and other anti-malware programs shall be installed and updated.

## Disclaimer

This document and its annexes have been prepared by the Centre for Cybersecurity Belgium (CCB), a federal administration created by the Royal Decree of 10 October 2014 and under the authority of the Prime Minister.

All texts, layouts, designs and other elements of any nature in this document are subject to **copyright law**. The reproduction of extracts from this document is authorised for non-commercial purposes only and provided that the source is acknowledged.

This document contains technical information written mainly in English. This information relating to the security of networks and information systems is addressed to IT services which use the English terms of computer language. A translation into Dutch, French or German of this technical information is also made available the CCB.

The CCB accepts **no responsibility for the content** of this document.
The information provided:

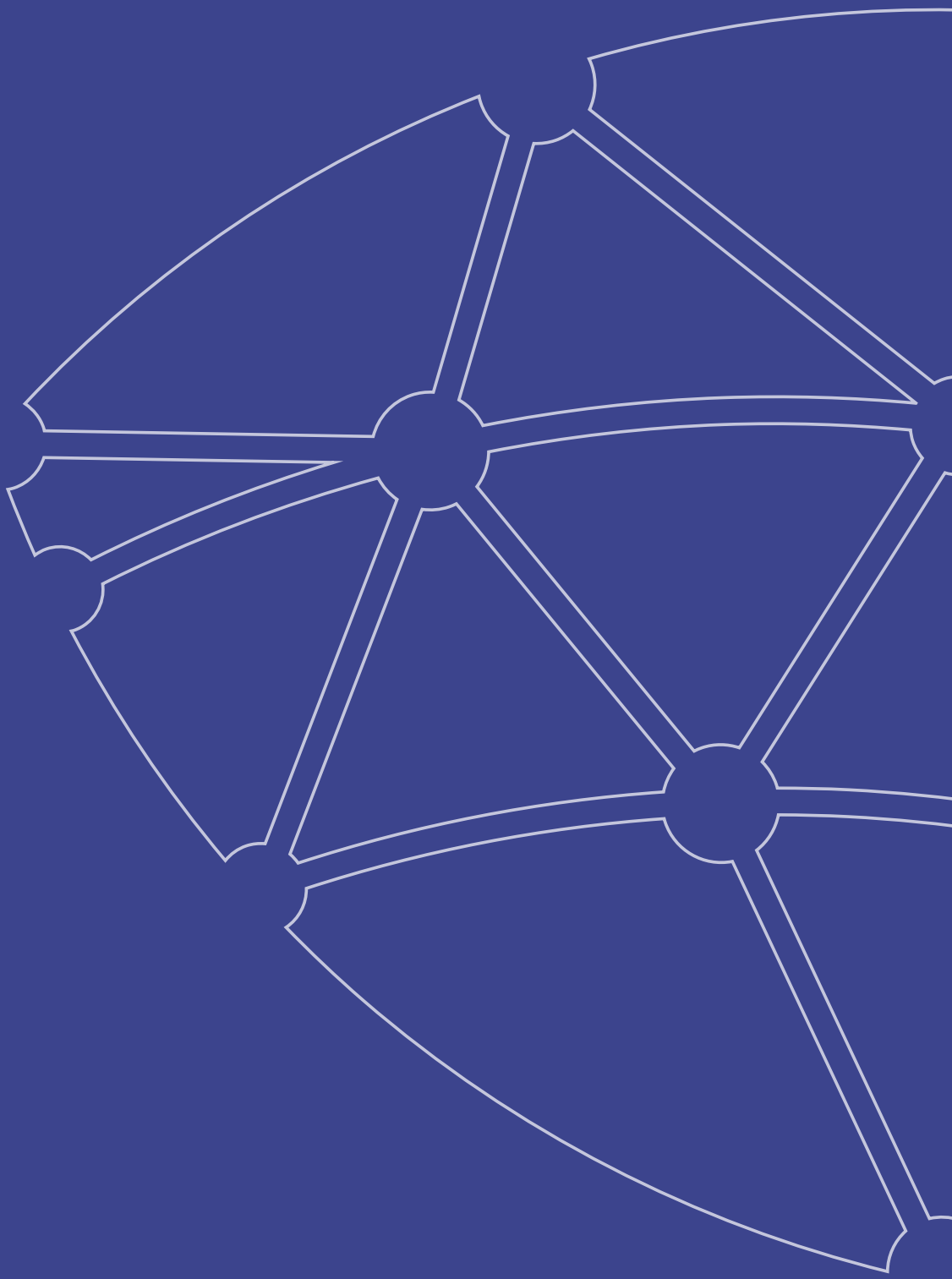
- is exclusively of a general nature and is not intended to take into consideration all particular situations.
- is not necessarily exhaustive, precise, or up to date on all points.

**Responsible editor**

Centre for Cybersecurity Belgium
Mr. De Bruycker, Director-General
Rue de la Loi, 18
1000 Brussels

**Legal depot**

D/2023/14828/001



Centre for Cybersecurity Belgium

Rue de la Loi, 18

1000 Brussels