CyFun®

BASIC

MATURITY LEVEL USE CASES 2023

Version 2025-10-01

TABLE OF CONTENTS

DESCRIPTION OF CYBERFUNDAMENTALS MATURITY LEVELS

This section describes the different CyberFundamentals Maturity levels in a holistic manner and is meant to be used as a guide during assessments. Although two approaches, documentation and implementation, need to be considered when carrying out assessments, the following provides an insight into how the maturity levels are understood as a whole.

The 5 CyberFundamentals Maturity Levels are:
- CyFun® Level 1 – Initial
- CyFun® Level 2 – Repeatable
- CyFun® Level 3 – Defined
- CyFun® Level 4 – Managed
- CyFun® Level 5 – Optimising

An important aspect of the CyberFundamentals Framework is that each maturity level builds on the previous maturity level. It is therefore assumed that cybersecurity practices that form part of a previous maturity level have already been established.

CYFUN® LEVEL 1 – INITIAL

Key elements: Process is unpredictable, reactive, not documented and poorly controlled

Safeguards or countermeasures have not been embedded in documented processes. This justifies the conclusion that cybersecurity controls (e.g. imposed via contract or sectoral requirements) have not been implemented.

There is a lack or a complete absence of governance and cybersecurity-related interventions are mainly limited to "break/fix" work.

There is no evidence of due diligence to demonstrate compliance with applicable legal, regulatory and/or contractual obligations.

CYFUN® LEVEL 2 – REPEATABLE

Key elements: Ad Hoc processes, mostly informal, project oriented and often reactive

Cybersecurity practices are "ad hoc" and when a control is implemented, it often lacks consistency and formality.

Cybersecurity practices tend to be project-oriented (driven by requirements set by a specific project). The intent of the respective controls is met in most cases, but the practice is not standardised across the organisation as a whole. At this level, cybersecurity practices are mainly focused on specific systems, networks, applications or processes for which controls need to be implemented in response to a compliance need and are often limited to a specific period in time. The latter could result in practices that have not been reviewed and updated in the past 2 years.

There is evidence of diligence to demonstrate compliance with specific legal, regulatory and/or contractual obligations, but in a way that is limited to the projects where this is required.

Implementation is dependent on the specific knowledge and effort of the person performing the task(s), and the implementation of these practices may be a single point of failure that is not proactively addressed.

It could be stated that due to their project orientation, CyFun® Level 2 cybersecurity practices focus on compliance rather than security and have therefore only rarely been rolled out organisation-wide.

CYFUN® LEVEL 3 – DEFINED

Key elements: Formal processes, organisation-oriented and proactive

Cybersecurity practices are standardised "organisation-wide" and implemented in accordance with formally defined and approved processes. Controls are implemented in accordance with documented and approved procedures.

Exceptions are documented, justified and approved. The number of exceptions from organisation-wide and standardised cybersecurity practices are limited to less than 5% of the total number of processes.

Assessment of the processes shows that less than 10% of the processes involve a deviation from the anticipated outcome of those processes.

CyFun® Level 3 cybersecurity practices focus on security over compliance. Compliance can reasonably be seen as a "natural by-product" of cybersecurity practices.

There is adequate evidence of due diligence to demonstrate compliance with specific legal, regulatory and/or contractual obligations.

CYFUN® LEVEL 4 – MANAGED

Key elements: Formal processes, organisation-oriented, controlled, proactive and measured

Cybersecurity practices build upon the CyFun® Level 3 maturity criteria and are "metrics-driven" in order to provide management with an insight into the cybersecurity status of the organisation.

Exceptions concerning cybersecurity practices that have been implemented organisation-wide are limited to less than 3% of all processes, and are documented, justified and approved.

Detailed performance metrics are collected, analysed and reported. This leads to a quantitative understanding of process capabilities and an ability to predict performance.

Assessment of the processes shows that less than 5% of the processes involve a deviation from the anticipated outcome of those processes.

Business stakeholders (senior management, board of directors...) are aware of the cybersecurity status of the organisation (by means of regular management reviews, for example) and situational awareness is also underpinned by detailed metrics.

CYFUN® LEVEL 5 – OPTIMISING

Key elements: Formal processes, organisation-oriented, controlled, proactive, measured and a focus on continual improvement

Cybersecurity practices build upon established CyFun® Level 4 maturity criteria and are implemented in a time-sensitive way in order to support operational efficiency. This may include automated actions (such as those carried out by means of machine learning or artificial intelligence (AI)).

Exceptions from cybersecurity practices implemented organisation-wide are limited to less than 0.5% of all processes, and are documented, justified and approved.

Quantitative performance objectives (targets) for process effectiveness and efficiency are set, based on the organisation's business goals.

Assessment of the processes shows that less than 1% of the processes involve a deviation from the anticipated outcome of those processes.

Process improvements are implemented in accordance with "continuous improvement" practices in order to influence process change.

The above is based on interpretations contained in the Secure Controls Framework – Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM).

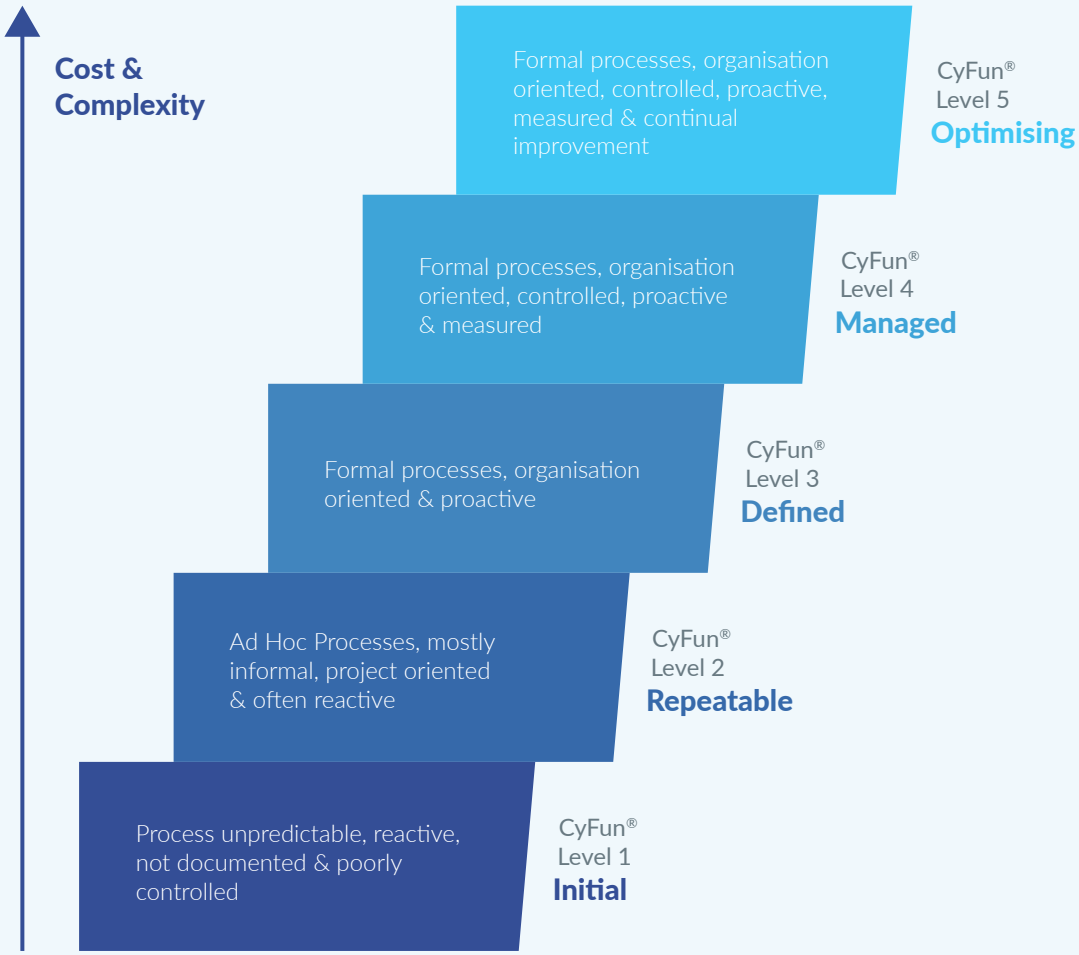


Figure: Overview of CyberFundamentals Maturity Levels


Username
Password
Protected
Balance:
5.367.50 $

Maturity level use cases **PROTECT**

Protect

Maturity level use cases ‘Protect’

PR.AC-1.1 Identities and credentials for authorised devices and users shall be managed.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version controlled and approved) documentation exists specifying how identities and credentials for authorised devices and users are managed.
2	Controlled (version and approved) documentation (policy, process, SOP…) on how identities and credentials for authorised devices and users are managed exists but has not been reviewed in the past 2 years.
3	Controlled (version and approved) documentation on how identities and credentials for authorised devices and users are managed is available and up to date. Exceptions from the process are documented and approved and are only applicable in less than 5% of the total number of authorised devices and users identified.
4	Controlled (version and approved) documentation on how identities and credentials for authorised devices and users are managed exists and is regularly reviewed and updated. Exceptions from the process are documented and approved and are only applicable in less than 3% of the total number of authorised devices and users identified.
5	Controlled (version and approved) documentation on how identities and credentials for authorised devices and users are managed exists and is regularly reviewed and updated. Exceptions from the process are documented and approved and are only applicable on less than 0.5% of the total number of authorised devices and users identified.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No management of identities and credentials for authorised devices and users has been defined or implemented.
2	Identities and credentials for authorised devices and users are managed informally by means of an ad hoc process.
3	Identities and credentials for authorised devices and users are managed as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for most activities. Reviews (e.g. audits) of the implemented process (e.g. by means of a review of the password policy) reveal that inconsistencies between what is documented and what is implemented in the field amount to less than 10%.
4	Identities and credentials for authorised devices and users are managed as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for most activities. Reviews (e.g. audits) show that the process is not followed in less than 5% of cases. Metrics, including targets, are in place to monitor the identity and credential management for authorised devices and users. Process performance is reported as described in the applicable process documentation.
5	Identities and credentials for authorised devices and users are managed as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for most activities. Reviews (e.g. audits) show that the process is not followed in less than 1% of cases. Metrics, including targets, are in place to monitor the identity and credential management for authorised devices and users. Process performance results are translated into opportunities for improvement. Process performance is reported as described in the applicable process documentation.

PR.AC-3.2 When accessed remotely, the organisation's networks shall be secured, including through the use of multi-factor authentication (MFA).

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version controlled and approved) documentation exists to ensure that the organisation's networks are secured when accessed remotely.
2	Controlled (version controlled and approved) documentation exists to ensure that the organisation's networks are secured when accessed remotely, but this documentation has not been reviewed in the past 2 years.
3	Controlled (version and approved) documentation that ensures that the organisation's networks are secured,, incl. the use of MFA when accessed remotely, is available and up-to-date. Exceptions from the requirement to use secure remote access protocols (e.g. MFA) are documented and approved and are limited to less than 5% of remote connections to the organisation's network measured against the average number of remote connections made in a formally predetermined period (e.g. by using activity logs covering a period of the past 6 months).
4	Controlled (version and approved) documentation that ensures that the organisation's networks are secured, incl. the use of MFA when accessed remotely, is available and regularly reviewed and updated. Exceptions from the requirement to use remote access protocols (e.g. MFA) are documented and approved and are limited to less than 3% of remote connections to the organisation's network (measured as explained under Maturity level 3).
5	Controlled (version and approved) documentation that ensures that the organisation's networks are secured, incl. the use of MFA when accessed remotely, is available and regularly reviewed and updated. Exceptions from the requirement to use remote access protocols (e.g. MFA) are documented and approved and are limited to less than 0.5% of remote connections to the organisation's network (measured as explained under Maturity level 3).

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No process has been implemented to ensure that the organisation's networks are secured when accessed remotely.
2	Securing the organisation's networks when accessed remotely is carried out on an ad-hoc basis without any formal management of the process.
3	Securing the organisation's networks when accessed remotely is carried out as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for most activities. Reviews (e.g. audits) of the implemented process show that inconsistencies between what is documented and what is implemented in the field (e.g. not using MFA where it is prescribed) amount to less than 10%.
4	Securing the organisation's networks when accessed remotely is carried out as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) show that the process is not followed in less than 5% cases. Metrics, including targets, are in place to monitor the process. Process performance is reported as described in the applicable process documentation.
5	Securing the organisation's networks when accessed remotely is carried out as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) show that the process is not followed in less than 1% cases. Metrics, including targets, are in place to monitor the process. Process performance results are translated into opportunities for improvement. Process performance is reported as described in the applicable process documentation.

PR.AC-4.1 Access permissions for users to the organisation's systems shall be defined and managed.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version controlled and approved) documentation on managing access permissions for users to the organisation's systems exists.
2	Controlled (version and approved) documentation (policy, process, SOP…) on managing access permissions for users of the organisation's systems exists but has not been reviewed in the past 2 years.
3	Controlled (version and approved) documentation on managing permissions that allow users to access the organisation's systems is available and up to date. Exceptions from the process are documented and approved and are only applicable to less than 5% of the total of identified users of the organisation's systems.
4	Controlled (version and approved) documentation on managing permissions that allow users to access the organisation's systems exists and is regularly reviewed and updated. Exceptions from the process are documented and approved and are only applicable to less than 3% of the total of identified users.
5	Controlled (version and approved) documentation on managing permissions that allow users to access the organisation's systems is available, regularly reviewed and up to date. Exceptions from the process are documented and approved and are only applicable to less than 0.5% of the total of identified users.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	Access permissions for users of the organisation's systems are neither defined nor managed (e.g. no access lists per system, no difference between user accounts or admin accounts, no central account management system).
2	Access permissions for users of the organisation's systems are managed by means of an ad hoc process and is done informally.
3	Access permissions for users of the organisation's systems are managed as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for most activities. Reviews (e.g. audits) of the implemented process reveal that inconsistencies between what is documented and what is implemented in the field amount to less than 10%.
4	User Access permissions are managed as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) show that the process is not followed in less than 5% of cases. Metrics, including targets, are in place to monitor the user access permission process. Process performance is reported as described in the applicable process documentation.
5	User Access permissions are managed as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) show that the process is not followed in less than 1% of cases. Metrics, including targets, are in place to monitor the user access permission process. Process performance results are translated in opportunities for improvement. Process performance is reported as described in the applicable process documentation.

PR.AC-4.2 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.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version controlled and approved) documentation stating who has access to the business' critical information and how to get access to that information exists.
2	Controlled (version and approved) documentation (policy, process, SOP…) stating who has access to the business' critical information and how to get access to that information exists, but the documentation has not been reviewed in the past 2 years.
3	Controlled (version and approved) documentation stating who has access to the business' critical information and how to get access to that information is available and up to date. Exceptions from the process are documented and approved and are only applicable to less than 5% of the total of the critical information identified in the organisation's critical information list (CIL).
4	Controlled (version and approved) documentation stating who has access to the business' critical information and how to get access to that information exists and is regularly reviewed and updated. Exceptions from the process are documented and approved and are only applicable to less than 3% of the total of the critical information identified in the organisation's critical information list (CIL).
5	Controlled (version and approved) documentation stating who has access to the business' critical information and how to get access to that information exists and is regularly reviewed and updated. Exceptions from the process are documented and approved and are only applicable to less than 0,5% of the total of the critical information identified in the organisation's critical information list (CIL).

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There are no requirements concerning the identification of who should have access and the means used to get access to the business' critical information are neither identified nor managed.
2	The identification of who has access to the business' critical information and how to get access to that information is managed by means of an ad hoc process and is done informally.
3	The identification of who has access to the business' critical information and how to get access to that information is performed as specified in the relevant process documentation, together with the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of the implemented process reveal that inconsistencies between what is documented and what is implemented in the field amount to less than 10%.
4	The identification of who has access to the business' critical information and in what way is performed as specified in the relevant process documentation, together with the documented exceptions. Evidence of process implementation is available for all activities. Reviews (e.g. audits) show that the process is not followed in less than 5% of cases. Metrics, including targets, are in place to monitor the process. Process performance is reported as described in the applicable process documentation.
5	The identification of who has access to the business' critical information and in what way is performed as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) show that the process is not followed in less than 1% of cases. Metrics, including targets, are in place to monitor the process. Process performance results are translated into opportunities for improvement. Process performance is reported as described in the applicable process documentation.

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).

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version controlled and approved) documentation exists to ensure that each employee only receive the system resources and authorisations needed to perform their job role.
2	Controlled (version controlled and approved) documentation exists to ensure that each employee only gets the system resources and authorisations needed to perform their job role, but this documentation has not been reviewed in the past 2 years.
3	Controlled (version and approved) documentation on the limitation of employee access to data and information is available and up to date. Exceptions from the principle of Least Privilege are documented and approved and may not exceed more than 4% of the accounts, processes, programs and other resources identified in the role description.
4	Controlled (version and approved) documentation on the limitation of employee access to data and information exists and is regularly reviewed and updated. Exceptions from the principle of Least Privilege are documented and approved and may not exceed more than 2% of the accounts, processes, programs and other resources identified in the role description.
5	Controlled (version and approved) documentation on the limitation of employee access to data and information exists and is regularly reviewed and updated. There are no exceptions from the principle of Least Privilege and access to accounts, processes, programs and other resources is as identified in the role description.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	Employee access to data and information is not limited to the systems and specific information they need to do their jobs.
2	Employee access to data and information is limited to the systems and specific information they need to do their jobs on an ad hoc basis and is managed informally.
3	The implementation of the principle of Least Privilege is performed as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of the implemented process show that inconsistencies between what is documented and what is implemented in the field amount to less than 10%.
4	The implementation of the principle of Least Privilege is performed as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) show that the process is not followed in less than 5% of cases. Metrics, including targets, are in place to monitor the process. Process performance is reported as described in the applicable process documentation.
5	The implementation of the principle of Least Privilege is performed as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) show that the process is not followed in less than 1% of cases. Metrics, including targets, are in place to monitor the process. Process performance results are translated into opportunities for improvement. Process performance is reported as described in the applicable process documentation.

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

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version controlled and approved) documentation exists to ensure that nobody has administrator privileges for daily tasks.
2	Controlled (version controlled and approved) documentation exists to ensure that nobody has administrator privileges for daily tasks, but this documentation has not been reviewed in the past 2 years.
3	Controlled (version and approved) documentation that ensures that nobody has administrator privileges for daily tasks is available and up to date. Exceptions concerning the granting of personnel administrator privileges for daily tasks are documented and approved and are limited to less than 5% of the personnel active within the entity.
4	Controlled (version and approved) documentation that ensures that nobody has administrator privileges for daily tasks is available, regularly reviewed and updated. Exceptions concerning the granting of personnel administrator privileges for daily tasks are documented and approved and are limited to less than 3% of the personnel active within the entity.
5	Controlled (version and approved) documentation that ensures that nobody has administrator privileges for daily tasks is available, regularly reviewed and updated. Exceptions concerning the granting of personnel administrator privileges for daily tasks are documented and approved and are limited to less than 0.5% of the personnel active in the entity.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No process has been implemented that ensures that nobody has administrator privileges for daily tasks.
2	Administrator privileges for daily tasks are informally granted on an ad hoc basis.
3	Ensuring that nobody has administrator privileges for daily tasks is carried out as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for most activities. Reviews (e.g. audits) of the implemented process show that inconsistencies between what is documented and what is implemented in the field amount to less than 10%.
4	Ensuring that nobody has administrator privileges for daily tasks is carried out as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) show that the process is not followed in less than 5% of cases. Metrics, including targets, are in place to monitor the process. Process performance is reported as described in the applicable process documentation.
5	Ensuring that nobody has administrator privileges for daily tasks is carried out as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) show that the process is not followed in less than 1% of cases. Metrics, including targets, are in place to monitor the process. Process performance results are translated into opportunities for improvement. Process performance is reported as described in the applicable process documentation.

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

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version controlled and approved) documentation on the installation and activation of firewalls exists (e.g. process documentation, inventories of installed and activated firewalls).
2	Controlled (version controlled and approved) documentation on the installation and activation of firewalls exists but has not been reviewed in the past 2 years. Inventories are outdated.
3	Controlled (version and approved) documentation on the installation and activation of firewalls exists. Inventories are up to date. Exceptions from the process are documented and approved and only apply to less than 5% of the gateways to the Internet.
4	Controlled (version and approved) documentation on the installation and activation of firewalls exists and is regularly reviewed and updated. Inventories are up to date. Exceptions from the process are documented and approved and only apply to less than 3% of the gateways to the Internet.
5	Controlled (version and approved) documentation on the installation and activation of firewalls exists and is regularly reviewed and updated. Inventories are up to date. Exceptions from the process are documented and approved and only apply to less than 0.5% of the gateways to the Internet.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	Firewalls have been installed and activated but no additional information is available.
2	Firewalls are installed and activated on an ad hoc basis. Information on the installed and activated firewalls is informal (e.g. "The ICT Manager knows where they are").
3	Firewalls are installed and activated as specified in the relevant process documentation, including the documented exceptions. Inventories, including location, firmware, serial number and maintenance data are available for more than 90% of the installed and activated firewalls. Evidence regarding process implementation is available for most activities.
4	Firewalls are installed and activated as specified in the relevant process documentation, including the documented exceptions. Inventories, including location, firmware, serial number and maintenance data are available for more than 95% of the installed and activated firewalls. Evidence regarding process implementation is available for all activities. Metrics on firewall updates, maintenance and replacement have been established and are monitored and acted upon. Clear targets with regard to updates are available, demonstrating the firewalls' capability to provide sufficient protection against threats.
5	Firewalls are installed and activated as specified in the relevant process documentation, including the documented exceptions. Inventories, including location, firmware, serial number and maintenance data are available for more than 99% of the installed and activated firewalls. Metrics on firewall updates, maintenance and replacement have been established and are monitored and acted upon. Evidence regarding process implementation is available for all activities. Clear targets with regard to updates are available, demonstrating the firewalls' capability to provide sufficient protection against threats, including measures to continuously improve that protection.

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

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version controlled and approved) documentation on network segmentation and segregation (e.g. network segmentation diagram) exists.
2	Controlled (version and approved) documentation on network segmentation and segregation (e.g. a network segmentation diagram) exists, but that documentation has not been reviewed in the last 2 years.
3	Controlled (version and approved) documentation on network segmentation and segregation (e.g. a network segmentation diagram) is available and up to date. Exceptions concerning the number of critical systems that are not segregated from each other (e.g. critical applications, domain controllers, servers, public-facing applications, endpoints, business-critical assets/data) have been documented and approved and are limited to less than 5% of the total number of critical systems identified.
4	Controlled (version and approved) documentation on network segmentation and segregation (e.g. a network segmentation diagram) is available and up to date. Exceptions concerning the number of critical systems that are not segregated from each other (e.g. critical applications, domain controllers, servers, public-facing applications, endpoints, business-critical assets/data) have been documented and approved and are limited to less than 3% of the total number of critical systems identified.
5	Controlled (version and approved) documentation on network segmentation and segregation (e.g. a network segmentation diagram) is available and up to date. There are no exceptions concerning the number of critical systems that are not segregated from each other (e.g. critical applications, domain controllers, servers, public-facing applications, endpoints, business-critical assets/data).

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No network segmentation or segregation has been implemented.
2	Network segmentation and segregation is carried out on an ad hoc basis without a corporate strategy.
3	Network segmentation and segregation are as documented in the relevant documentation. Evidence regarding process implementation is available for most activities. Reviews (e.g. audits) of what is implemented in the field show that inconsistencies with what is documented amount to less than 10%.
4	Network segmentation and segregation is as documented in the relevant documentation. Evidence on process implementation is available for all activities. Reviews (e.g. audits) of what is implemented in the field show that inconsistencies with what is documented amount to less than 5%. Metrics, including targets, are in place to monitor the accuracy of network visualisation to enable the integrity of the network to be assessed. The degree of accuracy of the network visualisation and the network integrity risks are reported as described in the applicable process documentation.
5	Network segmentation and segregation is as documented in the relevant documentation. Evidence on process implementation is available for all activities. Reviews (e.g. audits) of what is implemented in the field show that inconsistencies with what is documented amount to less than 1%. Metrics, including targets, are in place to monitor the accuracy of network visualisation to enable the integrity of the network to be assessed. The degree of accuracy of the network visualisation and the network integrity risks are reported as described in the applicable process documentation. The network integrity risks identified are translated into improvement opportunities that contribute towards the continuous improvement of network integrity.

PR.IP-4.1 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.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version controlled and approved) documentation exists to ensure that backups of the organisation's business-critical data are performed and stored on a system different from the device on which the original data reside.
2	Controlled (version controlled and approved) documentation exists to ensure that backups of organisation's business-critical data are performed and stored on a system different from the device on which the original data resides, but this documentation has not been reviewed in the past 2 years.
3	Controlled (version and approved) documentation to ensure that backups of the organisation's business-critical data are performed and stored on a different system is available and up to date. The process is applicable to more than 95% of the organisation's business critical data; exceptions are documented and approved.
4	Controlled (version and approved) documentation to ensure that backups of the organisation's business-critical data are performed and stored on another system is available, regularly reviewed and updated. The documentation specifying the back-up process prescribes that the process be applied to more than 97% of the organisation's business critical data; exceptions are documented and approved.
5	Controlled (version and approved) documentation to ensure that backups of the organisation's business-critical data are performed and stored on another system is available, regularly reviewed and updated. The documentation specifying the back-up process prescribes that the process be applied to more than 99.5% of the organisation's business critical data; exceptions are documented and approved.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No process has been implemented to ensure that backups of the organisation's business-critical data are performed and stored on a system different from the device on which the original data reside.
2	Backups of the organisation's business-critical data are demonstrably being made. Back-ups are taken and stored on a system different from the device on which the original data reside on an ad-hoc basis and are informally managed.
3	Backups of the organisation's business-critical data and the storage of the backups on a different system different from the device on which the original data reside are performed as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for most activities. Reviews (e.g. audits) of the implemented process show that less than 10% of back-up jobs failed to be carried out.
4	Backups of organisation's business-critical data and storage on a system different from the device on which the original data reside are performed as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for most activities. Reviews (e.g. audits) of the implemented process show that less than 5% back-up jobs failed to be carried out. Metrics, including targets, are in place to monitor the process. Process performance is reported as described in the applicable process documentation.
5	Backups of the organisation's business-critical data and storage on a system different from the device on which the original data reside are performed as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for most activities. Reviews (e.g. audits) of the implemented process show that less than 1% of back-up jobs failed to be carried out. Metrics, including targets, are in place to monitor the process. Process performance results are translated into process improvements. Process performance is reported as described in the applicable process documentation.

PR.MA-1.1 Patches and security updates for operating systems and critical system components shall be installed.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	Critical system components and operating systems that are essential for the performance of the business (both production as services) are not defined, nor is there a controlled (version controlled and approved) patching process in place.
2	Critical system components and operating systems that are essential for the performance of the business (both production as services) are defined and a patching process has been put in place in a controlled manner (formally approved and under version control), though this documentation and/or the patching process are outdated (e.g. not reviewed in the past 2 years).
3	Critical system components and operating systems that are essential for the performance of the business (both production as services) are defined and a patching process has been put in place in a controlled manner (formally approved and under version control). Documentation is regularly reviewed (e.g. yearly or earlier when needed). Exemptions to the patch management schedule are documented and limited to those cases that can be operationally explained.
4	Critical system components, operating systems and a patching process are formally documented and regularly reviewed, including a reporting mechanism. Exemptions and exceptions from the patch management schedule are documented and are limited to those cases that can be operationally explained; the patch management schedule includes priority for critical and security patches.
5	Critical system components, operating systems and a patching process are formally documented and regularly reviewed, including a reporting mechanism. Exemptions from the patch management schedule are documented, are limited to those cases that can be operationally explained and prioritise critical and security patches. Exemptions and exceptions are kept to a minimum by using documented patch management tools (e.g. vendor supported scanning tools).

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No patches are installed.
2	Patches are installed on an ad hoc basis without a clear definition regarding responsibilities and authorities.
3	The patching process is rolled out as documented. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of the patch management process show that the process is not followed in less than 10% of cases. The operational reason for documented exemptions and exceptions is valid.
4	The patching process is rolled out as documented. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) of the patch management process show that the process is not followed in less than 5% of cases. The operational reason for documented exemptions and exceptions is valid. Metrics, including targets, are in place to monitor the implementation of the patch management schedule. Performance of the patch management process is reported as described in the patching process.
5	The patching process is implemented as described. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) of the patch management process show that the process is not followed in less than 1% of cases. The operational reason for documented exemptions and exceptions is valid. Metrics, including targets, are in place to monitor the implementation of the patch management schedule. Patch management monitoring is translated into opportunities for improvement (e.g. optimisation of the schedule). Performance of the patch management process is reported as described in the patching process.

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

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version controlled and approved) documentation exists to ensure that activity logging is enabled, documented and reviewed.
2	Controlled (version controlled and approved) documentation exists to ensure that activity logging is enabled, documented and reviewed, but this documentation has not been reviewed in the past 2 years.
3	Controlled (version and approved) documentation that ensures that activity logging is enabled, documented and reviewed is available and up to date. Exceptions from the requirement to enable activity logging are documented and approved and may not exceed more than 4% of all protection/detection hardware and software deployed within the entity.
4	Controlled (version and approved) documentation that ensures that activity logging is enabled, documented and reviewed is available and is regularly reviewed and updated. Exceptions from the requirement to enable activity logging are documented and approved and may not exceed more than 2% of all protection/detection hardware and software deployed within the entity.
5	Controlled (version and approved) documentation that ensures that activity logging is enabled, documented and reviewed is available and is regularly reviewed and updated. Exceptions from the requirement to enable activity logging are documented and approved and are limited to less than 0.5% of all protection/detection hardware and software deployed within the entity.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	Activity logging is not enabled for any of the protection/detection hardware and software deployed within the entity.
2	The enabling of the activity logging functionality of the protection/detection hardware and software deployed within the entity and the reviewing of the logs are carried out on an ad hoc basis and is managed informally.
3	The enabling of the activity logging functionality of the protection/detection hardware and software deployed in the entity and the reviewing of the logs are carried out as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for most activities. Reviews (e.g. audits) of the implemented process show that inconsistencies between what is documented and what is implemented in the field amounts to less than 10%.
4	The enabling of the activity logging functionality of the protection/detection hardware and software deployed in the entity and the reviewing of the logs are carried out as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) show that the process is not followed in less than 5% of cases. Metrics, including targets, are in place to monitor the process. Process performance is reported as described in the applicable process documentation.
5	The enabling of the activity logging functionality of the protection/detection hardware and software deployed in the entity and the reviewing of the logs are carried out as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) show that the process is not followed in less than 1% of cases. Metrics, including targets, are in place to monitor the process. Process performance results are translated into opportunities for improvement. Process performance is reported as described in the applicable process documentation.


WARNING!
SYSTEM WARNING

Maturity level use cases

DETECT

Detect

Maturity level use cases ‘Detect’

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.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version controlled and approved) documentation exists to ensure that activity logging is enabled, backed up and reviewed.
2	Controlled (version controlled and approved) documentation exists to ensure that activity logging is enabled, backed up and reviewed, but this documentation has not been reviewed in the past 2 years.
3	Controlled (version and approved) documentation that ensures that activity logging is enabled, backed up and reviewed is available and up to date. Exceptions from the requirement to enable and back up activity logging and to review of the logs are documented and approved and may not exceed more than 4% of all protection/detection hardware and software deployed within the entity.
4	Controlled (version and approved) documentation that ensures that activity logging is enabled, documented and reviewed is available, regularly reviewed and updated. Exceptions from the requirement to enable and back up activity logging and review the logs are documented and approved and may not exceed more than 2% of all protection/detection hardware and software deployed within the entity.
5	Controlled (version and approved) documentation that ensures that activity logging is enabled, documented and reviewed is available, regularly reviewed and updated. Exceptions from the requirement to enable and back up activity logging and review the logs are documented and approved and are limited to less than 0.5% of all protection/detection hardware and software deployed within the entity.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	Activity logging is not enabled for any of the protection/detection hardware and software deployed within the entity.
2	The enabling of the activity logging functionality of the protection/detection hardware and software deployed within the entity and the backing up and reviewing of the logs are carried out on an ad hoc basis and is managed informally.
3	The enabling of the activity logging functionality of the protection/detection hardware and software deployed within the entity and the backing up and reviewing of the logs are carried out as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for most activities. Reviews (e.g. audits) of the implemented process show that inconsistencies between what is documented and what is implemented in the field amount to less than 10%.
4	The enabling of the activity logging functionality of the protection/detection hardware and software deployed in the entity and the backing up and reviewing of the logs are carried out as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) show that the process is not followed in less than 5% of cases. Metrics, including targets, are in place to monitor the process. Process performance is reported as described in the applicable process documentation.
5	The enabling of the activity logging functionality of the protection/detection hardware and software deployed in the entity and the backing up and reviewing of the logs are carried out as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) show that the process is not followed in less than 1% of cases. Metrics, including targets, are in place to monitor the process. Process performance results are translated into opportunities for improvement. Process performance is reported as described in the applicable process documentation.

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

Documentation Maturity

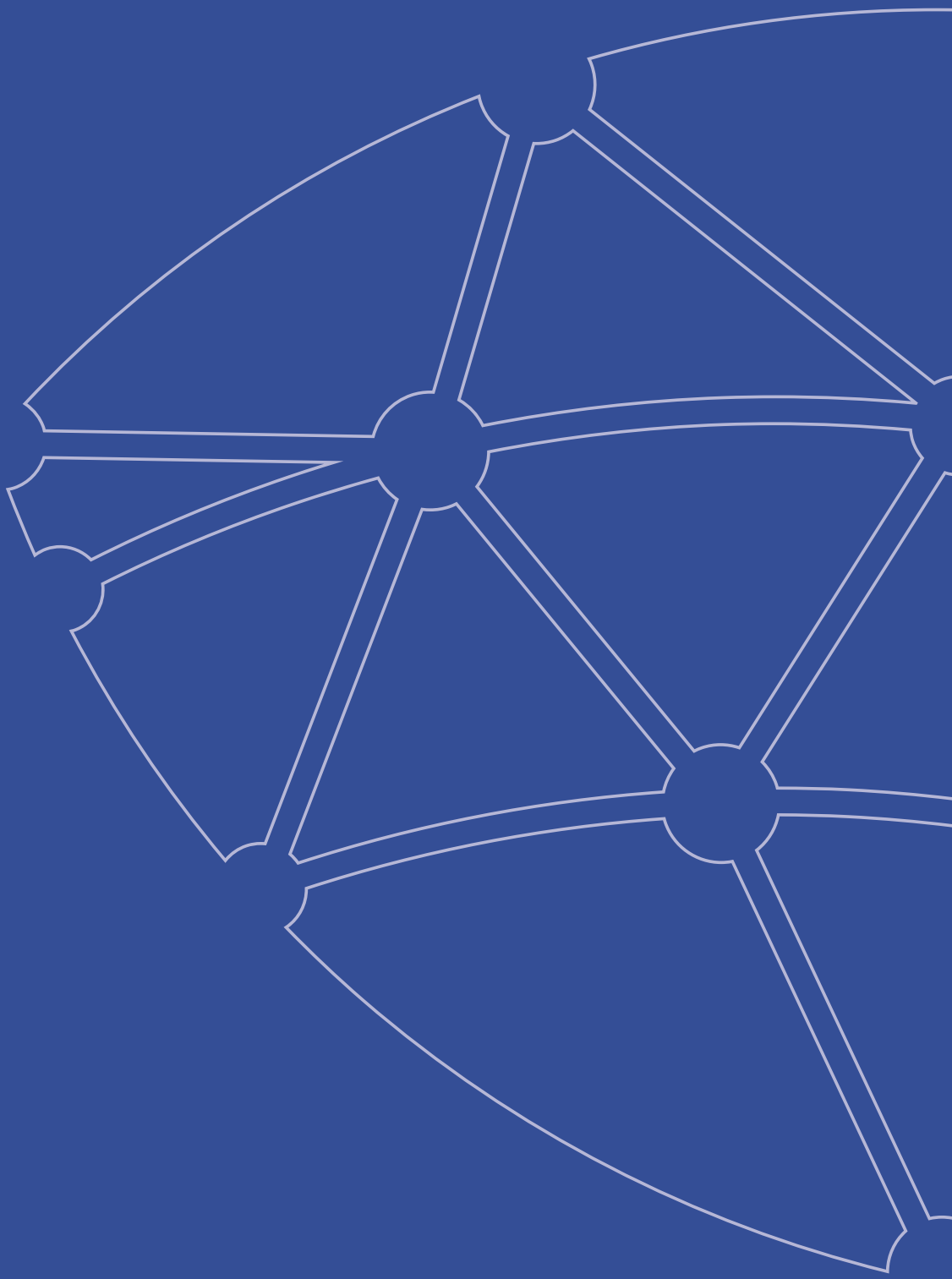
MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version controlled and approved) documentation on managing malware protection (virus, spyware, ransomware, adware, rootkits) exists.
2	A policy or process to manage malware protection is formally documented (version controlled and approved) but not reviewed regularly (e.g. was not reviewed in the past 2 years).
3	A policy or process to manage malware protection is formally documented (version controlled and approved) and reviewed regularly. Documented and approved exceptions (e.g. excluding file types from malware inspection) are applicable to less than 5% of the devices (computers, smart phones, tablets, servers...) used within company's business.
4	A policy or process to manage malware protection, including a reporting mechanism, is formally documented (version controlled and approved) and reviewed regularly. Documented and approved exceptions are applicable to less than 3% of the devices used within the company's business.
5	A policy or process to manage malware protection, including a reporting mechanism, is formally documented (version controlled and approved) and reviewed regularly. Documented and approved exceptions are applicable to less than 0.5% of the devices used within the company's business.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No malware protection policy or process is in place.
2	A process to manage malware protection is applied on an ad hoc basis without a clear definition of responsibilities and authorities.
3	The malware protection process is rolled out as documented. Evidence regarding process implementation is available for most activities. Reviews (e.g. audits) of the malware protection process show that the process is not followed (e.g. endpoints where the malware protection is not up to date) in less than 10% of cases.
4	The malware protection process is rolled out as documented. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) of the malware protection process show that the process is not followed in less than 5% of cases. Metrics, including targets, are in place to monitor the implementation of the malware protection process. The performance of malware protection is reported as described in the malware protection process.
5	The malware protection process is rolled out as documented. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) of the malware protection process show that the process is not followed in less than 1% of cases. Metrics, including targets, are in place to monitor the implementation of the malware protection process. Malware protection monitoring (e.g. analysis of effectiveness of malware protection) is translated into opportunities for improvement. The performance of malware protection is reported as described in the malware protection process.

Responsible editor

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



Centre for Cybersecurity Belgium

Rue de la Loi, 18

1000 Brussels