CyFun®

IMPORTANT

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).

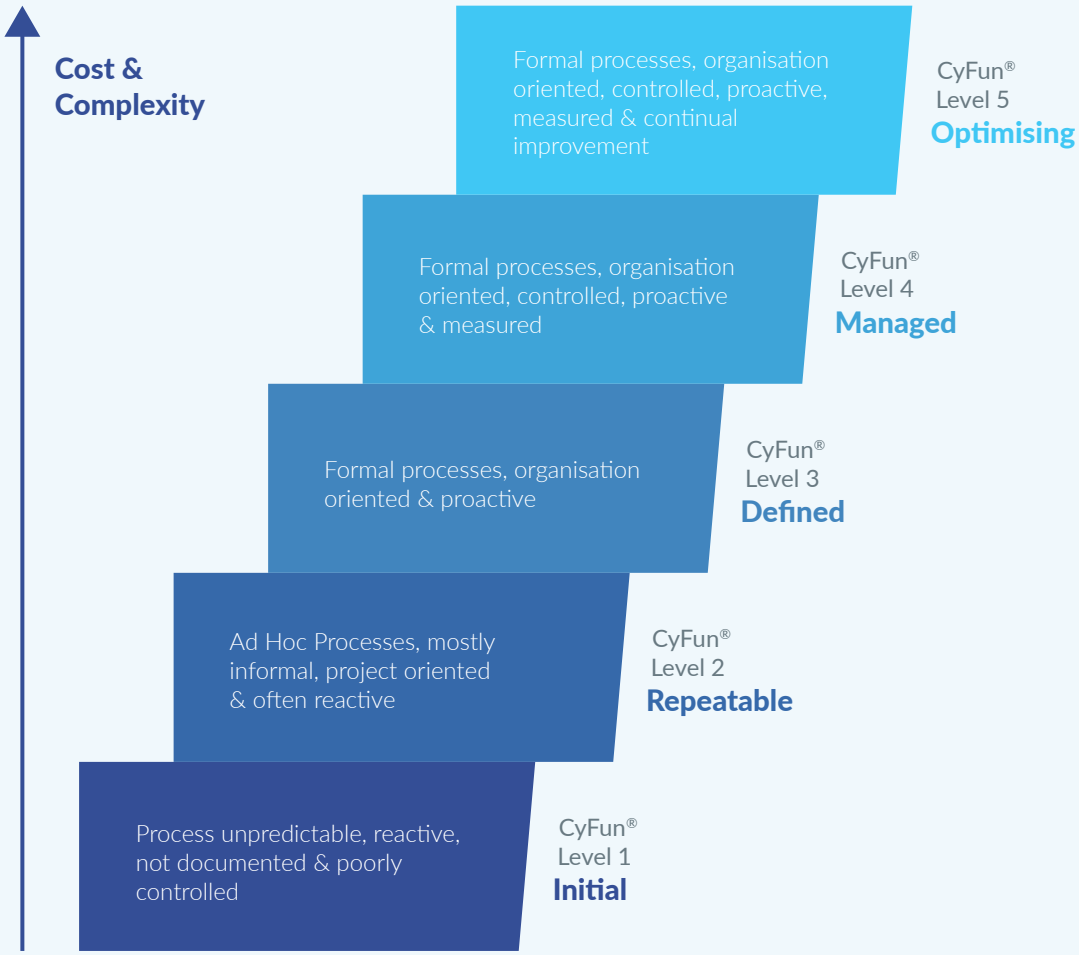


Figure: Overview of CyberFundamentals Maturity Levels

Maturity level use cases
IDENTIFY

Identify

Maturity level use cases ‘Identify’

ID.AM-6.1 Information security and cybersecurity roles, responsibilities and authorities within the organisation shall be documented, reviewed, authorised, and updated and aligned with organisation-internal roles and external partners.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There are no controlled (version controlled and approved) descriptions of roles, responsibilities and authorities for key positions in the organisation and external partners who have access to the organisation's ICT/OT environment.
2	There are controlled (version controlled and approved) descriptions of roles, responsibilities and authorities for key positions in the organisation and external partners who have access to the organisation's ICT/OT environment, but they have not been reviewed in the past 2 years.
3	There are controlled (version controlled and approved) and up-to-date descriptions of roles, responsibilities and authority for key positions in the organisation and external partners who have access to the organisation's ICT/OT environment. There is a documented and approved reason for missing descriptions of roles, responsibilities and authorities and the number of missing descriptions is less than 5% of the total number of identified key positions in the organisation and external partners that have access to the organisation's ICT/OT environment.
4	There are controlled (version controlled and approved) and up-to-date descriptions of roles, responsibilities and authority for key positions in the organisation and external partners who have access to the organisation's ICT/OT environment. There is a documented and approved reason for missing descriptions of roles, responsibilities and authorities and the number of missing descriptions is less than 3% of the total number of identified key positions in the organisation and external partners that have access to the organisation's ICT/OT environment.
5	There are controlled (version controlled and approved) and up-to-date descriptions of roles, responsibilities and authority for key positions in the organisation and external partners who have access to the organisation's ICT/OT environment. All roles, responsibilities and authorities of key positions in the organisation and external partners that have access to the organisation's ICT/OT environment are documented (no exceptions).

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no process to ensure that there is a description for the roles, responsibilities and authorities for key positions in the organisation and external partners who have access to the organisation's ICT/OT environment.
2	Roles, responsibilities and authorities for key positions in the organisation and external partners who have access to the organisation's ICT/OT environment are documented in an ad hoc way and managed informally.
3	Roles, responsibilities and authorities for key positions in the organisation and external partners who have access to the organisation's ICT/OT environment are documented. Reviews (e.g. audits) show that inconsistencies between what is documented and the real situation occur in less than 10% of cases.
4	A formal process has been implemented resulting in roles, responsibilities and authority for key positions in the organisation and external partners who have access to the organisation's ICT/OT environment being documented. Metrics have been deployed and minimum targets (e.g. a number of descriptions) identified. Reviews (e.g. audits) show that inconsistencies between what is documented and the real situation occur in less than 5% of the cases. Process performance is reported as described in the applicable process documentation.
5	A formal process has been implemented resulting in roles, responsibilities and authority for key positions in the organisation and external partners who have access to the organisation's ICT/OT environment being documented. Metrics, including minimum targets (e.g. a number of descriptions), are deployed to monitor the process. Reviews (e.g. audits) show that inconsistencies between what is documented and the real situation occur in less than 1% of the cases. Inconsistencies identified lead to improvement actions that contribute towards continuous process improvement. Process performance is reported as described in the applicable process documentation.

ID.GV-4.2 Information security and cybersecurity risks shall be documented, formally approved, and updated when changes occur.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no process documentation or formally approved documentation by management to ensure that information security and cybersecurity risks are documented, formally approved, and updated when changes occur.
2	The organisation has a controlled process documentation (versioned and approved) to ensure that information security and cybersecurity risks are documented, formally approved, and updated whenever changes occur, but that documentation has not been reviewed in the past 2 years.
3	Controlled (versioned, approved) process documentation exists to ensure that information security and cybersecurity risks are documented and formally approved, and that documentation is reviewed regularly. Of the total number of information security and cybersecurity risks identified, less than 5% do not have action plans to mitigate the identified risks. The reason for this is documented and approved.
4	Controlled (versioned, approved) process documentation exists to ensure that information security and cybersecurity risks are documented and formally approved, and that documentation is reviewed regularly. Of the total number of information security and cybersecurity risks identified, less than 3% do not have action plans to mitigate the identified risks. The reason for this is documented and approved.
5	Controlled (versioned, approved) process documentation exists to ensure that information security and cybersecurity risks are documented, and formally approved, and that documentation is reviewed regularly. All information security and cybersecurity risks identified have action plans to mitigate the identified risks.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no standard process to ensure that information security and cybersecurity risks are documented, formally approved, and updated when changes occur.
2	Information security and cybersecurity risks are documented, formally approved, and updated on an ad hoc basis whenever changes occur. This entire process is managed informally.
3	A formal process exists and is implemented to document, formally approve, and update information security and cybersecurity risks whenever changes occur. Evidence proving that information security and cybersecurity risks are documented, approved and updated, is available in most cases. Taking into account the exceptions identified in the documentation, reviews (e.g. audits) show that in less than 10% of the total number of information security and cybersecurity risks identified, the progress of action plans to control risks is not monitored.
4	A formal process exists and has been implemented to document, formally approve, and update information security and cybersecurity risks whenever changes occur. Evidence proving that information security and cybersecurity risks are documented, approved and updated is available at all times. Taking into account the exceptions identified in the documentation, reviews (e.g. audits) show that in less than 5% of the total number of identified information security and cybersecurity risks identified, the progress of action plans to control risks is not monitored. Detailed process performance metrics, including minimum process performance targets, are measured and reported.
5	A formal process exists and has been implemented to document, formally approve, and update information security and cybersecurity risks whenever changes occur. Evidence proving that information security and cybersecurity risks are documented, approved and updated is available at all times. Taking into account the exceptions identified in the documentation, reviews (e.g. audits) show that in less than 10% of the total number of information security and cybersecurity risks identified, the progress of action plans to control risks is not monitored. Detailed process performance metrics, including minimum process performance targets, are measured, reported and show continuous improvement.

ID.RA-5.2 The organisation shall conduct and document risk assessments in which risk is determined by threats, vulnerabilities, impact on business processes and assets, and the likelihood of their occurrence.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no process documentation or formally approved documentation by management to ensure that the organisation conducts and documents risk assessments.
2	The organisation has controlled process documentation (versioned and approved) to ensure that it conducts and documents risk assessments in which risk is determined by threats, vulnerabilities, impact on business processes and assets, and the likelihood of their occurrence, but that documentation has not been reviewed in the past 2 years.
3	Controlled (versioned, approved) process documentation exists to ensure that the organisation conducts and documents risk assessments in which risk is determined by threats, vulnerabilities, impact on business processes and assets, and the likelihood of their occurrence, and this documentation is reviewed regularly. No risk assessments are performed for less than 5% of the total number of core processes identified within the organisation. The reason for this is documented and approved.
4	Controlled (versioned, approved) process documentation exists to ensure that the organisation conducts and documents risk assessments in which risk is determined by threats, vulnerabilities, impact on business processes and assets, and the likelihood of their occurrence, and this documentation is reviewed regularly. No risk assessments are performed for less than 3% of the total number of core processes identified within the organisation. The reason for this is documented and approved.
5	Controlled (versioned, approved) process documentation exists to ensure that the organisation conducts and documents risk assessments in which risk is determined by threats, vulnerabilities, impact on business processes and assets, and the likelihood of their occurrence, and this documentation is reviewed regularly. No risk assessments are performed for less than 0.5% of the total number of processes identified within the organisation, which practically amounts to none. If exclusions are made, the reason for that is documented and approved.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no standard process to ensure that the organisation conducts and documents risk assessments.
2	Risk assessments in which risk is determined by threats, vulnerabilities, impact on business processes and assets, and the likelihood of their occurrence are performed on an ad hoc basis (e.g. intuitive ranking of the risks) and are managed informally.
3	A formal process exists and is implemented to perform risk assessments in which risk is determined by threats, vulnerabilities, impact on business processes and assets, and the likelihood of their occurrence. Evidence, in line with the processes on which risk assessments are performed, is mostly available. For less than 10% of the processes on which risk assessments are performed, reviews (e.g. audits) show that risks are not determined by threats, vulnerabilities, impact on business processes and assets, and the likelihood of their occurrence (e.g. handling multiple scales in the organisation).
4	A formal process exists and is implemented to perform risk assessments in which risk is determined by threats, vulnerabilities, impact on business processes and assets, and the likelihood of their occurrence. Evidence, in line with the processes on which risk assessments are performed, is always available. For less than 5% of the processes on which risk assessments are performed, reviews (e.g. audits) show that risks are not determined by threats, vulnerabilities, impact on business processes and assets, and the likelihood of their occurrence. Detailed process performance metrics, including minimal process performance targets, are measured and reported.

MATURITY	EVIDENCE TO BE CONSIDERED
5	A formal process exists and is implemented to perform risk assessments in which risk is determined by threats, vulnerabilities, impact on business processes and assets, and the likelihood of their occurrence. Evidence, in line with the processes on which risk assessments are performed, is always available. For less than 1% of the processes on which risk assessments are performed, reviews (e.g. audits) show that risks are not determined by threats, vulnerabilities, impact on business processes and assets, and the likelihood of their occurrence. Detailed process performance metrics, including minimal process performance targets, are measured, reported and show continuous improvement.

ID.RA-6.1 A comprehensive strategy shall be developed and implemented to manage risks to the organisation's critical systems, that includes the identification and prioritisation of risk responses.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no controlled (version-controlled and approved) documented strategy to manage risks to the organisation's critical systems that includes the identification and prioritisation of risk responses.
2	There is a controlled (version controlled and approved) documented strategy to manage risks to the organisation's critical systems that includes the identification and prioritisation of risk responses, but it has not been reviewed in the past 2 years.
3	There is a controlled (version controlled and approved) documented strategy to manage risks to the organisation's critical systems, including the identification and prioritisation of risk responses. The strategy however only covers a part of the organisation's critical systems. The organisation's critical systems that are not covered are limited to less than 5% of all of the critical systems identified within the organisation. The reason for the exclusion of critical systems is documented and approved.
4	There is a controlled (version controlled and approved) documented strategy to manage risks to the organisation's critical systems, including the identification and prioritisation of risk responses. The strategy however only covers a part of the organisation's critical systems. The organisation's critical systems that are not covered are limited to less than 3% of all of the critical systems identified within the organisation. The reason for the exclusion of critical systems is documented and approved.
5	There is a controlled (version controlled and approved) documented strategy to manage risks to the organisation's critical systems, including the identification and prioritisation of risk responses. The strategy covers all of the organisation's critical systems. There are no exclusions.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no strategy to manage risks to the organisation's critical systems.
2	The strategy to manage risks to the organisation's critical systems that has been developed is implemented on an ad hoc basis and managed informally.
3	A comprehensive strategy has been developed and implemented to manage risks to the organisation's critical systems, that includes the identification and prioritisation of risk responses, 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	A comprehensive strategy has been developed and implemented to manage risks to the organisation's critical systems, that includes the identification and prioritisation of risk responses, including the documented exceptions. Evidence regarding process implementation is available for all 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 5%. Metrics, including targets, are in place to monitor the implementation of the strategy. Process performance is reported as described in the applicable process documentation.
5	A comprehensive strategy is developed and implemented to manage risks to the organisation's critical systems, that includes the identification and prioritisation of risk responses, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) of the implemented process show that inconsistencies between what is documented and reality amount to less than 1%. Metrics, including targets, are in place to monitor the implementation of the strategy. Process performance results are translated into process improvements. Process performance is reported as described in the applicable process documentation.

ID.RM-1.1 A cyber risk management process that identifies key internal and external stakeholders and facilitates addressing risk-related issues and information shall be created, documented, reviewed, approved, and updated when changes occur.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no controlled (version-controlled and approved) documented cyber risk management process that identifies key internal and external stakeholders and facilitates the addressing of risk-related issues and information.
2	There is a controlled (version controlled and approved) documented cyber risk management process that identifies key internal and external stakeholders and facilitates the addressing of risk-related issues and information which, however, has not been reviewed in the past 2 years.
3	There is a controlled (version controlled and approved) documented cyber risk management process that is regularly reviewed and updated, identifies key internal and external stakeholders and facilitates the addressing of risk-related issues and information. The process is updated whenever changes occur. The number of key internal and external stakeholders for which the process exceptionally does not provide risk management is limited to less than 5% of the total number of identified key internal and external stakeholders (examples of which include customers, investors and shareholders, suppliers, government agencies and the wider community). This is documented and approved.

MATURITY	EVIDENCE TO BE CONSIDERED
4	There is a controlled (version controlled and approved) documented cyber risk management process that is regularly reviewed and updated, identifies key internal and external stakeholders and facilitates the addressing of risk-related issues and information. The process is updated whenever changes occur. The number of key internal and external stakeholders for which the process exceptionally does not provide risk management is limited to less than 3% of the total number of identified key internal and external stakeholders (examples of which include customers, investors and shareholders, suppliers, government agencies and the wider community). This is documented and approved.
5	There is a controlled (version controlled and approved) documented cyber risk management process that is regularly reviewed and updated, identifies key internal and external stakeholders and facilitates the addressing of risk-related issues and information. The process is updated whenever changes occur. The cyber risk management process applies to all key internal and external stakeholders without exception.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version checked and approved) cyber risk management process has been created or implemented.
2	Cyber risk management of key internal and external stakeholders that supports the addressing of risk-related issues and information is performed on an ad hoc and informal basis.
3	The cyber risk management process that identifies key internal and external stakeholders and facilitates the addressing of risk-related issues and information is implemented as documented. Evidence regarding process implementation is available for most activities. Reviews (e.g. audits) reveal inconsistencies between documentation and reality in less than 10% of cases.
4	The cyber risk management process that identifies key internal and external stakeholders and facilitates the addressing of risk-related issues and information is implemented as documented. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) reveal inconsistencies between documentation and reality in less than 5% of cases. Metrics have been deployed and minimal targets on process performance have been identified. Process performance is reported as described in the applicable process documentation.
5	The cyber risk management process that identifies key internal and external stakeholders and facilitates the addressing of risk-related issues and information is implemented as documented. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) reveal inconsistencies between documentation and reality in less than 1% of cases. Inconsistencies identified lead to improvement actions that contribute towards continuous process improvement. Process performance is reported as described in the applicable process documentation.

ID.RM-2.1 The organisation shall clearly determine its risk appetite.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no process documentation or formally approved documentation by management to ensure that the organisation clearly determines its risk appetite.
2	The organisation has controlled process documentation (versioned and approved) to ensure that it clearly determines its risk appetite (e.g. by means of clearly articulated risk appetite statements), but that documentation has not been reviewed in the past 2 years.
3	Controlled (versioned, approved) process documentation exists to ensure that the organisation clearly determines its risk appetite (e.g. by means of clearly articulated risk appetite statements), and this documentation is reviewed regularly. The acceptable deviation from the level set by the risk appetite and business objectives is defined in the form of risk tolerance. For less than 5% of the risk appetite statements, no risk tolerances are established. The reason for this is documented and approved by the management.
4	Controlled (versioned, approved) process documentation exists to ensure that the organisation clearly determines its risk appetite (e.g. by means of clearly articulated risk appetite statements), and this documentation is reviewed regularly. The acceptable deviation from the level set by the risk appetite and business objectives is defined in the form of risk tolerance. For less than 3% of the risk appetite statements, no risk tolerances are established. The reason for this is documented and approved by the management.
5	Controlled (versioned, approved) process documentation exists to ensure that the organisation clearly determines its risk appetite, and this documentation is reviewed regularly. Risk tolerances are established for all risk appetite statements.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no standard process to ensure that the organisation clearly determines its risk appetite.
2	Risk assessment results are disseminated to relevant stakeholders on an ad hoc basis and are managed informally.
3	A formal process exists and is implemented to determine the organisation's risk appetite, for example, by means of risk appetite statements that reflect the organisation's internal and external context, for which evidence is mostly available, considering the documented and approved exceptions. Reviews (e.g. audits) show that determining the risk appetite is not happening according to the documented process in less than 10% of the sample used during a review.
4	A formal process exists and is implemented to determine the organisation's risk appetite, for example, by means of risk appetite statements that reflect the organisation's internal and external context, for which evidence is always available, considering the documented and approved exceptions. Reviews (e.g. audits) show that determining the risk appetite is not happening according to the documented process in less than 5% of the sample used during a review. Detailed process performance metrics, including minimal process performance targets, are measured and reported.
5	A formal process exists and is implemented to determine the organisation's risk appetite, for example, by means of risk appetite statements that reflect the organisation's internal and external context, for which evidence is always available, considering the documented and approved exceptions. Reviews (e.g. audits) show that determining the risk appetite is not happening according to the documented process in less than 1% of the sample used during a review. Detailed process performance metrics, including minimal process performance targets, are measured, reported and show continuous improvement.


Username
Password
Protected
Balance:
5.367.50 $

Maturity level use cases **PROTECT**

Protect

Maturity level use cases ‘Protect’

PR.AC-3.3 Usage restrictions, connection requirements, implementation guidance, and authorisations for remote access to the organisation’s critical systems environment shall be identified, documented and implemented.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	Usage restrictions, connection requirements, implementation guidance, and authorisations for remote access to the organisation’s critical systems environment are not identified or documented.
2	Usage restrictions, connection requirements, implementation guidance, and authorisations for remote access to the organisation’s critical systems environment are identified and documented in a controlled (version and approved) way (e.g. user authentication policies); However, that documentation has not been reviewed in the past 2 years.
3	Usage restrictions, connection requirements, implementation guidance, and authorisations for remote access to the organisation’s critical systems environment are identified and documented in a controlled (version and approved) way. Exceptions from usage restrictions and authorisations for remote access to the organisation’s critical systems environment (e.g. OT devices) are documented, approved and limited to less than 5% of the organisation’s critical systems.
4	Usage restrictions, connection requirements, implementation guidance, and authorisations for remote access to the organisation’s critical systems environment are identified and documented in a controlled (version and approved) way. Exceptions from usage restrictions and authorisations for remote access to the organisation’s critical systems environment (e.g. OT devices) are documented, approved and limited to less than 3% of the total of the organisation’s critical systems.
5	Usage restrictions, connection requirements, implementation guidance, and authorisations for remote access to the organisation’s critical systems environment are identified and documented in a controlled (version and approved) way. There are no exceptions.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There are no usage restrictions, connection requirements, implementation guidance, and authorisations for remote access to the organisation's critical systems environment.
2	Usage restrictions, connection requirements, implementation guidance, and authorisations for remote access to the organisation's critical systems environment are implemented on an ad hoc basis and are managed informally.
3	Usage restrictions, connection requirements, implementation guidance, and authorisations for remote access to the organisation's critical systems environment are as documented in the relevant documentation. Evidence is available for most activities. Reviews (e.g. audits) of what is present in the field reveal less than 10% inconsistencies with what is documented.
4	Usage restrictions, connection requirements, implementation guidance, and authorisations for remote access to the organisation's critical systems environment are as documented in the relevant documentation. Evidence of implementation is available for all activities. Reviews (e.g. by means of audits) reveal less than 5% inconsistencies with what is documented. Detailed metrics of the process, for which minimum targets for metrics have been established, are captured and reported.
5	Usage restrictions, connection requirements, implementation guidance, and authorisations for remote access to the organisation's critical systems environment are as documented in the relevant documentation. Evidence of implementation is available for all activities. Reviews (e.g. by means of audits) reveals less than 1% inconsistencies with what is documented. Detailed metrics of the process, for which minimum targets for metrics have been established, are captured, and reported, and show continuous improvement of process performance.

PR.AC-5.3 Where appropriate, the network integrity of the organisation's critical systems shall be protected by;

(1) identifying, documenting, and controlling connections between system components.

(2) limiting external connections to the organisation's critical systems.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	Connections between system components and external connections to the organisation's critical systems are not identified or documented.
2	Connections between system components and external connections to the organisation's critical systems are identified and document in a controlled (version and approved) way, in the form of a network architecture diagram, for example; However, that documentation has not been reviewed in the past 2 years.
3	Connections between system components and external connections to the organisation's critical systems are identified and documented in a controlled (version and approved) way, in the form of a network architecture diagram, for example. Exceptions from the required level of detail regarding critical systems on the entity's network architecture diagram are documented and approved and are limited to less than 5% of the total number of critical systems identified.
4	Connections between system components and external connections to the organisation's critical systems are identified and documented in a controlled (version and approved) way, in the form of a network architecture diagram, for example. This documentation is reviewed and updated regularly. Exceptions from the required level of detail regarding critical systems on the entity's network architecture diagram are documented and approved and are limited to less than 3% of the total number of identified critical systems.
5	Connections between system components and external connections to the organisation's critical systems are identified and documented in a controlled (version and approved) way, in the form of a network architecture diagram, for example. This documentation is reviewed and updated regularly. There are no exceptions regarding the required level of detail regarding critical systems on the entity's network architecture diagram.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	The lack of documentation regarding connections between system components and external connections to the organisation's critical systems hampers the protection of network integrity of the organisation's critical systems.
2	Interrelated and interdependent connections are identified and controlled on an ad hoc basis without a corporate strategy. External connections to the critical systems are identified and limited on an ad hoc basis without a corporate strategy
3	Connections between system components and external connections to the organisation's critical systems are as documented in the relevant documentation, such as by means of a network architecture diagram. Reviews (e.g. audits) of what is present in the field show that inconsistencies with what is documented amount to less than 10%.
4	Connections between system components and external connections to the organisation's critical systems are as documented in the relevant documentation, such as by means of a network architecture diagram, and reviews (e.g. audits) of what is present 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 and to enable the assessment of network integrity. The degree of accuracy of the network visualisation and network integrity risks are reported as described in the applicable process documentation.

MATURITY	EVIDENCE TO BE CONSIDERED
5	Connections between system components and external connections to the organisation's critical systems are as documented in the relevant documentation, such as by means of a network architecture diagram, and reviews (e.g. audits) of what is present 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 and to enable the assessment of network integrity. The degree of accuracy of the network visualisation and network integrity risks are reported as described in the applicable process documentation. Any network integrity risks identified are translated into improvement opportunities that contribute towards the continuous improvement of network integrity.

PR.AC-5.4 The organisation shall monitor and control connections and communications at the external boundary and at key internal boundaries within the organisation's critical systems by implementing boundary protection devices where appropriate.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no controlled (version controlled and approved) documentation on the monitoring and control of connections and communications at (1) the external boundary and at (2) key internal boundaries within the organisation's critical systems.
2	Controlled (version controlled and approved) documentation (policy, process, SOP...) on the monitoring and controlling of connections and communications at (1) the external boundary and at (2) key internal boundaries within the organisation's critical systems exists but hasn't been reviewed in the previous 2 years.
3	Controlled (version controlled and approved) documentation (policy, process, SOP...) on the monitoring and control of critical external and internal connections and communications exists; the core critical network infrastructure configuration is documented and fully described. Limitations on the monitoring and control of external and internal connections and communications to the critical systems are defined and documented and regularly reviewed. For less than 5% of identified limitations, the description of these limitations can be confined to simply stating the main features.
4	Controlled (version controlled and approved) documentation (policy, process, SOP...) on the monitoring and control of critical external and internal connections and communications exists; the critical network infrastructure configuration is documented and fully described. Limitations on the monitoring and control of external and internal connections and communications to the critical systems are defined and documented, updated and regularly reviewed. For less than 3% of identified limitations, the description of these limitations can be confined to simply stating the main features. In line with this, the documentation reflects the critical network infrastructure configuration.
5	Controlled (version controlled and approved) documentation (policy, process, SOP...) on the monitoring and control of critical external and internal connections and communications exists; the network infrastructure configuration is documented and fully described. Limitations on the monitoring and control of external and internal connections and communications to the systems are defined and documented, updated and regularly reviewed. Documentation shows that the network infrastructure is fully described.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	Connections and communications at the external boundary and at key internal boundaries are not monitored or controlled.
2	Connections and communications at the external boundary and at key internal boundaries are monitored and controlled on an ad hoc basis without any underlying strategy.
3	Documentation (policy, process, SOP, architecture,...) on the monitoring and control of connections and communications at the external boundary and at key internal boundaries is implemented (incl. boundary protection devices where relevant). Evidence regarding process implementation is available for most activities. Reviews (e.g. audits) show that inconsistencies between what is documented and what is implemented in the field amount to less than 10%.
4	Documentation (policy, process, SOP, architecture, covered critical business areas...) on the monitoring and control of the critical external and internal connections and communications (incl. boundary protection devices where relevant) is implemented and measurable. Minimum targets for process performance have been established. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) show that inconsistencies between what is documented and what is implemented in the field amount to less than 5%. Status is reported as established in appropriate process documentation.
5	Documentation (policy, process, SOP, architecture, covered critical business areas...) on the monitoring and control of the critical external and internal connections and communications (incl. boundary protection devices where relevant) is implemented and measurable. Minimum targets for process performance have been established. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) show that inconsistencies between what is documented and what is implemented in the field amount to less than 1%. Status is reported as established in appropriate process documentation. Improvement initiatives are defined and have, for example, a zero-trust security framework as end-goal.

PR.DS-5.1 The organisation shall take appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorised access and activities, including data leakage, is detected.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	The process for taking appropriate actions when unauthorised access and activities are detected is not documented or not formally approved by management.
2	Controlled process documentation (version control, approved) exists that provide a framework for taking appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points whenever unauthorised access and activities, including data leakage are detected, but this documentation has not been reviewed in the past 2 years.
3	Controlled process documentation (version control, approved) exists to make sure that appropriate actions are taken whenever unauthorised access and activities, including data leakage, occur. Exceptions from the monitoring of its critical systems at external borders and critical internal points are documented, approved and limited to less than 5% of all of the organisation's critical systems at external borders and critical internal points.

MATURITY	EVIDENCE TO BE CONSIDERED
4	Controlled process documentation (version control, approved) exists to ensure that appropriate actions are taken whenever unauthorised access and activities, including data leakage, occur. Exceptions from the monitoring of its critical systems at external borders and critical internal points are documented, approved and limited to less than 3% of all of the organisation's critical systems at external borders and critical internal points.
5	Controlled process documentation (version control, approved) exists to ensure that appropriate actions are taken whenever unauthorised access and activities, including data leakage, occur. Exceptions from the monitoring of its critical systems at external borders and critical internal points are documented, approved and limited to less than 0.5% (which in practice means almost no exceptions) of all of the organisation's critical systems at external borders and critical internal points.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There are no usage restrictions, connection requirements, implementation guidance, and authorisations for remote access to the organisation's critical systems environment.
2	Usage restrictions, connection requirements, implementation guidance, and authorisations for remote access to the organisation's critical systems environment are implemented on an ad hoc basis and managed informally.
3	The organisation takes appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorised access and activities, including data leakage, is detected as documented in the relevant documentation. Evidence is available for most activities. Reviews (e.g. by means of audits) show that cases of unauthorised access and activities that are inconsistently handled in comparison with what is prescribed in the process documentation amount to less than 10%.
4	The organisation takes appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorised access and activities, including data leakage, is detected as documented in the relevant documentation. Evidence is available for all activities. Reviews (e.g. by means of audits) show that cases of unauthorised access and activities that are inconsistently handled in comparison with what is prescribed in the process documentation amount to less than 5%. Detailed metrics of the process, for which minimum targets for metrics have been established, are captured and reported.
5	The organisation takes appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorised access and activities, including data leakage, is detected as documented in the relevant documentation. Evidence is available for all activities. Reviews (e.g. by means of audits) show that cases of unauthorised access and activities that are inconsistently handled in comparison with what is prescribed in the process documentation amount to less than 1%. Detailed metrics of the process, for which minimum targets for metrics have been established, are captured, reported, and show continuous improvement in process performance.

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

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	The organisation has no process documentation, or documentation approved by management detailing how to establish and maintain a configuration baseline for its business-critical systems.
2	The organisation has a controlled process documentation (version controlled and approved) detailing how to establish and maintain a configuration baseline for its business-critical systems, but that documentation has not been reviewed in the past 2 years.
3	The organisation has a controlled process documentation (version controlled and approved) detailing how to establish and maintain a configuration baseline for its business-critical systems. For less than 5% of the business-critical systems, there is a documented and approved exception detailing why the configuration information does not exist or is incomplete (e.g. functional settings that determine how an asset operates, versions of software currently installed (BIOS, firmware, operating system, applications, etc.), or specifying patches (including security patches) that are installed, ports that are active for normal and emergency operations and how they are configured, and services that are enabled…).
4	The organisation has a controlled process documentation (version controlled and approved) detailing how to establish and maintain a configuration baseline for its business-critical systems. For less than 3% of the business-critical systems, there is a documented and approved exception detailing why the configuration information does not exist or is incomplete (e.g. functional settings that determine how an asset operates, versions of software currently installed (BIOS, firmware, operating system, applications, etc.), or specifying patches (including security patches) that are installed, ports that are active for normal and emergency operations and how they are configured, and services that are enabled…).
5	The organisation has a controlled process documentation (version controlled and approved) detailing how to establish and maintain a configuration baseline for its business-critical systems. For less than 0.5% (which for practical purposes amounts to no exceptions at all) of the business-critical systems, there is a documented and approved exception detailing why the configuration information does not exist or is incomplete.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No baseline configuration for the organisation's business-critical systems has been identified or maintained (e.g. functional settings that determine how an asset operates, versions of software currently installed (BIOS, firmware, operating system, applications, etc.), patches (including security patches) that are installed, ports that are active for normal and emergency operations and how they are configured, services that are enabled…).
2	The baseline configuration for the organisation's business-critical systems is identified and maintained on an ad hoc basis and managed informally.
3	The baseline configuration for the organisation's business-critical systems is identified and maintained (kept up to date). Evidence is available for most activities. Reviews (e.g. by means of audits) show that for less than 10% of the business-critical systems, the baseline configuration deviates from reality.
4	The baseline configuration for the organisation's business-critical systems is identified and maintained. Evidence is available for all activities. Reviews (e.g. by means of audits) show that for less than 5% of the business-critical systems, the baseline configuration deviates from reality. Detailed metrics of the process, for which minimum targets for metrics have been established, are captured and reported.
5	The baseline configuration for the organisation's business-critical systems is identified and maintained. Evidence is available for all activities. Reviews (e.g. by means of audits) show that for less than 1% of the business-critical systems, the baseline configuration deviates from reality. Detailed metrics of the process, for which minimum targets for metrics have been established, are captured, reported, and show continuous improvement in process performance.

PR.DS-4.1 Capacity planning shall ensure adequate resources for organisation's critical system information processing, networking, telecommunications, and data storage.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no controlled (version controlled and approved) documented capacity planning process to ensure adequate resources for the organisation's critical system information processing, networking, telecommunications, and data storage.
2	There is a controlled (version controlled and approved) documented capacity planning process that ensures adequate resources for the organisation's critical system information processing, networking, telecommunications, and data storage, however it has not been reviewed in the past 2 years.
3	There is a controlled (version controlled and approved) and documented capacity planning process that is regularly reviewed and updated and ensures adequate resources for the organisation's critical system information processing, networking, telecommunications, and data storage. Exceptions from capacity planning are allowed for less than 5% of the critical assets (system information processing, networking, telecommunications, data storage). This is documented and approved.
4	There is a controlled (version controlled and approved) and documented capacity planning process that is regularly reviewed and updated and ensures adequate resources for the organisation's critical system information processing, networking, telecommunications, and data storage. Exceptions from capacity planning are allowed for less than 3% of the critical assets (system information processing, networking, telecommunications, data storage). This is documented and approved.
5	There is a controlled (version controlled and approved and documented capacity planning process that is regularly reviewed and updated and ensures adequate resources for the organisation's critical system information processing, networking, telecommunications, and data storage. There are no exceptions concerning critical assets (system information processing, networking, telecommunications, data storage) for which capacity planning is not foreseen.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version checked and approved) capacity planning process has been created or implemented.
2	Capacity planning to ensure adequate resources for the organisation's critical system information processing, networking, telecommunications, and data storage is performed on an ad hoc and informal basis.
3	Capacity planning to ensure adequate resources for the organisation's critical system information processing, networking, telecommunications, and data storage is implemented as documented. Evidence on process implementation is available for most activities. Reviews (e.g. audits) show inconsistencies between documentation and reality in less than 10% of cases.
4	Capacity planning to ensure adequate resources for the organisation's critical system information processing, networking, telecommunications, and data storage is implemented as documented. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) show inconsistencies between planned capacity and real needs in less than 5% of cases. Metrics have been deployed and minimum targets on process performance identified. Process performance is reported as described in the applicable process documentation.
5	Capacity planning to ensure adequate resources for the organisation's critical system information processing, networking, telecommunications, and data storage is implemented as documented. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) reveal inconsistencies between planned capacity and real needs in less than 1% of cases. Identified inconsistencies lead to improvement actions that contribute towards continuous process improvement. Process performance is reported as described in the applicable process documentation.

PR.IP-9.1 Incident response plans (incident response and business continuity) and recovery plans (incident recovery and disaster recovery) shall be established, maintained, approved, and tested to determine the effectiveness of the plans, and the readiness to execute the plans.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There are no formal incident response plans (Incident Response and Business Continuity) or recovery plans (Incident Recovery and Disaster Recovery). If there were any (informal), they have not been approved by management.
2	The organisation has controlled (versioned and approved) incident response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery), however they have not been reviewed in the past 2 years.
3	Controlled (versioned and approved) incident response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) exist. Less than 5% of these plans are exempt from testing in order to determine the effectiveness of the plans, and the readiness to execute the plans. The reason for this is documented and approved by the management.

MATURITY	EVIDENCE TO BE CONSIDERED
4	Controlled (versioned and approved) incident response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) exist. Less than 3% of these plans are exempt from testing to determine the effectiveness of the plans, and the readiness to execute the plans. The reason for this is documented and approved by the management.
5	Controlled (versioned and approved) incident response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) exist. Less than 0.5% of these plans (which practically amounts to none) are exempt from testing to determine the effectiveness of the plans, and the readiness to execute the plans. The reason for this is documented and approved by the management.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no standard process to ensure that the organisation establishes, maintains and approves incident response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery). Nor is there a standard process to test these plans to determine the effectiveness of the plans, and the organisation's readiness to execute the plans.
2	A process is intuitively in place to ensure that the organisation creates, maintains and approves incident response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery). These plans are tested in an ad hoc way to determine the effectiveness of the plans and the organisation's readiness to implement the plans. Management of the process takes place outside a formal framework.
3	A formal process exists and has been implemented to establish, maintain, approve, and test incident response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery). Evidence is available for most response and recovery plan testing. Regular reviews (e.g. audits) show that it was not possible to determine the effectiveness of the plans, and the readiness to execute the plans in less than 10% of test events held during a predefined period.
4	A formal process exists and has been implemented to establish, maintain, approve, and test incident response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery). Evidence is available for all response and recovery plan testing. Regular reviews (e.g. audits) show that it was not possible to determine the effectiveness of the plans, and the readiness to execute the plans in less than 5% of test events held during a predefined period. Detailed process performance metrics (covering the complete response and recovery plan life cycle: establishment, maintenance, approval, and testing), including minimal process performance targets, are measured, and reported.
5	A formal process exists and has been implemented to establish, maintain, approve, and test incident response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery). Evidence is available for all response and recovery plan testing. Regular reviews (e.g. audits) show that it was not possible to determine the effectiveness of the plans, and the readiness to execute the plans in less than 1% of test events held during a predefined period. Detailed process performance metrics (covering the complete response and recovery plan life cycle: establishment, maintenance, approval, and testing), including minimal process performance targets, are measured, reported, and show continuous improvement.


WARNING!
SYSTEM WARNING

Maturity level use cases **DETECT**

Detect

Maturity level use cases ‘Detect’

DE.CM-1.2 The organisation shall monitor and identify unauthorised use of its business-critical systems through the detection of unauthorised local connections, network connections and remote connections.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version controlled and approved) documentation on monitoring and identifying the unauthorised use of business-critical systems through the detection of unauthorised local connections, network connections and remote connections exists.
2	A controlled (version controlled and approved) documentation (policy, process, SOP…) on monitoring and identifying the unauthorised use of business-critical systems through the detection of unauthorised local connections, network connections and remote connections exists, but has not been reviewed in the past 2 years.
3	A controlled (version controlled and approved) documentation (policy, process, SOP…) on monitoring and identifying the unauthorised use of business-critical systems through the detection of unauthorised local connections, network connections and remote connections exists and is regularly reviewed. Exceptions that apply to monitoring and identifying the unauthorised use of business-critical systems are documented, approved and are limited to less than 5% of the business-critical systems.
4	A controlled (version controlled and approved) documentation (policy, process, SOP…) on monitoring and identifying the unauthorised use of business-critical systems through the detection of unauthorised local connections, network connections and remote connections exists, is up to date and is regularly reviewed. Exceptions that apply to monitoring and identifying the unauthorised use of business-critical systems are documented, approved and are limited to less than 3% of the business-critical systems.
5	A controlled (version-controlled and approved) documentation (policy, process, SOP…) on monitoring and identifying the unauthorised use of business-critical systems through the detection of unauthorised local connections, network connections and remote connections exists for all business-critical systems, is up to date and is regularly reviewed. Any possible exceptions are kept to a strict minimum (less than 0.5% of the business-critical systems) and are documented and approved.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	The organisation neither monitors nor identifies the unauthorised use of its business-critical systems.
2	The organisation monitors and identifies the unauthorised use of its business-critical systems by detecting unauthorised local connections, network connections and remote connections on an ad hoc basis but without a supporting policy.
3	The organisation monitors and identifies the unauthorised use of its business-critical systems by detecting unauthorised local connections, network connections and remote connections as documented in policies, processes, SOPs etc.). Evidence regarding process implementation is available for most activities. Reviews (e.g. audits) show that inconsistencies between what is documented and what is implemented in the field amount to less than 10%.
4	The organisation monitors and identifies the unauthorised use of its business-critical systems by detecting unauthorised local connections, network connections and remote connections as documented in policies, processes, SOPs etc.). Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) show inconsistencies between what is documented and what is implemented in the field amount to less than 5%. Minimum process performance targets are established. Process performance is measured and reported.
5	The organisation performs the monitoring and identifying of unauthorised use of its business-critical systems by detecting unauthorised local connections, network connections and remote connections as documented in policies, processes, SOPs etc.). Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) show that inconsistencies between what is documented and what is implemented in the field amount to less than 1%. Minimum process performance targets are established. Process performance is measured, reported and is continually improving.

DE.DP-5.1 Improvements derived from the monitoring, measurement, assessment, testing, review, and lessons learned, shall be incorporated into detection process revisions.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no controlled (version controlled and approved) process documentation that provides that improvements derived from the monitoring, measurement, assessment, testing, review, and lessons learned will be incorporated into the detection process.
2	There is controlled (version controlled and approved) process documentation that provides that improvements derived from the monitoring, measurement, assessment, testing, review, and lessons learned will be incorporated into the detection process, but it has not been reviewed in the past 2 years.
3	There is controlled (version-controlled and approved) process documentation that provides that improvements derived from the monitoring, measurement, assessment, testing, review, and lessons learned will be incorporated into the detection process. The process does not consider all improvements that facilitate the continuous improvement of the detection process (test results, lessons learned… are not considered, for example). The reason for improvements being excluded is documented and approved.
4	There is controlled (version controlled and approved) process documentation that provides that improvements derived from the monitoring, measurement, assessment, testing, review, and lessons learned will be incorporated into the detection process. The process does not consider lessons learned as a source for improvements that are to be incorporated into revisions of the detection process. The reasoning for that is documented and approved.
5	There is controlled (version controlled and approved) process documentation that provides that improvements derived from the monitoring, measurement, assessment, testing, review, and lessons learned will be incorporated into the detection process. The documented process does consider all improvements derived from the monitoring, measurement, assessment, testing, review, and lessons learned.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no process that provides that improvements derived from the monitoring, measurement, assessment, testing, review, and lessons learned will be incorporated into the detection process.
2	The process that provides that improvements will be incorporated into the detection process is implemented on an ad hoc basis and is managed informally.
3	The process that provides that improvements will be incorporated into the detection process is implemented, including the documented exceptions. Evidence regarding process implementation is available for most improvements. Reviews (e.g. audits) of the implemented process show that inconsistencies between the identified improvements and what is incorporated into detection process revisions amount to less than 10%.
4	The process that provides that improvements derived from the monitoring, measurement, assessment, testing, review, and lessons learned will be incorporated into the detection process, is implemented and takes the documented exceptions into consideration. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) of the implemented process show that inconsistencies between the identified improvements and what is incorporated into detection process revisions amount to less than 5%. Metrics, including targets, are in place to monitor the implementation of the process. Process performance is reported as described in the applicable process documentation.
5	The process that provides that improvements derived from the monitoring, measurement, assessment, testing, review, and lessons learned will be incorporated into the detection process, is implemented and takes the documented exceptions into consideration. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) of the implemented process show that inconsistencies between the identified improvements and what is incorporated into detection process revisions amount to less than 1%. Metrics, including targets, are in place to monitor the implementation of the process. Process performance results are translated into process improvements. Process performance is reported as described in the applicable process documentation.

Maturity level use cases
RESPOND

Respond

Maturity level use cases ‘Respond’

RS.AN-5.1 The organisation shall implement vulnerability management processes and procedures that include processing, analysing and remedying vulnerabilities from internal and external sources.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version controlled and approved) documentation (e.g. policy, process…) on managing vulnerabilities, including processing, analysing and remedying vulnerabilities from internal and external sources, exists.
2	A policy or process to manage vulnerabilities, including processing, analysing and remedying vulnerabilities from internal and external sources, is formally documented (version controlled and approved) but not reviewed regularly (e.g. has not been reviewed in the past 2 years).
3	A policy or process to manage vulnerabilities is formally documented (version controlled and approved) and reviewed regularly. Exceptions (e.g. for reason of acceptable use or acceptable risk) are documented and approved and limited to a target of 5% of the assets in scope or as defined through a risk assessment.
4	A policy or process to manage and report vulnerabilities is formally documented (version controlled and approved) and reviewed regularly. Exceptions (e.g. for reason of acceptable use or acceptable risk) are documented and approved and limited to a target of 3% of the assets in scope or as defined through a risk assessment.
5	A policy or process to manage and report vulnerabilities is formally documented (version controlled and approved) and reviewed regularly. Exceptions (e.g. for reason of acceptable use or acceptable risk) are documented and approved and limited to a target of 0.5% of the assets in scope or as defined through a risk assessment.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No vulnerability management policy, including processing, analysing and remedying vulnerabilities from internal and external sources, or process is in place.
2	Vulnerability management is performed in an ad hoc way, without clear responsibilities and authorities.
3	The vulnerability management process is rolled out as documented. Evidence regarding process implementation is available for most activities. Reviews (e.g. audits) of the vulnerability management process show that the process is not followed (e.g. vulnerabilities identified but not remediated as prescribed in the vulnerability management process; information from internal and/or external sources is neglected) in less than 10% cases.
4	The vulnerability management process is rolled out as documented. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) of the vulnerability management 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 vulnerability management process (e.g. by implementing KPIs such as “time to detect”, “time to resolve”, “number of open high/critical patches…). Performance with regard to vulnerability management is reported as described in the vulnerability management process.
5	The vulnerability management process is rolled out as documented. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) of the vulnerability management 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 vulnerability management process (e.g. by implementing KPIs such as “time to detect”, “time to resolve”, “number of open high/critical patches…). Vulnerability management monitoring (e.g. by means of KPI analysis) is translated into opportunities for improvement. Performance with regard to vulnerability management is reported as described in the vulnerability management process.

RC.CO-3.1 The organisation shall communicate recovery activities to predefined stakeholders, executive and management teams.

Documentation Maturity

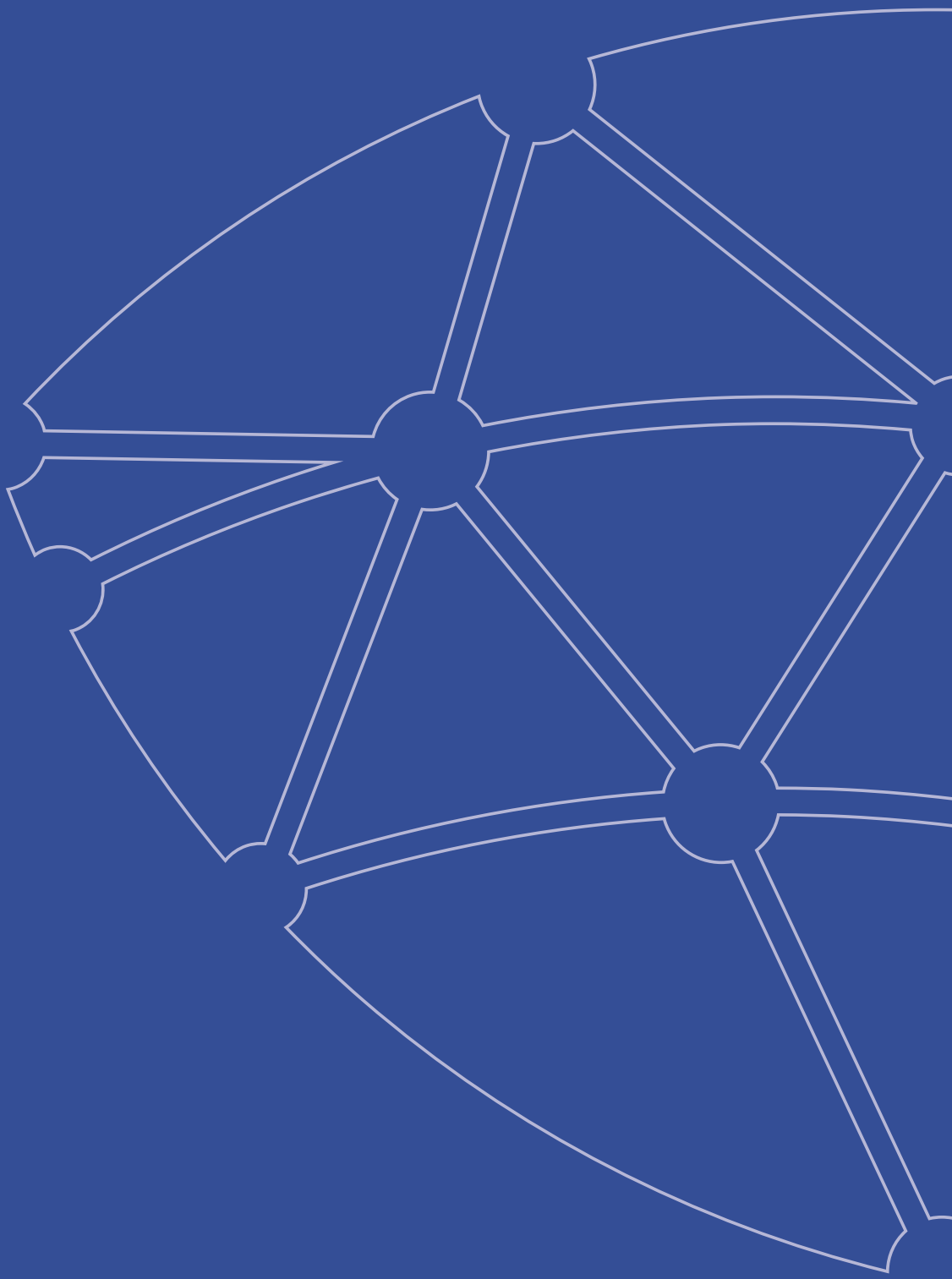
MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no controlled (version controlled and approved), documented process to ensure that recovery activities are communicated to predefined stakeholders, executive and management teams.
2	There is a controlled (version controlled and approved), documented process for the communication of recovery activities to predefined stakeholders, executive and management teams, however it has not been reviewed in the past 2 years.
3	There is a controlled (version controlled and approved), documented process, that is regularly reviewed and up to date, for the communication of recovery activities to predefined stakeholders, executive and management teams. There is no communication to all stakeholders, but there is a documented and approved reason for this.
4	There is a controlled (version controlled and approved), documented process, that is regularly reviewed and up to date, for the communication of recovery activities to predefined stakeholders, executive and management teams. Communications are made to all internal stakeholders. There is a documented and approved reason for not communicating to external stakeholders.
5	There is a controlled (version controlled and approved), documented process, that is regularly reviewed and up to date, for the communication of recovery activities to predefined stakeholders, executive and management teams. Communications are made to all (internal & external) stakeholders. There are no exceptions.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no communication of recovery activities to predefined stakeholders, executive and management teams.
2	The communication of recovery activities to predefined stakeholders, executive and management teams is performed on an ad hoc and informal basis.
3	The communication of recovery activities to predefined stakeholders, executive and management teams is 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, exercises) of the implemented process show that inconsistencies between what is documented and reality amount to less than 10%.
4	The communication of recovery activities to predefined stakeholders, executive and management teams 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, exercises) of the implemented process show that inconsistencies between what is documented and reality amount to less than 5%. Metrics, including targets, are in place to monitor the process. Process performance is reported as described in the applicable process documentation.
5	The communication of recovery activities to predefined stakeholders, executive and management teams 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, exercises) of the implemented process show that inconsistencies between what is documented and reality amount to less than 1%. 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.

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