CyFun®

ESSENTIAL

MATURITY LEVEL USE CASES

Version 2025-10-01

TABLE OF CONTENTS

MATURITY LEVEL USE CASES 'DETECT' 29

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).

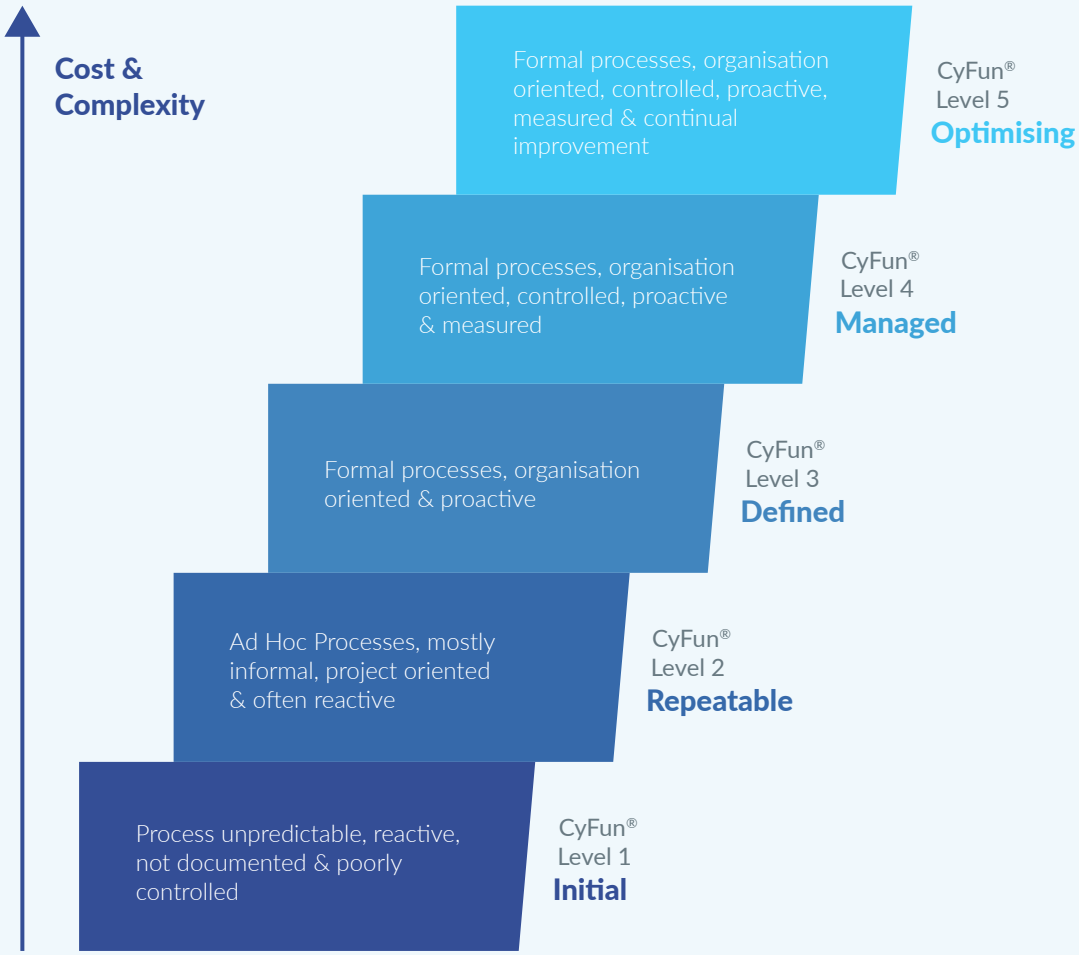


Figure: Overview of CyberFundamentals Maturity Levels

Maturity level use cases
IDENTIFY

Identify

Maturity level use cases ‘Identify’

ID.AM-6.2 The organisation shall appoint an information security officer.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	The function of information security officer does not exist.
2	The function of information security officer is identified on the formally approved organisation chart of the organisation but no job description exists.
3	A formally approved job description of an information security officer is available that includes the role and the responsibilities but lacks the authorities.
4	A formally approved job description of an information security officer is available that includes the role, the responsibilities and the authorities.
5	A formally approved job description of an information security officer is available with the role, the responsibilities and the authority, and explicitly identifies the position as a member of the organisation's executive committee.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No information security officer is appointed, and no such task is performed.
2	Informally, the CFO assumes the role of information security officer, but it is unclear what his/her duties are.
3	An information security officer is formally appointed but the job description shows that he/she does not have full authority to decide on information security. This has been confirmed during reviews (e.g. audits).
4	An information security officer is formally appointed, and the job description shows that he/she has full authority to decide on information security. This has been confirmed during reviews (e.g. audits) and is reported as described in the applicable process documentation.
5	An information security officer is formally appointed, and the job description shows that he/she has full authority to decide on information security. The function is part of the organisation's executive committee and participates in strategic information security discussions. This has been confirmed during reviews (e.g. audits) as described in the applicable process documentation. Findings during reviews (e.g. audits) regarding the implementation of the job description led to improvement opportunities that are pursued further.

ID.RA-5.3 Risk assessment results shall be disseminated to relevant stakeholders.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no process documentation or documentation formally approved by management that ensures that risk assessment results are disseminated to relevant stakeholders.
2	The organisation has controlled process documentation (versioned and approved) to ensure that risk assessment results are disseminated to relevant stakeholders, but that documentation has not been reviewed in the past 2 years.
3	Controlled (versioned, approved) process documentation exists to ensure that the risk assessment results are disseminated to relevant stakeholders, and that documentation is reviewed regularly. Of the total number of relevant stakeholders identified for the organisation (e.g. during a context analysis), no risk assessment results are distributed for less than 5%. The reason for this is documented and approved.
4	Controlled (versioned, approved) process documentation exists to ensure that the risk assessment results are disseminated to relevant stakeholders, and that documentation is reviewed regularly. Of the total number of relevant stakeholders identified for the organisation (e.g. during a context analysis), no risk assessment results are distributed for less than 3%. The reason for this is documented and approved.
5	Controlled (versioned, approved) process documentation exists to ensure that the risk assessment results are disseminated to relevant stakeholders, and that documentation is reviewed regularly. Of the total number of relevant stakeholders identified for the organisation (e.g. during a context analysis), no risk assessment results are distributed for less than 0.5% (which practically amounts to none). The reason for this is documented and approved.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no standard process to ensure that risk assessment results are disseminated to relevant stakeholders.
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 distribute risk assessment results to relevant stakeholders. Evidence is mostly available, taking into account the documented and approved exceptions. Reviews (e.g. audits) show that in less than 10% of cases, the risk assessment results are not disseminated where they should be.
4	A formal process exists and is implemented to distribute risk assessment results to relevant stakeholders. Evidence is always available, taking into account the documented and approved exceptions. Reviews (e.g. audits) show that in less than 5% of cases, the risk assessment results are not disseminated where they should be. Detailed process performance metrics, including minimum process performance targets, are measured and reported.
5	A formal process exists and is implemented to distribute risk assessment results to relevant stakeholders. Evidence is always available, taking into account the documented and approved exceptions. Reviews (e.g. audits) show that in less than 1% of cases, the risk assessment results are not disseminated where they should be. Detailed process performance metrics, including minimum process performance targets, are measured, reported and show continuous improvement.

ID.SC-1.1 The organisation shall document, review, approve, update when changes occur, and implement a cyber supply chain risk management process that supports the identification, assessment, and mitigation of the risks associated with the distributed and interconnected nature of ict/ot product and service supply chains.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no documentation or documentation formally approved by management (strategy, objectives, policies, and procedures) that supports the identification, assessment, and mitigation of the risks associated with the distributed and interconnected nature of ICT/OT product and service supply chains.
2	The organisation has controlled (versioned and approved) documentation (strategy, objectives, policies, and procedures) to ensure that risks associated with the distributed and interconnected nature of ICT/OT product and service supply chains are identified, assessed, and mitigated, but that documentation has not been reviewed in the past 2 years.
3	Controlled (versioned, approved) documentation (strategy, objectives, policies and procedures) exists to ensure that the organisation identifies, assesses, and mitigates cybersecurity supply chain risks. This documentation is reviewed regularly, approved, and updated whenever changes occur. No supply chain risk management plan exists for less than 5% of the organisation's critical mission and business functions. The reason for this has been documented and approved by the management.
4	Controlled (versioned, approved) documentation (strategy, objectives, policies, and procedures) exists to ensure that the organisation identifies, assesses, and mitigates cybersecurity supply chain risks. This documentation is reviewed regularly, approved, and updated whenever changes occur. No supply chain risk management plan exists for less than 3% of the organisation's critical mission and business functions. The reason for this has been documented and approved by the management.
5	Controlled (versioned, approved) documentation (strategy, objectives, policies, and procedures) exists to ensure that the organisation identifies, assesses, and mitigates cybersecurity supply chain risks. This documentation is reviewed regularly, approved, and updated whenever changes occur. A supply chain risk management plan exists for all the organisation's critical mission and business functions.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no standard process to ensure that the organisation documents, reviews, and approves updates whenever changes occur, and implements a cyber supply chain risk management process supporting the identification, assessment, and mitigation of the risks associated with the distributed and interconnected nature of ICT/OT product and service supply chains.
2	Supply chain risk management plans are intuitively created and implemented without a formal framework.
3	A formal cyber supply chain risk management process exists and is implemented to ensure that the organisation identifies, assesses, and mitigates cybersecurity supply chain risks, taking into account the documented and approved exceptions (namely the absence of supply chain risk management plans for critical mission and business functions). Evidence is available for most cybersecurity supply chain risks. Assessments show, for less than 10% of the sample used during an assessment, that the identified risk response actions for a specific supply chain cybersecurity risk cannot be shown to adequately mitigate the cybersecurity risk.

MATURITY	EVIDENCE TO BE CONSIDERED
4	A formal cyber supply chain risk management process exists and is implemented to ensure that the organisation identifies, assesses, and mitigates cybersecurity supply chain risks, taking into account the documented and approved exceptions (namely the absence of supply chain risk management plans for critical mission and business functions). Evidence is available for all cybersecurity supply chain risks. Assessments show, for less than 5% of the sample used during an assessment, that the identified risk response actions for a specific supply chain cybersecurity risk cannot be shown to adequately mitigate the cybersecurity risk. Detailed process performance metrics, including minimum process performance targets, are measured and reported.
5	A formal cyber supply chain risk management process exists and is implemented to ensure that the organisation identifies, assesses, and mitigates cybersecurity supply chain risks, taking into account the documented and approved exceptions (namely the absence of supply chain risk management plans for critical mission and business functions). Evidence is available for all cybersecurity supply chain risks. Assessments show, for less than 1% of the sample used during an assessment, that the identified risk response actions for a specific supply chain cybersecurity risk cannot be shown to adequately mitigate the cybersecurity risk. Detailed process performance metrics, including minimum process performance targets, are measured, and reported and show continuous improvement.

ID.SC-3.2 Contractual 'information security and cybersecurity' requirements for suppliers and third-party partners shall be implemented to ensure a verifiable flaw remediation process, and to ensure the correction of flaws identified during 'information security and cybersecurity' testing and evaluation.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no process documentation or documentation formally approved by management to ensure that contractual 'information security and cybersecurity' requirements for suppliers and third-party partners are implemented.
2	The controlled (version control, approved) process documentation to ensure that contractual 'information security and cybersecurity' requirements for suppliers and third-party partners are implemented exists but has not been reviewed in the past 2 years.
3	Controlled (version control, approved) process documentation to ensure that contractual 'information security and cybersecurity' requirements for suppliers and third-party partners are implemented exists and is regularly reviewed. These requirements guarantee that a verifiable flaw remediation process is in place and that flaws identified during 'information security and cybersecurity' testing and evaluation are corrected. The suppliers and third-party partners concerned are identified and exceptions from the implementation of these contractual requirements are documented, approved and limited to less than 5% of the total number of suppliers and third-party partners concerned.
4	Controlled (version control, approved) process documentation to ensure that contractual 'information security and cybersecurity' requirements for suppliers and third-party partners are implemented exists and is regularly reviewed. These requirements guarantee that a verifiable flaw remediation process is in place and that flaws identified during 'information security and cybersecurity' testing and evaluation are corrected. The suppliers and third-party partners concerned are identified and exceptions from the implementation of these contractual requirements are documented, approved and limited to less than 3% of the total number of suppliers and third-party partners concerned.
5	Controlled (version control, approved) process documentation to ensure that contractual 'information security and cybersecurity' requirements for suppliers and third-party partners are implemented exists and is regularly reviewed. These requirements guarantee that a verifiable flaw remediation process is in place and that flaws identified during 'information security and cybersecurity' testing and evaluation are corrected. The suppliers and third-party partners concerned are identified and exceptions from the implementation of these contractual requirements are documented, approved and limited to less than 0.5% (which practically amounts to none) of the total number of suppliers and third-party partners concerned.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no standard process to ensure that contractual 'information security and cybersecurity' requirements for suppliers and third-party partners are implemented.
2	Contractual 'information security and cybersecurity' requirements for suppliers and third-party partners are implemented in an ad hoc way and are managed informally.
3	A formal process to implement contractual 'information security and cybersecurity' requirements for suppliers and third-party partners exists and has been implemented. Evidence is available for most suppliers and third-party partners. Regular reviews (e.g. audits) show that inconsistencies between what is documented, including the exceptions, and what is implemented amount to less than 10%.

MATURITY	EVIDENCE TO BE CONSIDERED
4	A formal process to implement contractual 'information security and cybersecurity' requirements for suppliers and third-party partners exists and has been implemented. Evidence is available for all suppliers and third-party partners. Regular reviews (e.g. audits) show that inconsistencies between what is documented, including the exceptions, and what is implemented amount to less than 5%. Detailed process performance metrics, including minimum process performance targets, are measured and reported.
5	A formal process to implement contractual 'information security and cybersecurity' requirements for suppliers and third-party partners exists and has been implemented. Evidence is available for all suppliers and third-party partners. Regular reviews (e.g. audits) show that inconsistencies between what is documented, including the exceptions, and what is implemented amount to less than 1%. Detailed process performance metrics, including minimum process performance targets, are measured, reported and show continuous improvement.

ID.SC-3.3 The organisation shall establish contractual requirements permitting the organisation to review the 'information security and cybersecurity' programmes implemented by suppliers and third-party partners.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no process documentation or documentation formally approved by management to ensure that contractual requirements that allow the organisation to assess "information security and cybersecurity" programmes implemented by suppliers and external partners.
2	The controlled (version control, approved) process documentation to ensure that contractual requirements that allow the organisation to assess "information security and cybersecurity" programmes implemented by suppliers and external partners exists, but has not been reviewed in the past 2 years.
3	Controlled (version control, approved) process documentation to ensure that contractual requirements that allow the organisation to assess "information security and cybersecurity" programmes implemented by suppliers and external partners exists and is regularly reviewed. The suppliers and third-party partners concerned are identified and exceptions from the implementation of these contractual requirements are documented, approved and limited to less than 5% of the total number of the suppliers and third-party partners concerned.
4	Controlled (version control, approved) process documentation to ensure that contractual requirements that allow the organisation to assess "information security and cybersecurity" programmes implemented by suppliers and external partners exists and is regularly reviewed. The suppliers and third-party partners concerned are identified and exceptions from the implementation of these contractual requirements are documented, approved and limited to less than 3% of the total number of the suppliers and third-party partners concerned.
5	Controlled (version control, approved) process documentation ensuring that contractual requirements that allow the organisation to assess "information security and cybersecurity" programmes implemented by suppliers and external partners exists and is regularly reviewed. The suppliers and third-party partners concerned are identified and exceptions from the implementation of these contractual requirements are documented, approved and limited to less than 0.5% (which practically amounts to none) of the total number of the suppliers and third-party partners concerned.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no standard process to ensure that requirements that allow the organisation to assess "information security and cybersecurity" programmes implemented by suppliers and external partners are included in contracts with those suppliers and external partners.
2	Contractual requirements that allow the organisation to assess "information security and cybersecurity" programmes implemented by suppliers and external partners are implemented in an ad hoc way and are managed informally.
3	A formal process to implement contractual requirements that allow the organisation to assess "information security and cybersecurity" programmes implemented by suppliers and external partners exist and has been implemented. Evidence is available for most suppliers and third-party partners. Regular reviews (e.g. audits) show that inconsistencies between what is documented, including the exceptions, and what is implemented amount to less than 10%.
4	A formal process to implement contractual requirements that allow the organisation to assess "information security and cybersecurity" programmes implemented by suppliers and external partners exist and has been implemented. Evidence is available for all suppliers and third-party partners. Regular reviews (e.g. audits) show that inconsistencies between what is documented, including the exceptions, and what is implemented amount to less than 5%. Detailed process performance metrics, including minimum process performance targets, are measured and reported.
5	A formal process to implement contractual requirements that allow the organisation to assess "information security and cybersecurity" programmes implemented by suppliers and external partners exist and has been implemented. Evidence is available for all suppliers and third-party partners. Regular reviews (e.g. audits) show that inconsistencies between what is documented, including the exceptions, and what is implemented amount to less than 1%. Detailed process performance metrics, including minimum 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-7.1 The organisation shall perform a documented risk assessment on its critical system transactions and authenticate users, devices, and other assets commensurate with the risk of the transaction.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There are no controlled (version controlled and approved) risk assessments, or related process documentation, concerning business-critical system transactions and the verification of users, devices and other assets in proportion to the risk of the transaction.
2	Controlled (version controlled and approved) risk assessments, and related process documentation concerning business-critical system transactions and the verification of users, devices and other assets in proportion to the risk of the transaction are available, but have not been reviewed in the past 2 years.
3	The organisation is able to provide regularly reviewed, documented risk assessments, supported by related process documentation, for critical system transactions. There is no documented risk assessment for less than 5% of critical system transactions. The reason for this is documented, approved and proportionate to the risk of the transaction.
4	The organisation is able to provide regularly reviewed, documented risk assessments, supported by related process documentation, for critical system transactions. There is no documented risk assessment for less than 3% of critical system transactions. The reason for this is documented, approved and proportionate to the risk of the transaction.
5	The organisation is able to provide regularly reviewed, documented risk assessments, supported by related process documentation, for nearly all critical system transactions. There is no documented risk assessment for less than 0.5% of critical system transactions. The reason for this is documented, approved and proportionate to the risk of the transaction.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No risk assessments for business-critical system transactions and the verification of users, devices and other assets, are performed, nor is there a process that would mandate this.
2	Risk assessments for business-critical system transactions and the verification of users, devices and other assets are conducted in an ad hoc way without a well-defined strategy.
3	Documentation (policy, process, SOP,...) on the performance of risk assessments is implemented and results in risk assessments concerning business-critical system transactions and the verification of users, devices and other assets. 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,...) on the performance of risk assessments is implemented and results in risk assessments concerning business-critical system transactions and the verification of users, devices and other assets (e.g. single factor, multi-factor). Risk mitigation is proportional to the risk of the transaction and covers different risk categories. 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%. Minimum process performance targets are established. Process performance is measured and reported.
5	Documentation (policy, process, SOP,...) on the performance of risk assessments is implemented and results in risk assessments concerning business-critical system transactions and the verification of users, devices and other assets (e.g. single factor, multi-factor). Risk mitigation is proportional to the risk of the transaction and covers different risk categories. 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 continually improving.

PR.IP-9.2 The organisation shall coordinate the development and the testing of incident response plans and recovery plans with stakeholders responsible for related 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 (informally), 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), but they have not been reviewed in the past 2 years.
3	Controlled (versioned, 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 to determine the effectiveness of the plans, and the readiness to execute the plans. The reason for that is documented and has been approved by the management.
4	Controlled (versioned, 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 that is documented and has been approved by the management.
5	Controlled (versioned, approved) incident response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) exists. 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 that is documented and has been 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 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 readiness to implement the plans. Management of the process takes place outside a formal framework.
3	A formal process exists and is 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 in less than 10% of test events during a predefined period, it is not possible to determine the effectiveness of the plans or the readiness to execute the plans.
4	A formal process exists and is 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 in less than 5% of test events during a predefined period, it is not possible to determine the effectiveness of the plans, or the readiness to execute the plans. Detailed process performance metrics (covering the complete response and recovery plan life cycle: establishment, maintenance, approval, and testing) that include minimum process performance targets, are measured, and reported.

MATURITY	EVIDENCE TO BE CONSIDERED
5	A formal process exists and is 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 in less than 1% of test events during a predefined period, it is not possible to determine the effectiveness of the plans or the readiness to execute the plans. Detailed process performance metrics (covering the complete response and recovery plan life cycle: establishment, maintenance, approval, and testing), including minimum process performance targets, are measured, reported, and show continuous improvement.

PR.MA-1.5 The organisation shall prevent the unauthorised removal of maintenance equipment containing critical system information relating to the organisation.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version controlled and approved) documentation on preventing the unauthorised removal of maintenance equipment containing critical system information exists.
2	Controlled (version and approved) documentation (policy, process, SOP...) on preventing the unauthorised removal of maintenance equipment containing critical system information is available but has not been reviewed in the past 2 years.
3	Controlled (version and approved) documentation (policy, process, SOP...) on preventing the unauthorised removal of maintenance equipment containing critical system information is available and regularly reviewed. Controlled (version and approved) documentation (policy, process, SOP...) detailing situations in which maintenance equipment containing critical system information may be removed without prior authorisation is limited to less than 5% of identified cases.
4	Controlled (version and approved) documentation (policy, process, SOP...) on preventing the unauthorised removal of maintenance equipment containing critical system information is available and regularly reviewed. Controlled (version and approved) documentation (policy, process, SOP...) detailing situations in which maintenance equipment containing critical system information may be removed without prior authorisation is limited to less than 3% of identified cases.
5	Controlled (version and approved) documentation (policy, process, SOP...) on preventing the unauthorised removal of maintenance equipment containing critical system information is available and regularly reviewed. There are no situations in which maintenance equipment containing critical system information may be removed without prior authorisation.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	The unauthorised removal of maintenance equipment containing organisation's critical system information is not prevented.
2	The unauthorised removal of maintenance equipment containing organisation's critical system information is prevented informally and on an ad hoc basis. The practices are not covered by a standard organisation-wide policy.

MATURITY	EVIDENCE TO BE CONSIDERED
3	A formal process for preventing the unauthorised removal of maintenance equipment containing critical system information is present and implemented. Evidence is available for most activities. Regular 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 unauthorised removal of maintenance equipment containing organisation's critical system information is prevented formally by implementing the respective process. Evidence is available for all activities. Regular reviews (e.g. audits) show that 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 unauthorised removal of maintenance equipment containing organisation's critical system information is prevented formally by implementing the respective process. Evidence is available for all activities. Regular 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 shows continuous improvement.

PR.MA-1.6 Maintenance tools and portable storage devices shall be inspected when brought into the facility and shall be protected by anti-malware solutions so that they are scanned for malicious code before they are used on the organisation's systems.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no process documentation or documentation formally approved by management to ensure that maintenance tools and portable storage devices are inspected when they enter the facility and are protected by anti-malware solutions so that they are scanned for malicious code before being used on the organisation's systems.
2	Controlled (versioned, approved) process documentation to ensure that maintenance tools and portable storage devices are inspected as they enter the facility and are protected by anti-malware solutions so that they are scanned for malicious code before being used on the organisation's systems exists, but has not been reviewed in the past 2 years.
3	Controlled (versioned, approved) process documentation exists to ensure that maintenance tools and portable storage media are inspected as they enter the facility and are protected by anti-malware solutions so that they are scanned for malicious code before being used on the organisation's systems, and that documentation is reviewed regularly. Maintenance tools and portable storage media entering the organisation are logged to enable exceptions to be identified, documented, approved and limited to less than 5% of the total number of maintenance tools and portable storage media entering the organisation during a predefined period.
4	Controlled (versioned, approved) process documentation exists to ensure that maintenance tools and portable storage media are inspected as they enter the facility and protected by anti-malware solutions so that they are scanned for malicious code before being used on the organisation's systems, and that documentation is reviewed regularly. Maintenance tools and portable storage media entering the organisation are logged to enable exceptions to be identified, documented, approved and limited to less than 3% of the total number of maintenance tools and portable storage media entering the organisation during a predefined period.

MATURITY	EVIDENCE TO BE CONSIDERED
5	Controlled (versioned, approved) process documentation exists to ensure that maintenance tools and portable storage media are inspected as they enter the facility and are protected by anti-malware solutions so that they are scanned for malicious code before being used on the organisation's systems, and that documentation is reviewed regularly. Maintenance tools and portable storage media entering the organisation are logged to enable exceptions to be identified, documented, approved and limited to less than 0.5% (which practically amounts to none) of the total number of maintenance tools and portable storage media entering the organisation during a predefined period.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no standard process to ensure that maintenance tools and portable storage devices are inspected when they enter the facility and are protected by anti-malware solutions so that they are scanned for malicious code before being used on the organisation's systems.
2	Maintenance tools and portable storage devices are inspected in an ad hoc way when they enter the facility and are protected in an ad hoc way by anti-malware solutions so that they are scanned for malicious code before being used on the organisation's systems. All of this is managed informally.
3	A formal process to inspect maintenance tools and portable storage devices when they enter the facility and make sure that they are protected by anti-malware solutions so that they are scanned for malicious code before being used on the organisation's systems exists and is implemented. Evidence is available for most maintenance tools and portable storage devices that enter the organisation during a predefined period. Regular reviews (e.g. audits) show that inconsistencies between what is documented, including the exceptions, and what is implemented amount to less than 10%.
4	A formal process to inspect maintenance tools and portable storage devices when they enter the facility and make sure that they are protected by anti-malware solutions so that they are scanned for malicious code before being used on the organisation's systems exists and is implemented. Evidence is available for all maintenance tools and portable storage devices that enter the organisation during a predefined period. Regular reviews (e.g. audits) show less than 5% inconsistencies between what is documented, including the exceptions, and what is implemented. Detailed process performance metrics, including minimum process performance targets, are measured and reported.
5	A formal process to inspect maintenance tools and portable storage devices when they enter the facility and make sure that they are protected by anti-malware solutions so that they are scanned for malicious code before being used on the organisation's systems exists and is implemented. Evidence is available for all maintenance tools and portable storage devices that enter the organisation over a predefined period. Regular reviews (e.g. audits) show inconsistencies between what is documented, including the exceptions, and what is implemented amount to less than 1%. Detailed process performance metrics, including minimum process performance targets, are measured, reported and show continuous improvement.

PR.MA-1.7 The organisation shall verify security controls following hardware and software maintenance or repairs/patching and take action as appropriate.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no process documentation or documentation formally approved by management to ensure that security checks are carried out after hardware and software maintenance or repairs/patching and appropriate actions are taken as a consequence.
2	Controlled (versioned, approved) process documentation exists to ensure that security checks are carried out after hardware and software maintenance or repairs/patching and that the required actions are taken as a consequence, but has not been reviewed in the past 2 years.

MATURITY	EVIDENCE TO BE CONSIDERED
3	Controlled (versioned, approved) process documentation exists to ensure that security checks are carried out after hardware and software maintenance or repairs/patching and that the required actions are taken as a consequence, and that documentation is reviewed regularly. Hardware and software maintenance or repairs/patching are logged to enable exceptions to be identified, documented, approved and limited to less than 5% of the total number of instances of hardware and software maintenance or repairs/patching over a predefined period.
4	Controlled (versioned, approved) process documentation exists to ensure that security checks are carried out after hardware and software maintenance or repairs/patching and that the required actions are taken as a consequence, and that documentation is reviewed regularly. Hardware and software maintenance or repairs/patching are logged to enable exceptions to be identified, documented, approved and limited to less than 3% of the total number of instances of hardware and software maintenance or repairs/patching during a predefined period.
5	Controlled (versioned, approved) process documentation exists to ensure that security checks are carried out after hardware and software maintenance or repairs/patching and that the required actions are taken as a consequence, and that documentation is reviewed regularly. Hardware and software maintenance or repairs/patching are logged to enable exceptions to be identified, documented, approved and limited to less than 0.5% (which practically amounts to none) of the total number of instances of hardware and software maintenance or repairs/patching during a predefined period.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no standard process to ensure that security checks are carried out after hardware and software maintenance and repairs/patching and that appropriate actions are taken as a consequence.
2	Security checks are carried out on an ad hoc basis after hardware and software maintenance and repairs/patching and appropriate actions are taken in an ad hoc way. This entire process is managed informally.
3	A formal process exists and is implemented to carry out security checks after hardware and software maintenance or repairs/patching and appropriate actions are taken as a result of those checks. Evidence is available for most hardware and software maintenance and repairs/patching over a predefined period. Regular reviews (e.g. audits) show that inconsistencies between what is documented, including the exceptions, and what is implemented account for less than 10%.
4	A formal process exists and is implemented to carry out security checks after hardware and software maintenance or repairs/patching and appropriate actions are taken as a result of those checks. Evidence is available for all hardware and software maintenance and repairs/patching during a predefined period. Regular reviews (e.g. audits) show that inconsistencies between what is documented, including the exceptions, and what is implemented amount to less than 5%. Detailed process performance metrics, including minimum process performance targets, are measured and reported.
5	A formal process exists and is implemented to carry out security checks after hardware and software maintenance or repairs/patching and appropriate actions are taken as a result of those checks. Evidence is available for all hardware and software maintenance and repairs/patching during a predefined period. Regular reviews (e.g. audits) show that inconsistencies between what is documented, including the exceptions, and what is implemented amount to less than 1%. Detailed process performance metrics, including minimum process performance targets, are measured, reported and show continuous improvement.

PR.PT-2.3 Portable storage devices containing system data shall be controlled and protected while in transit and in storage.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no process documentation or documentation formally approved by management to ensure that portable storage devices containing system data are controlled and protected while in transit or in storage.
2	Controlled (versioned, approved) process documentation to ensure that portable storage devices containing system data are controlled and protected while in transit or in storage exists, but has not been reviewed in the past 2 years.
3	Controlled (versioned, approved) process documentation to ensure that portable storage devices containing system data are controlled and protected while in transit or in storage exists, and that documentation is reviewed regularly. Portable storage devices containing system data that are in transit or in storage are known and exceptions relating to their protection are documented, approved and limited to less than 5% of the total number of portable storage devices containing system data that are in transit or in storage during a predefined period.
4	Controlled (versioned, approved) process documentation to ensure that portable storage devices containing system data are controlled and protected while in transit or in storage exists, and that documentation is reviewed regularly. Portable storage devices containing system data that are in transit or in storage are known and exceptions relating to their protection are documented, approved and limited to less than 3% of the total number of portable storage devices containing system data that are in transit or in storage during a predefined period.
5	Controlled (versioned, approved) process documentation ensuring that portable storage devices containing system data are controlled and protected while in transit or in storage exists, and that documentation is reviewed regularly. Portable storage devices containing system data that are in transit or in storage are known and exceptions relating to their protection are documented, approved and limited to less than 0.5% (which practically amounts to none) of the total number of portable storage devices containing system data that are in transit or in storage during a predefined period.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no documentation or documentation formally approved by management (strategy, objectives, policies or procedures) that supports the coordination of development and testing of incident response plans and recovery plans with stakeholders responsible for related plans.
2	The organisation has controlled (versioned and approved) documentation (strategy, objectives, policies, and procedures) to coordinate the development and the testing of incident response plans and recovery plans with stakeholders responsible for related plans, but that documentation has not been reviewed in the past 2 years.
3	Controlled (versioned, approved) documentation exists to ensure the coordination of development and testing of incident response plans and recovery plans with stakeholders responsible for related plans. In situations where it is not possible to carry out that coordination, this is documented and approved and is limited to less than 5% of all active incident response plans and recovery plans in which stakeholders have the responsibility for related plans.

MATURITY	EVIDENCE TO BE CONSIDERED
4	Controlled (versioned, approved) documentation exists to ensure the coordination of development and testing of incident response plans and recovery plans with stakeholders responsible for related plans. In situations where it is not possible to carry out that coordination, this is documented and approved and is limited to less than 3% of all active incident response plans and recovery plans in which stakeholders have the responsibility for related plans.
5	Controlled (versioned, approved) documentation exists to ensure the coordination of development and testing of incident response plans and recovery plans with stakeholders responsible for related plans. In situations where it is not possible to carry out that coordination, this is documented and approved and is limited to less than 0.5% (which practically amounts to none) of all active incident response plans and recovery plans in which stakeholders have the responsibility for related plans.


WARNING!
SYSTEM WARNING

Maturity level use cases

DETECT

Detect

Maturity level use cases ‘Detect’

DE.AE-1.1 The organisation shall ensure that a baseline of network operations and expected data flows for its critical systems is developed, documented and maintained to track events.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no process documentation or documentation formally approved by management to ensure that a baseline of network operations and expected data flows for the critical systems is developed, documented and maintained to track events.
2	Controlled (versioned, approved) process documentation to ensure that a baseline of network operations and expected data flows for the critical systems is developed, documented and maintained to track events exists, but has not been reviewed in the past 2 years.
3	Controlled (versioned, approved) process documentation to ensure that a baseline of network operations and expected data flows for the critical systems is developed, documented and maintained to track events exists, and that documentation is reviewed regularly. For less than 5% of the critical systems, exceptions with regard to the baseline (development, depth of documentation and maintenance) are allowed, documented and approved.
4	Controlled (versioned, approved) process documentation to ensure that a baseline of network operations and expected data flows for the critical systems is developed, documented and maintained to track events exists, and that documentation is reviewed regularly. For less than 3% of the critical systems exceptions with regard to the baseline (development, depth of documentation and maintenance) are allowed, documented and approved.
5	Controlled (versioned, approved) process documentation to ensure that a baseline of network operations and expected data flows for the critical systems is developed, documented and maintained to track events exists, and that documentation is reviewed regularly. For less than 0.5% of the critical systems (which practically amounts to no exceptions at all), exceptions with regard to the baseline (development, depth of documentation and maintenance) are allowed, documented and approved.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no standard process to ensure that a baseline of network operations and expected data flows for the critical systems is developed, documented and maintained to track events.
2	There is an ad hoc process to develop, document and maintain a baseline of network operations and expected data flows for the critical systems. Events are tracked informally.
3	A formal process exists and is implemented to develop, document and maintain a baseline of network operations and expected data flows for the critical systems so that events can be tracked. Evidence is available for most critical systems. Regular reviews (e.g. audits) show that less than 10% of events during a predefined period cannot be tracked because of inconsistent baselines (e.g. incomplete logging or logs that contain insufficient information).
4	A formal process exists and is implemented to develop, document and maintain a baseline of network operations and expected data flows for the critical systems so that events can be tracked. Evidence is available for all critical systems. Regular reviews (e.g. audits) show that less than 5% of events during a predefined period cannot be tracked because of inconsistent baselines (e.g. incomplete logging, or logs that contain insufficient information). Detailed process performance metrics, including minimum process performance targets, are measured and reported.
5	A formal process exists and is implemented to develop, document and maintain a baseline of network operations and expected data flows for the critical systems so that events can be tracked. Evidence is available for all critical systems. Regular reviews (e.g. audits) show that less than 1% of events during a predefined period cannot be tracked because of inconsistent baselines (e.g. incomplete logging, or logs that contain insufficient information). Detailed process performance metrics, including minimum process performance targets, are measured and reported and show continuous improvement.

DE.AE-4.1 Negative impacts on the organisation's operations, assets, and individuals resulting from detected events shall be determined and correlated with risk assessment outcomes.

Documentation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	There is no controlled (version controlled and approved), documented process to ensure that negative impacts on the organisation's operations, assets, and individuals that are the result of detected events are determined and correlated with risk assessment outcomes.
2	There is a controlled (version controlled and approved), documented process to ensure that negative impacts on the organisation's operations, assets, and individuals that are the result of detected events are determined and correlated with risk assessment outcomes. However, it has not been reviewed in the past 2 years.
3	There is a controlled (version controlled and approved), documented process to ensure that negative impacts on the organisation's operations, assets, and individuals that are the result of detected events are determined and correlated with risk assessment outcomes. The process does allow exceptions that specify what negative impacts of detected events do not have to be determined and therefore do not have to be correlated with risk assessment outcomes. These exceptions are documented and approved.
4	There is a controlled (version controlled and approved), documented process to ensure that negative impacts on the organisation's operations, assets, and individuals that are the result of detected events are determined and correlated with risk assessment outcomes. The process does allow exceptions that specify what negative impacts do not have to be determined and therefore not have to be correlated with risk assessment outcomes. These exceptions are risk-based, documented and approved.
5	There is a controlled (version controlled and approved), documented process to ensure that negative impacts on the organisation's operations, assets, and individuals that are the result of detected events are determined and correlated with risk assessment outcomes. The process does not allow any exceptions.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	Negative impacts on the organisation's operations, assets, and individuals that are the result of detected events are not determined and therefore not correlated with risk assessment outcomes.
2	Negative impacts on the organisation's operations, assets, and individuals that are the result of detected events are determined and correlated with risk assessment outcomes on an ad hoc basis and are managed informally.
3	Negative impacts on the organisation's operations, assets, and individuals that are the result of detected events are determined and correlated with risk assessment outcomes 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 reveal that inconsistencies between what is documented and reality amount to less than 10%.

MATURITY	EVIDENCE TO BE CONSIDERED
4	Negative impacts on the organisation's operations, assets, and individuals that are the result of detected events are determined and correlated with risk assessment outcomes as specified in the relevant process documentation, including the documented exceptions. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) of the implemented process reveal 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	Negative impacts on the organisation's operations, assets, and individuals that are the result of detected events are determined and correlated with risk assessment outcomes as specified in the relevant process documentation. Evidence regarding process implementation is available for all activities. Reviews (e.g. audits) of the implemented process reveal 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.

DE.DP-5.2 The organisation shall conduct specialised assessments including in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, performance/load testing, and verification and validation testing of the organisation's critical systems.

Documentation Maturity

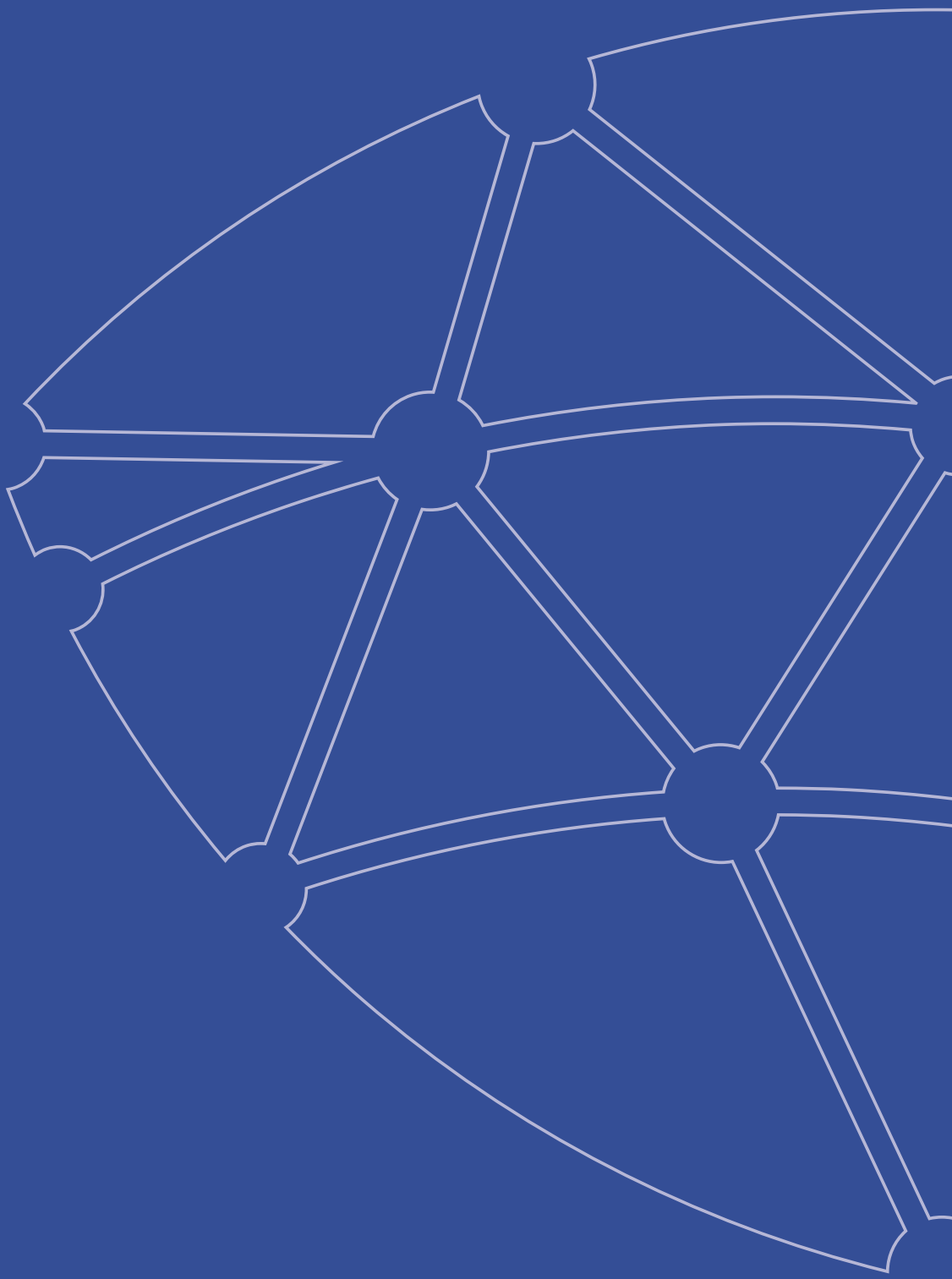
MATURITY	EVIDENCE TO BE CONSIDERED
1	No controlled (version controlled and approved) documentation concerning the performance of specialised assessments on the organisation's critical systems exists.
2	Controlled (version and approved) documentation (policy, process, SOP...) concerning the performance of specialised assessments on the organisation's critical systems is available but has not been reviewed in the past 2 years.
3	Controlled (version and approved) documentation concerning the performance of specialised assessments on the organisation's critical systems is available and regularly reviewed. Exceptions relating to the performance of specialised assessments on the organisation's critical systems are documented, approved and limited to less than 5% of the total number of critical systems identified.
4	Controlled (version and approved) documentation concerning the performance of specialised assessments on the organisation's critical systems is available and regularly reviewed. Exceptions relating to the performance of specialised assessments on the organisation's critical systems are documented, approved and limited to less than 3% of the total number of critical systems identified.
5	Controlled (version and approved) documentation concerning the performance of specialised assessments on the organisation's critical systems is available and regularly reviewed. There are no exceptions relating to the performance of specialised assessments on the organisation's critical systems.

Implementation Maturity

MATURITY	EVIDENCE TO BE CONSIDERED
1	No specialised assessments, e.g. in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, performance/load testing, and verification and validation testing, are performed on the organisation's critical systems.
2	Specialised assessments of the organisation's critical systems are performed in an ad hoc and informal manner and without a clear policy or process.
3	A formal process for performing specialised assessments on the organisation's critical systems is present and is implemented. Evidence is available for most activities. Regular reviews (e.g. assessment reports, assessment calendar) show that inconsistencies between what is documented and what is implemented in the field amount to less than 10%.
4	Specialised assessments on the organisation's critical systems are performed in a formal way by implementing the respective process. Evidence is available for all activities. Regular reviews (e.g. assessment reports, assessment calendar) show that 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	Specialised assessments on the organisation's critical systems are performed in a formal way by implementing the respective process. Evidence is available for all activities. Regular reviews (e.g. assessment reports, assessment calendar) 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 shows continuous improvement.

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