TLP:GREEN

CENTRE FOR
CYBERSECURITY
BELGIUM

CyberFundamentals Maturity Level Assessment of Key & Management aspect related Measures

Cybersecurity Certification Authority

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

.be

Change Log

CENTRE FOR CYBERSECURITY BELGIUM

Version	Changes
01 May 2024	Creation of the document – baseline of all use cases
09 September 2024	New slide 4 “Clarifications” Updated use case “PR.PT-1.1 Logs shall be maintained, documented and reviewed.”

Disclaimer

To guide organisations in the CyFun® self-assessment (Basic, Important and Essential) and to support the CyFun® Conformity Assessment Scheme, CCB has created assessments of the different maturity levels for key measures and measures related to entity management.

The attached assessments are **intended as guidance** to help assessors distinguish between the different maturity levels. An entity's maturity level assessment may differ from this because of:

- Context, perspective or scope
- Organisation-specific implementations

As described in the CyFun® Conformity Assessment Scheme, it remains up to the assessor to evaluate the self-assessment along with supporting objective evidence.

More information on the CyFun® Conformity Assessment Scheme can be found on www.cyfun.eu

Clarifications

Review: In the implementation guidance the terminology “review” is used in the evidence to be considered. “Review” is defined as the internal assessment activity undertaken by the organisation to determine the suitability, adequacy and effectiveness of the subject under assessment to assign a maturity level. (Based on the definition of “review” in ISO/IEC 27000)

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

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

IMPORTANT

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, which, however, 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. For missing descriptions of roles, responsibilities and authorities, there is a documented and approved reason while 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. For missing descriptions of roles, responsibilities and authorities, there is a documented and approved reason while 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).

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

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

IMPORTANT

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 ad hoc and their management is informal.
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) reveal inconsistencies between what is documented and the real situation in less than 10% of the cases.

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

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
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 minimal targets (e.g. number of descriptions) identified. Reviews (e.g. audits) reveal inconsistencies between what is documented and the real situation 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 minimal targets (e.g. number of descriptions), are deployed to monitor the process. Reviews (e.g. audits) reveal inconsistencies between what is documented and the real situation in less than 1% of the cases. Identified inconsistencies lead to improvement actions that contribute to continuous process improvement. Process performance is reported as described in the applicable process documentation.

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

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	The function of information security officer doesn’t exist.
2	The function of information security officer is identified on the formally approved organization chart of the organization but there exist no function description.
3	A formally approved job description of an information security officer is available that includes the role and responsibilities but lacks the authorities.
4	A formally approved job description of an information security officer is available that includes the role, responsibilities and authorities.
5	A formally approved job description of an information security officer is available with the role, responsibilities and authority, explicitly identifying the position as a member of the organisation's executive committee.

CENTRE FOR CYBERSECURITY BELGIUM

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

Implementation Maturity

ESSENTIAL

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 is 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 is confirmed during reviews (e.g. audits) 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 DIRCOM and participates in strategic information security discussions. This is confirmed during reviews (e.g. audits) is reported 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 further pursued.

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

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	There is no process documentation or formally approved documentation by management that ensures 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 when 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, formally approved, and this documentation is reviewed regularly. On the total number of identified information security and cybersecurity risks, less than 5% do not have action plans to mitigate the identified risks. The reason therefor is documented and approved.
4	Controlled (versioned, approved) process documentation exists to ensure that Information security and cybersecurity risks are documented, formally approved, and this documentation is reviewed regularly. On the total number of identified information security and cybersecurity risks, less than 3% do not have action plans to mitigate the identified risks. The reason therefor is documented and approved.
5	Controlled (versioned, approved) process documentation exists to ensure that Information security and cybersecurity risks are documented, formally approved, and this documentation is reviewed regularly. All identified information security and cybersecurity risks have action plans to mitigate the identified risks.

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

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	There is no standard process ensuring 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 when changes occur on an ad hoc basis. This is all managed informally.
3	A formal process exist and is implemented to document, formally approve, and update information security and cybersecurity risks when changes occur. Evidence, proving that information security and cybersecurity risks are documented, approved and updated, is mostly available. Reviews (e.g. audits) show for less than 10% of the total number of identified information security and cybersecurity risks, considering the exceptions identified in the documentation, that progress of action plans to control risks is not monitored.
4	A formal process exist and is implemented to document, formally approve, and update information security and cybersecurity risks when changes occur. Evidence, proving that information security and cybersecurity risks are documented, approved and updated, is always available. Reviews (e.g. audits) show for less than 5% of the total number of identified information security and cybersecurity risks, considering the exceptions identified in the documentation, that progress of action plans to control risks is not monitored. Detailed process performance metrics, including minimal process performance targets, are measured and reported.
5	A formal process exist and is implemented to document, formally approve, and update information security and cybersecurity risks when changes occur. Evidence, proving that information security and cybersecurity risks are documented, approved and updated, is always available. Reviews (e.g. audits) show for less than 10% of the total number of identified information security and cybersecurity risks, considering the exceptions identified in the documentation, that progress of action plans to control risks is not monitored. Detailed process performance metrics, including minimal process performance targets, are measured, reported and show continuous improvement.

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

Documentation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	There is no process documentation or formally approved documentation by management that ensures that the organization conducts and documents risk assessments.
2	The organisation has a controlled process documentation (versioned and approved) to ensure that the organization 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 organization 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. On the total number of identified organisation’s core processes, for less than 5% no risk assessments are performed. The reason therefor is documented and approved.
4	Controlled (versioned, approved) process documentation exists to ensure that the organization 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. On the total number of identified organisation’s core processes, for less than 3% no risk assessments are performed. The reason therefor is documented and approved.
5	Controlled (versioned, approved) process documentation exists to ensure that the organization 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. On the total number of identified organisation’s processes, for less than 0,5% of those processes, which practically amounts to none, no risk assessments are performed. If exclusions are made, the reason therefor is documented and approved.

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

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	There is no standard process ensuring that the organization 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 managed informally.
3	A formal process exist 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. Reviews (e.g. audits) show for less than 10% of the processes on which risk assessments are performed, 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).

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

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
4	A formal process exist 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. Reviews (e.g. audits) show for less than 5% of the processes on which risk assessments are performed, 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.
5	A formal process exist 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. Reviews (e.g. audits) show for less than 1% of the processes on which risk assessments are performed, 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-5.3 Risk assessment results shall be disseminated to relevant stakeholders.

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	There is no process documentation or formally approved documentation by management that ensures that risk assessment results are disseminated to relevant stakeholders.
2	The organisation has a 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 this documentation is reviewed regularly. On the total number of identified organisation's relevant stakeholders (e.g. during a context analysis), for less than 5% no risk assessment results are distributed. The reason therefor is documented and approved.
4	Controlled (versioned, approved) process documentation exists to ensure that the risk assessment results are disseminated to relevant stakeholders, and this documentation is reviewed regularly. On the total number of identified organisation's relevant stakeholders (e.g. during a context analysis), for less than 3% no risk assessment results are distributed. The reason therefor is documented and approved.
5	Controlled (versioned, approved) process documentation exists to ensure that the risk assessment results are disseminated to relevant stakeholders, and this documentation is reviewed regularly. On the total number of identified organisation's relevant stakeholders (e.g. during a context analysis), for less than 0,5% (which practically amounts to none) no risk assessment results are distributed. The reason therefor is documented and approved.

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

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	There is no standard process ensuring that risk assessment results are disseminated to relevant stakeholders.
2	Risk assessment results are disseminated to relevant stakeholders on an ad hoc basis and managed informally.
3	A formal process exist and is implemented to distribute risk assessment results to relevant stakeholders. Evidence is mostly available, considering the documented and approved exceptions. Reviews (e.g. audits) show for less than 10% of the cases the risk assessment results are not disseminated where they should be.
4	A formal process exist and is implemented to distribute risk assessment results to relevant stakeholders. Evidence is always available, considering the documented and approved exceptions. Reviews (e.g. audits) show for less than 5% of the cases the risk assessment results are not disseminated where they should be. Detailed process performance metrics, including minimal process performance targets, are measured and reported.
5	A formal process exist and is implemented to distribute risk assessment results to relevant stakeholders. Evidence is always available, considering the documented and approved exceptions. Reviews (e.g. audits) show for less than 1% of the cases the risk assessment results are not disseminated where they should be. 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 organization’s critical systems, that includes the identification and prioritization of risk responses.

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	There is no controlled (version controlled and approved) documented strategy to manage risks to the organization’s critical systems, that includes the identification and prioritization of risk responses.
2	There is a controlled (version controlled and approved) documented strategy to manage risks to the organization’s critical systems, that includes the identification and prioritization of risk responses, which, however, hasn’t been reviewed in the past 2 years.
3	There is a controlled (version controlled and approved) documented strategy to manage risks to the organization’s critical systems, including the identification and prioritization of risk responses. The strategy however only covers a part of the organization’s critical systems. The organization’s critical systems that are not covered are limited to less than 5% of the total of identified organization’s critical systems. The reason for exclusion of critical systems is documented and approved.
4	There is a controlled (version controlled and approved) documented strategy to manage risks to the organization’s critical systems, including the identification and prioritization of risk responses. The strategy however only covers a part of the organization’s critical systems. The organization’s critical systems that are not covered are limited to less than 3% of the total of identified organization’s critical systems. The reason for exclusion of critical systems is documented and approved.
5	There is a controlled (version controlled and approved) documented strategy to manage risks to the organization’s critical systems, including the identification and prioritization of risk responses. The strategy covers all the organization’s critical systems. There are no exclusions.

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

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	There is no strategy to manage risks to the organization’s critical systems.
2	The strategy to manage risks to the organization’s critical systems that has been developed is implemented on an ad hoc basis and managed informally.
3	A comprehensive strategy is developed and implemented to manage risks to the organization’s critical systems, that includes the identification and prioritization of risk responses, including the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of the implemented process reveal less than 10% inconsistencies between what is documented and what is implemented in the field.

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

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
4	A comprehensive strategy is developed and implemented to manage risks to the organization’s critical systems, that includes the identification and prioritization of risk responses, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) of the implemented process reveal less than 5% inconsistencies between what is documented and what is implemented in the field. 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 organization’s critical systems, that includes the identification and prioritization of risk responses, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) of the implemented process reveal less than 1% inconsistencies between what is documented and reality. Metrics, including targets, are in place to monitor the implementation of the strategy. Process performance results are translated in 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.

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

IMPORTANT

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, have not been reviewed in the past 2 years.
3	There is a controlled (version controlled and approved) regularly reviewed and up-to-date documented cyber risk management process that identifies key internal and external stakeholders that facilitates the addressing of risk-related issues and information. The process is updated when 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 (which include e.g. customers, investors and shareholders, suppliers, government agencies and the wider community). This is documented and approved.
4	There is a controlled (version controlled and approved) regularly reviewed and up-to-date documented cyber risk management process that identifies key internal and external stakeholders that facilitates the addressing of risk-related issues and information. The process is updated when 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 (which include e.g. 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) regularly reviewed and up-to-date documented cyber risk management process that identifies key internal and external stakeholders that facilitates the addressing of risk-related issues and information. The process is updated when changes occur. The cyber risk management process apply to all key internal and external stakeholders without exception.

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.

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	There is no controlled (version checked and approved) cyber risk management process created nor implemented.
2	Cyber risk management of key internal and external stakeholders that supports the addressing of risk-related issues and information is done 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 on process implementation is available for most activities. Reviews (e.g. audits) reveal in less than 10% of the cases inconsistencies between documentation and reality.

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.

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
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 on process implementation is available for all activities. Reviews (e.g. audits) reveal in less than 5% of the cases inconsistencies between documentation and reality. Metrics have been deployed and minimal targets on process performance 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 on process implementation is available for all activities. Reviews (e.g. audits) reveal inconsistencies between documentation and reality in less than 1% of the cases. Identified inconsistencies lead to improvement actions that contribute to continuous process improvement. Process performance is reported as described in the applicable process documentation.

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

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	There is no process documentation or formally approved documentation by management that ensures that the organization clearly determines its risk appetite.
2	The organisation has a controlled process documentation (versioned and approved) to ensure that the organization clearly determines its risk appetite (e.g. by 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 organization clearly determines its risk appetite (e.g. by 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 through risk tolerance. For less than 5% of the risk appetite statements no risk tolerances are established. The reason therefor is documented and approved by the management.
4	Controlled (versioned, approved) process documentation exists to ensure that the organization clearly determines its risk appetite (e.g. by 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 through risk tolerance. For less than 3% of the risk appetite statements no risk tolerances are established. The reason therefor is documented and approved by the management.
5	Controlled (versioned, approved) process documentation exists to ensure that the organization clearly determines its risk appetite, and this documentation is reviewed regularly. For all risk appetite statements risk tolerances are established.

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

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	There is no standard process ensuring that the organization clearly determines its risk appetite.
2	Risk assessment results are disseminated to relevant stakeholders on an ad hoc basis and managed informally.
3	A formal process exist and is implemented to determine the organization’s risk appetite through e.g. risk appetite statements reflecting the organization’s internal and external context for which evidence is mostly available, considering the documented and approved exceptions. Reviews (e.g. audits) show for less than 10% of the sample used during a review that determining the risk appetite is not happening according to the documented process.

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

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
4	A formal process exist and is implemented to determine the organization’s risk appetite through e.g. risk appetite statements reflecting the organization’s internal and external context for which evidence is always available, considering the documented and approved exceptions. Reviews (e.g. audits) show for less than 5% of the sample used during a review that determining the risk appetite is not happening according to the documented process. Detailed process performance metrics, including minimal process performance targets, are measured and reported.
5	A formal process exist and is implemented to determine the organization’s risk appetite through e.g. risk appetite statements reflecting the organization’s internal and external context for which evidence is always available, considering the documented and approved exceptions. Reviews (e.g. audits) show for less than 1% of the sample used during a review that determining the risk appetite is not happening according to the documented process. Detailed process performance metrics, including minimal process performance targets, are measured, reported and show continuous improvement.

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

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	There is no documentation or formally approved documentation 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 a 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 organization identifies, assesses, and mitigates cybersecurity supply chain risks. This documentation is reviewed regularly, approved, updated when changes occur. No supply chain risk management plan exists for less than 5% of the organisation's critical mission and business functions. The reason therefor is documented and approved by the management.

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

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	Controlled (versioned, approved) documentation (strategy, objectives, policies, and procedures) exists to ensure that the organization identifies, assesses, and mitigates cybersecurity supply chain risks. This documentation is reviewed regularly, approved, updated when changes occur. No supply chain risk management plan exists for less than 3% of the organisation's critical mission and business functions. The reason therefor is documented and approved by the management.
5	Controlled (versioned, approved) documentation (strategy, objectives, policies, and procedures) exists to ensure that the organization identifies, assesses, and mitigates cybersecurity supply chain risks. This documentation is reviewed regularly, approved, updated when changes occur. Supply chain risk management plan exists for all the organisation's critical mission and business functions.

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

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	There is no standard process ensuring that the organization documents, reviews, approves, updates when 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 exist and is implemented ensuring that the organization identifies, assesses, and mitigates cybersecurity supply chain risks, taking into account the documented and approved exceptions (being missing 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 cyber security risk cannot be shown to adequately mitigate the cyber security risk.

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

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	A formal cyber supply chain risk management process exist and is implemented ensuring that the organization identifies, assesses, and mitigates cybersecurity supply chain risks, taking into account the documented and approved exceptions (being missing 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 cyber security risk cannot be shown to adequately mitigate the cyber security risk. Detailed process performance metrics, including minimal process performance targets, are measured and reported.
5	A formal cyber supply chain risk management process exist and is implemented ensuring that the organization identifies, assesses, and mitigates cybersecurity supply chain risks, taking into account the documented and approved exceptions (being missing 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 cyber security risk cannot be shown to adequately mitigate the cyber security risk. Detailed process performance metrics, including minimal process performance targets, are measured, 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

ESSENTIAL

Maturity	Evidence to be considered
1	There is no process documentation or formally approved documentation by the management ensuring that contractual ‘information security and cybersecurity’ requirements for suppliers and third-party partners are implemented.
2	The controlled (version control, approved) process documentation ensuring 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 ensuring 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 flaws identified during ‘information security and cybersecurity’ testing and evaluation are corrected. Concerned suppliers and third-party partners are identified and exceptions on the implementation of these contractual requirements are documented, approved and limited to less than 5% of the total number of concerned suppliers and third-party partners.

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.

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	Controlled (version control, approved) process documentation ensuring 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 flaws identified during ‘information security and cybersecurity’ testing and evaluation are corrected. Concerned suppliers and third-party partners are identified and exceptions on the implementation of these contractual requirements are documented, approved and limited to less than 3% of the total number of concerned suppliers and third-party partners
5	Controlled (version control, approved) process documentation ensuring 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 flaws identified during ‘information security and cybersecurity’ testing and evaluation are corrected. Concerned suppliers and third-party partners are identified and exceptions on 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 concerned suppliers and third-party partners.

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.

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	There is no standard process ensuring 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 is ad hoc implemented and managed informally.
3	A formal process to implement contractual ‘information security and cybersecurity’ requirements for suppliers and third-party partners exist and is implemented. Evidence is available for most suppliers and third-party partners. Regular reviews (e.g. audits) show less then 10% inconsistencies between what is documented, including the exceptions, and what is implemented.

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.

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	A formal process to implement contractual ‘information security and cybersecurity’ requirements for suppliers and third-party partners exist and is implemented. Evidence is available for all suppliers and third-party partners. Regular reviews (e.g. audits) show less then 5% inconsistencies between what is documented, including the exceptions, and what is implemented. Detailed process performance metrics, including minimal 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 exist and is implemented. Evidence is available for all suppliers and third-party partners. Regular reviews (e.g. audits) show less then 1% inconsistencies between what is documented, including the exceptions, and what is implemented. Detailed process performance metrics, including minimal process performance targets, are measured, reported and show continuous improvement.

ID.SC-3.3 The organization shall establish contractual requirements permitting the organization to review the ‘information security and cybersecurity’ programs implemented by suppliers and third-party partners.

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	There is no process documentation or formally approved documentation by the management ensuring that contractual requirements that allow the organisation to assess "information security and cybersecurity" programs implemented by suppliers and external partners.
2	The controlled (version control, approved) process documentation ensuring that contractual requirements that allow the organisation to assess "information security and cybersecurity" programs implemented by suppliers and external partners exists, but has not been reviewed in the past 2 years.
3	Controlled (version control, approved) process documentation ensuring that contractual requirements that allow the organisation to assess "information security and cybersecurity" programs implemented by suppliers and external partners exists and is regularly reviewed. Concerned suppliers and third-party partners are identified and exceptions on the implementation of these contractual requirements are documented, approved and limited to less than 5% of the total number of concerned suppliers and third-party partners.

ID.SC-3.3 The organization shall establish contractual requirements permitting the organization to review the ‘information security and cybersecurity’ programs implemented by suppliers and third-party partners.

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	Controlled (version control, approved) process documentation ensuring that contractual requirements that allow the organisation to assess "information security and cybersecurity" programs implemented by suppliers and external partners exists and is regularly reviewed. Concerned suppliers and third-party partners are identified and exceptions on the implementation of these contractual requirements are documented, approved and limited to less than 3% of the total number of concerned suppliers and third-party partners.
5	Controlled (version control, approved) process documentation ensuring that contractual requirements that allow the organisation to assess "information security and cybersecurity" programs implemented by suppliers and external partners exists and is regularly reviewed. Concerned suppliers and third-party partners are identified and exceptions on 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 concerned suppliers and third-party partners.

ID.SC-3.3 The organization shall establish contractual requirements permitting the organization to review the ‘information security and cybersecurity’ programs implemented by suppliers and third-party partners.

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	There is no standard process ensuring that requirements that allow the organisation to assess "information security and cybersecurity" programs 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" programs implemented by suppliers and external partners are ad hoc implemented and managed informally.
3	A formal process to implement contractual requirements that allow the organisation to assess "information security and cybersecurity" programs implemented by suppliers and external partners exist and is implemented. Evidence is available for most suppliers and third-party partners. Regular reviews (e.g. audits) show less then 10% inconsistencies between what is documented, including the exceptions, and what is implemented.

ID.SC-3.3 The organization shall establish contractual requirements permitting the organization to review the ‘information security and cybersecurity’ programs implemented by suppliers and third-party partners.

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	A formal process to implement contractual requirements that allow the organisation to assess "information security and cybersecurity" programs implemented by suppliers and external partners exist and is implemented. Evidence is available for all suppliers and third-party partners. Regular reviews (e.g. audits) show less then 5% inconsistencies between what is documented, including the exceptions, and what is implemented. Detailed process performance metrics, including minimal 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" programs implemented by suppliers and external partners exist and is implemented. Evidence is available for all suppliers and third-party partners. Regular reviews (e.g. audits) show less then 1% inconsistencies between what is documented, including the exceptions, and what is implemented. Detailed process performance metrics, including minimal process performance targets, are measured, reported and show continuous improvement.

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

Documentation Maturity

BASIC

Maturity	Evidence to be considered
1	No controlled (version controlled and approved) documentation on how identities and credentials for authorized devices and users are managed exists.
2	Controlled (version and approved) documentation (policy, process, SOP…) on how identities and credentials for authorized devices and users are managed exists but hasn’t been reviewed in the previous 2 years.
3	Controlled (version and approved) documentation on how identities and credentials for authorized devices and users are managed is available and up-to-date. Exceptions on the process are documented and approved and are only applicable on less than 5% of the total of identified authorized devices and users.

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

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

BASIC

Maturity	Evidence to be considered
4	Controlled (version and approved) documentation on how identities and credentials for authorized devices and users are managed exists and is regularly reviewed and updated. Exceptions on the process are documented and approved and are only applicable on less than 3% of the total of identified authorized devices and users.
5	Controlled (version and approved) documentation on how identities and credentials for authorized devices and users are managed exists and is regularly reviewed and updated. Exceptions on the process are documented and approved and are only applicable on less than 0,5% of the total of identified authorized devices and users.

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
1	There is no management of identities and credentials for authorized devices and users defined no implemented.
2	Management of identities and credentials for authorized devices and users is managed through and ad hoc process and is done informally.
3	Identities and credentials for authorized devices and users are managed as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of the implemented process reveal less than 10% inconsistencies between what is documented and what is implemented in the field (e.g. through review of the password policy).

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
4	Identities and credentials for authorized devices and users are managed as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits) show less then 5% cases where the process is not followed. Metrics, including targets, are in place to monitor the identity and credential management for authorized devices and users. Process performance is reported as described in the applicable process documentation.

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

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

BASIC

Maturity	Evidence to be considered
5	Identities and credentials for authorized devices and users are managed as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits) show less then 1% cases where the process is not followed. Metrics, including targets, are in place to monitor the identity and credential management for authorized devices and users. Process performance results are translated in opportunities for improvement. Process performance is reported as described in the applicable process documentation.

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

Documentation Maturity

BASIC

Maturity	Evidence to be considered
1	No controlled (version controlled and approved) documentation exists to ensure that the organization's networks when accessed remotely is secured.
2	Controlled (version controlled and approved) documentation exists to ensure that the organization's networks when accessed remotely is secured, but this documentation hasn’t been reviewed in the previous 2 years.
3	Controlled (version and approved) documentation that ensures that the organization's networks when accessed remotely is secured, incl. the use of MFA, is available and up-to-date. Exceptions on securing remote access protocols (e.g. the use of MFA) are documented and approved and are limited to less than 5% of remote connections to the organisation's network measured against the average number of remote connections made in a formally predetermined period (e.g. using activity logs covering a period of the previous 6 months).

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

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

BASIC

Maturity	Evidence to be considered
4	Controlled (version and approved) documentation that ensures that the organization's networks when accessed remotely is secured, incl. the use of MFA, is available, regularly reviewed and updated. Exceptions on securing remote access protocols (e.g. the use of MFA) are documented and approved and are limited to less than 3% of remote connections to the organisation's network (measured as explained in Maturity level 3).
5	Controlled (version and approved) documentation that ensures that the organization's networks when accessed remotely is secured, incl. the use of MFA, is available, regularly reviewed and updated. Exceptions on securing remote access protocols (e.g. the use of MFA) are documented and approved and are limited to less than 0,5% of remote connections to the organisation's network (measured as explained in Maturity level 3).

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
1	There is no process implemented to ensure that the organization's networks when accessed remotely is secured.
2	Securing the organization's networks when accessed remotely is done on an ad-hoc basis without formal management of the process.
3	Securing the organization's networks when accessed remotely is done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of the implemented process reveals less than 10% inconsistencies (e.g. not using MFA where it is prescribed) between what is documented and what is implemented in the field.

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

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

BASIC

Maturity	Evidence to be considered
4	Securing the organization's networks when accessed remotely is done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) show less then 5% cases where the process is not followed. Metrics, including targets, are in place to monitor the process. Process performance is reported as described in the applicable process documentation.
5	Securing the organization's networks when accessed remotely is done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) show less then 1% cases where the process is not followed. Metrics, including targets, are in place to monitor the process. Process performance results are translated in opportunities for improvement. Process performance is reported as described in the applicable process documentation.

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

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization's critical systems environment are not identified nor documented.
2	Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization's critical systems environment are identified and document in a controlled (version and approved) way (e.g. user authentication policies); However, that documentation has not been reviewed in the last 2 years.
3	Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization's critical systems environment are identified and document in a controlled (version and approved) way. Exceptions on usage restrictions and authorizations for remote access to the organization's critical systems environment (e.g. OT devices) are documented, approved and limited to less than 5% of the total of the organization's critical systems.
4	Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization's critical systems environment are identified and document in a controlled (version and approved) way. Exceptions on usage restrictions and authorizations for remote access to the organization's critical systems environment (e.g. OT devices) are documented, approved and limited to less than 3% of the total of the organization's critical systems.
5	Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization's critical systems environment are identified and document in a controlled (version and approved) way. There are no exceptions.

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

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	There are no usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization’s critical systems environment.
2	Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization’s critical systems environment are implemented on an ad hoc basis and managed informally.
3	Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization’s critical systems environment are as documented in the relevant documentation. Evidence is available for most activities. Review (e.g. audits) of what is present in the field reveals less than 10% inconsistencies with what is documented.
4	Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization’s critical systems environment are as documented in the relevant documentation. Evidence of implementation is available for all activities. Review (e.g. through audits) reveals less than 5% inconsistencies with what is documented. Detailed metrics of the process, for which minimal targets for metrics have been established, are captured and reported.
5	Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization’s critical systems environment are as documented in the relevant documentation. Evidence of implementation is available for all activities. Review (e.g. through audits) reveals less than 1% inconsistencies with what is documented. Detailed metrics of the process, for which minimal targets for metrics have been established, are captured, reported, and show continuous improvement of process performance.

PR.AC-4.1 Access permissions for users of the organization’s systems shall be defined and managed.

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

BASIC

Maturity	Evidence to be considered
1	No controlled (version controlled and approved) documentation on managing access permissions for users to the organization’s systems exists.
2	Controlled (version and approved) documentation (policy, process, SOP…) on managing access permissions for users of the organization’s systems exists but hasn’t been reviewed in the previous 2 years.
3	Controlled (version and approved) documentation on managing access permissions for users to the organization’s systems is available and up-to-date. Exceptions on the process are documented and approved and are only applicable to less than 5% of the total of identified users of the organization’s systems.

PR.AC-4.1 Access permissions for users of the organization’s systems shall be defined and managed.

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

BASIC

Maturity	Evidence to be considered
4	Controlled (version and approved) documentation on managing access permissions for users to the organization’s systems exists and is regularly reviewed and updated. Exceptions on the process are documented and approved and are only applicable to less than 3% of the total of identified users.
5	Controlled (version and approved) documentation on managing access permissions for users of the organization’s systems is available, regularly reviewed and up-to-date. Exceptions on the process are documented and approved and are only applicable to less than 0,5% of the total of identified users.

PR.AC-4.1. Access permissions for users of the organization’s systems shall be defined and managed.

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

BASIC

Maturity	Evidence to be considered
1	Access permissions for users of the organization’s systems are not defined nor managed (e.g. No access lists per system, no difference between user accounts or admin accounts, No central account management system).
2	Access permissions for users of the organization’s systems are managed through and ad hoc process and is done informally.
3	Access permissions for users of the organization’s systems are managed as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of the implemented process reveal less than 10% inconsistencies between what is documented and what is implemented in the field.

PR.AC-4.1. Access permissions for users of the organization’s systems shall be defined and managed.

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

BASIC

Maturity	Evidence to be considered
4	User Access permissions are managed as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) show less then 5% cases where the process is not followed. Metrics, including targets, are in place to monitor the user access permission process. Process performance is reported as described in the applicable process documentation.

PR.AC-4.1. Access permissions for users of the organization’s systems shall be defined and managed.

CENTRE FOR
CYBERSECURITY
BELGIUM

Implementation Maturity

BASIC

Maturity	Evidence to be considered
5	User Access permissions are managed as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) show less then 1% cases where the process is not followed. Metrics, including targets, are in place to monitor the user access permission process. Process performance results are translated in opportunities for improvement. Process performance is reported as described in the applicable process documentation.

CENTRE FOR CYBERSECURITY BELGIUM

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

Documentation Maturity

BASIC

Maturity	Evidence to be considered
1	No controlled (version controlled and approved) documentation on who has access to the business' critical information and how to get access to that information exists.
2	Controlled (version and approved) documentation (policy, process, SOP…) on who has access to the business' critical information and how to get access to that information exists, but the documentation hasn't been reviewed in the previous 2 years.
3	Controlled (version and approved) documentation on who has access to the business' critical information and how to get access to that information is available and up-to-date. Exceptions on the process are documented and approved and are only applicable to less than 5% of the total of the critical information identified in the organisation's critical information list (CIL).

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

Documentation Maturity

BASIC

Maturity	Evidence to be considered
4	Controlled (version and approved) documentation on who has access to the business' critical information and how to get access to that information exists and is regularly reviewed and updated. Exceptions on the process are documented and approved and are only applicable to less than 3% of the total of the critical information identified in the organisation's critical information list (CIL).
5	Controlled (version and approved) documentation on who has access to the business' critical information and how to get access to that information exists and is regularly reviewed and updated. Exceptions on the process are documented and approved and are only applicable to less than 0,5% of the total of the critical information identified in the organisation's critical information list (CIL).

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
1	There are no requirements for the identification on who should have access and the means used to get access to the business’ critical information identified nor managed.
2	The identification on who has access to the business’ critical information and how to get access to that information is managed through and ad hoc process and is done informally.
3	The identification on who has access to the business’ critical information and how to get access to that information is performed as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of the implemented process reveal less than 10% inconsistencies between what is documented and what is implemented in the field.

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
4	The identification on who and how one has access to the business’ critical information is done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) show less then 5% cases where the process is not followed. Metrics, including targets, are in place to monitor the process. Process performance is reported as described in the applicable process documentation.

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
5	The identification on who and how one has access to the business’ critical information is done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) show less then 1% cases where the process is not followed. Metrics, including targets, are in place to monitor the process. Process performance results are translated in opportunities for improvement. Process performance is reported as described in the applicable process documentation.

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

Documentation Maturity

BASIC

Maturity	Evidence to be considered
1	No controlled (version controlled and approved) documentation exists to ensure that each employee only gets the system resources and authorisations needed to perform its function.
2	Controlled (version controlled and approved) documentation exists to ensure that each employee only gets the system resources and authorisations needed to perform its function, but this documentation hasn’t been reviewed in the previous 2 years.
3	Controlled (version and approved) documentation on the limitation of employee access to data and information is available and up-to-date. Exceptions on the principle of Least Privilege are documented and approved and may not exceed more than 4% of the accounts, processes, programs and other resources identified in the role description.

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

Documentation Maturity

BASIC

Maturity	Evidence to be considered
4	Controlled (version and approved) documentation on the limitation of employee access to data and information exists and is regularly reviewed and updated. Exceptions on the principle of Least Privilege are documented and approved and may not exceed more than 2% of the accounts, processes, programs and other resources identified in the role description.
5	Controlled (version and approved) documentation on the limitation of employee access to data and information exists and is regularly reviewed and updated. There are no exceptions on the principle of Least Privilege and access to accounts, processes, programs and other resources is as identified in the role description.

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
1	Employee access to data and information is not limited to the systems and specific information they need to do their jobs.
2	Employee access to data and information is limited to the systems and specific information they need to do their jobs on an ad hoc basis and is managed informally.
3	The implementation of the principle of Least Privilege is performed as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of the implemented process reveals less than 10% inconsistencies between what is documented and what is implemented in the field.

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
4	The implementation of the principle of Least Privilege is performed as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) show less then 5% cases where the process is not followed. Metrics, including targets, are in place to monitor the process. Process performance is reported as described in the applicable process documentation.

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

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

BASIC

Maturity	Evidence to be considered
5	The implementation of the principle of Least Privilege is performed as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) show less then 1% cases where the process is not followed. Metrics, including targets, are in place to monitor the process. Process performance results are translated in opportunities for improvement. Process performance is reported as described in the applicable process documentation.

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

Documentation Maturity

BASIC

Maturity	Evidence to be considered
1	No controlled (version controlled and approved) documentation exists to ensure that nobody has administrator privileges for daily tasks.
2	Controlled (version controlled and approved) documentation exists to ensure that nobody has administrator privileges for daily tasks, but this documentation hasn’t been reviewed in the previous 2 years.
3	Controlled (version and approved) documentation that ensures that nobody has administrator privileges for daily tasks is available and up-to-date. Exceptions on granting personnel administrator privileges for daily tasks are documented and approved and are limited to less than 5%of the personnel active in the entity.

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

Documentation Maturity

BASIC

Maturity	Evidence to be considered
4	Controlled (version and approved) documentation that ensures that nobody has administrator privileges for daily tasks is available, regularly reviewed and updated. Exceptions on granting personnel administrator privileges for daily tasks are documented and approved and are limited to less than 3% of the personnel active in the entity.
5	Controlled (version and approved) documentation that ensures that nobody has administrator privileges for daily tasks is available, regularly reviewed and updated. Exceptions on granting personnel administrator privileges for daily tasks are documented and approved and are limited to less than 0,5% of the personnel active in the entity.

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
1	There is no process implemented that ensures that nobody has administrator privileges for daily tasks.
2	Administrator privileges for daily tasks are informally granted on an ad hoc basis.
3	Ensuring that nobody has administrator privileges for daily tasks is done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of the implemented process reveals less than 10% inconsistencies between what is documented and what is implemented in the field.

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
4	Ensuring that nobody has administrator privileges for daily tasks is done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) show less then 5% cases where the process is not followed. Metrics, including targets, are in place to monitor the process. Process performance is reported as described in the applicable process documentation.
5	Ensuring that nobody has administrator privileges for daily tasks is done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) show less then 1% cases where the process is not followed. Metrics, including targets, are in place to monitor the process. Process performance results are translated in opportunities for improvement. Process performance is reported as described in the applicable process documentation.

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

BASIC

Documentation Maturity

Maturity	Evidence to be considered
1	No controlled (version controlled and approved) documentation on the installation and activation of firewalls exists (e.g. process documentation, inventories of installed and activated firewalls).
2	Controlled (version controlled and approved) documentation on the installation and activation of firewalls exists but hasn't been reviewed in the previous 2 years. Inventories are outdated.
3	Controlled (version and approved) documentation on the installation and activation of firewalls exists. Inventories are up-to-date. Exceptions on the process are documented and approved and are only applicable on less than 5% of the gateways to the Internet.
4	Controlled (version and approved) documentation on the installation and activation of firewalls exists and is regularly reviewed and updated. Inventories are up-to-date. Exceptions on the process are documented and approved and are only applicable on less than 3% of the gateways to the Internet.
5	Controlled (version and approved) documentation on the installation and activation of firewalls exists and is regularly reviewed and updated. Inventories are up-to-date. Exceptions on the process are documented and approved and are only applicable on less than 0,5% of the gateways to the Internet.

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
1	There are firewalls installed and activated but no additional information is available.
2	Firewalls are installed and activated on an ad hoc basis. Information on the installed and activated firewalls is informal (e.g. “The ICT Manager knows where they are”).
3	Firewalls are installed and activated as specified in the relevant process documentation, including the documented exceptions. Inventories, including location, firmware, serial number, and data on maintenance, are available for more than 90% of the installed and activated firewalls. Evidence on process implementation is available for most activities.

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

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

BASIC

Maturity	Evidence to be considered
4	Firewalls are installed and activated as specified in the relevant process documentation, including the documented exceptions. Inventories, including location, firmware, serial number, and data on maintenance, are available for more than 95% of the installed and activated firewalls. Evidence on process implementation is available for all activities. Metrics on firewall update, maintenance and replacement are established monitored and acted upon. Clear targets on updates are available demonstrating firewalls capability to provide sufficient protection against threats.
5	Firewalls are installed and activated as specified in the relevant process documentation, including the documented exceptions. Inventories, including location, firmware, serial number, and data on maintenance, are available for more than 99% of the installed and activated firewalls. Metrics on firewall update, maintenance and replacement are established monitored and acted upon. Evidence on process implementation is available for all activities. Clear targets on updates are available demonstrating firewalls capability to provide sufficient protection against threats, including measures to continuously improve this protection.

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

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

BASIC

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

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
1	There is no network segmentation nor segregation implemented.
2	Network segmentation and segregation is done on an ad hoc basis without a corporate strategy.
3	Network segmentation and segregation is as documented in the relevant documentation. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of what is implemented in the field reveals less than 10% inconsistencies with what is documented.

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
4	Network segmentation and segregation is as documented in the relevant documentation. Evidence on process implementation is available for all activities. Reviews (e.g. audits) of what is implemented in the field reveals less than 5% inconsistencies with what is documented. Metrics, including targets, are in place to monitor the accuracy of network visualisation to able 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.
5	Network segmentation and segregation is as documented in the relevant documentation. Evidence on process implementation is available for all activities. Reviews (e.g. audits) of what is implemented in the field reveals less than 1% inconsistencies with what is documented. Metrics, including targets, are in place to monitor the accuracy of network visualisation to able 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. Identified network integrity risks are translated into improvement opportunities that contribute to the continuous improvement of network integrity.

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

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

(2) Limiting external connections to the organization's critical systems.

Documentation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	Connections between system components and external connections to the organization's critical systems are not identified nor documented.
2	Connections between system components and external connections to the organization's critical systems are identified and document in a controlled (version and approved) way in for example a network architecture diagram; However, that documentation has not been reviewed in the last 2 years.
3	Connections between system components and external connections to the organization's critical systems are identified and documented in a controlled (version and approved) way in for example a network architecture diagram. Exceptions on the level of detailing critical systems in the entity's network architecture diagram are documented, approved and limited to less than 5% of the total number of identified critical systems.

PR.AC-5.3 Where appropriate, network integrity of the organization's critical systems shall be protected by
(1) Identifying, documenting, and controlling connections between system components.
(2) Limiting external connections to the organization's critical systems.

Documentation Maturity

IMPORTANT

Maturity	Evidence to be considered
4	Connections between system components and external connections to the organization's critical systems are identified and documented in a controlled (version and approved) way in for example a network architecture diagram. This documentation is reviewed and updated regularly. Exceptions on the level of detailing critical systems in the entity’s network architecture diagram are documented, approved and limited to less than 3% of the total number of identified critical systems.
5	Connections between system components and external connections to the organization's critical systems are identified and documented in a controlled (version and approved) way in for example a network architecture diagram. This documentation is reviewed and updated regularly. There are no exceptions on the level of detailing critical systems in the entity’s network architecture diagram.

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

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

(2) Limiting external connections to the organization's critical systems.

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	The lack of documentation on connections between system components and external connections to the organization'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 organization's critical systems are as documented in the relevant documentation, e.g. network architecture diagram. Review (e.g. audits) of what is present in the field reveals less than 10% inconsistencies with what is documented.

PR.AC-5.3 Where appropriate, network integrity of the organization's critical systems shall be protected by
(1) Identifying, documenting, and controlling connections between system components.
(2) Limiting external connections to the organization's critical systems.

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
4	Connections between system components and external connections to the organization's critical systems are as documented in the relevant documentation, e.g. network architecture diagram, and review (e.g. audits) of what is present in the field reveals less than 5% inconsistencies with what is documented. Metrics, including targets, are in place to monitor the accuracy of network visualisation to able 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.
5	Connections between system components and external connections to the organization's critical systems are as documented in the relevant documentation, e.g. network architecture diagram, and review (e.g. audits) of what is present in the field reveals less than 1% inconsistencies with what is documented. Metrics, including targets, are in place to monitor the accuracy of network visualisation to able 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. Identified network integrity risks are translated into improvement opportunities that contribute to the continuous improvement of network integrity.

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

Documentation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	There is no controlled (version controlled and approved) documentation on monitoring and controlling of connections and communications at (1) the external boundary and at (2) key internal boundaries within the organization's critical systems.
2	Controlled (version 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 organization's critical systems exists but hasn't been reviewed in the previous 2 years.
3	Controlled (version and approved) documentation (policy, process, SOP…) on the monitoring and controlling 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 controlling 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 kept to just stating the main features.

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

Documentation Maturity

IMPORTANT

Maturity	Evidence to be considered
4	Controlled (version and approved) documentation (policy, process, SOP…) on the monitoring and controlling of critical external and internal connections and communications exists; the critical network infrastructure configuration is documented and fully described. Limitations on the monitoring and controlling external and internal connections and communications to the critical systems are defined and documented; up-to-date and regularly reviewed. For less than 3% of identified limitations, the description of these limitations can be kept to just stating the main features. In line with this, the documentation reflects the critical network infrastructure configuration.
5	Controlled (version and approved) documentation (policy, process, SOP…) on the monitoring and controlling of critical external and internal connections and communications exists; the network infrastructure configuration is documented and fully described. Limitations on the monitoring and controlling external and internal connections and communications to the systems are defined and documented; up-to-date and regularly reviewed. Documentation shows the network infrastructure configuration is fully described.

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

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	Connections and communications at the external boundary and at key internal boundaries are not monitored nor 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 controlling of connections and communications at the external boundary and at key internal boundaries is implemented (incl. boundary protection devices where relevant). Evidence on process implementation is available for most activities. Reviews (e.g. audits) show less then 10% inconsistencies between what is documented and what is implemented in the field.

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

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
4	Documentation (policy, process, SOP, architecture, covered critical business areas…) on the monitoring and controlling of the critical external and internal connections and communications (incl. boundary protection devices where relevant) is implemented and measurable. Minimal targets for process performance have been established. Evidence on process implementation is available for all activities. Reviews (e.g. audits) show less then 5% inconsistencies between what is documented and what is implemented in the field. Status is reported as established in appropriate process documentation.
5	Documentation (policy, process, SOP, architecture, covered critical business areas…) on the monitoring and controlling of the critical external and internal connections and communications (incl. boundary protection devices where relevant) is implemented and measurable. Minimal targets for process performance have been established. Evidence on process implementation is available for all activities. Reviews (e.g. audits) show less then 1% inconsistencies between what is documented and what is implemented in the field. 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.AC-7.1 The organization shall perform a documented risk assessment on organization's critical system transactions and authenticate users, devices, and other assets commensurate with the risk of the transaction.

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	There is no controlled (version-controlled and approved) risk assessments, nor related process documentation, of business-critical system transactions and 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, of business-critical system transactions and verification of users, devices and other assets in proportion to the risk of the transaction are available, but haven't been reviewed in the previous 2 years.
3	The organisation has regularly reviewed documented risk assessments, supported by related process documentation, available 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.

PR.AC-7.1 The organization shall perform a documented risk assessment on organization's critical system transactions and authenticate users, devices, and other assets commensurate with the risk of the transaction.

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	The organisation has regularly reviewed documented risk assessments, supported by related process documentation, available 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 has regularly reviewed documented risk assessments, supported by related process documentation, available 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.

PR.AC-7.1 The organization shall perform a documented risk assessment on organization's critical system transactions and authenticate users, devices, and other assets commensurate with the risk of the transaction.

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	No risk assessments for business-critical system transactions and verification of users, devices and other assets, are done, nor is there a process that would mandate this.
2	Risk assessments for business-critical system transactions and verification of users, devices and other assets are conducted ad hoc without a well-defined strategy.
3	Documentation (policy, process, SOP,…) on the performance of risk assessments is implemented and results in risk assessments for business-critical system transactions and verification of users, devices and other assets. Evidence on process implementation is available for most activities. Reviews (e.g. audits) show less then 10% inconsistencies between what is documented and what is implemented in the field.

PR.AC-7.1 The organization shall perform a documented risk assessment on organization's critical system transactions and authenticate users, devices, and other assets commensurate with the risk of the transaction.

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	Documentation (policy, process, SOP,…) on the performance of risk assessments is implemented and results in risk assessments for business-critical system transactions and 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 on process implementation is available for all activities. Reviews (e.g. audits) show less then 5% inconsistencies between what is documented and what is implemented in the field. Minimal process performance targets are established. Process performance is measured and reported.

PR.AC-7.1 The organization shall perform a documented risk assessment on organization's critical system transactions and authenticate users, devices, and other assets commensurate with the risk of the transaction.

Implementation Maturity

ESSENTIAL

Maturity	**Evidence to be considered**
5	Documentation (policy, process, SOP,…) on the performance of risk assessments is implemented and results in risk assessments for business-critical system transactions and 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 on process implementation is available for all activities. Reviews (e.g. audits) show less then 1% inconsistencies between what is documented and what is implemented in the field. Minimal process performance targets are established. Process performance is measured, reported and continually improving.

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

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	There is no controlled (version-controlled and approved) documented capacity planning process that ensures adequate resources for organization'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 organization's critical system information processing, networking, telecommunications, and data storage, which, however, have not been reviewed in the past 2 years.
3	There is a controlled (version controlled and approved) regularly reviewed and up-to-date documented capacity planning process that ensures adequate resources for organization's critical system information processing, networking, telecommunications, and data storage. For less than 5% of the critical assets (system information processing, networking, telecommunications, data storage) exceptions on capacity planning are allowed. This is documented and approved.
4	There is a controlled (version controlled and approved) regularly reviewed and up-to-date documented capacity planning process that ensures adequate resources for organization's critical system information processing, networking, telecommunications, and data storage. For less than 3% of the critical assets (system information processing, networking, telecommunications, data storage) exceptions on capacity planning are allowed. This is documented and approved.
5	There is a controlled (version controlled and approved) regularly reviewed and up-to-date documented capacity planning process that ensures adequate resources for organization's critical system information processing, networking, telecommunications, and data storage. There are no exceptions on critical assets (system information processing, networking, telecommunications, data storage) where capacity planning is not foreseen.

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

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	There is no controlled (version checked and approved) capacity planning process created nor implemented.
2	Capacity planning ensuring adequate resources for organization's critical system information processing, networking, telecommunications, and data storage is done on an ad hoc and informal basis.
3	Capacity planning ensuring adequate resources for organization'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) reveal in less than 10% of the cases inconsistencies between documentation and reality.

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

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
4	Capacity planning ensuring adequate resources for organization's critical system information processing, networking, telecommunications, and data storage is implemented as documented. Evidence on process implementation is available for all activities. Reviews (e.g. audits) reveal in less than 5% of the cases inconsistencies between planned capacity and real needs. Metrics have been deployed and minimal targets on process performance identified. Process performance is reported as described in the applicable process documentation.
5	Capacity planning ensuring adequate resources for organization's critical system information processing, networking, telecommunications, and data storage is implemented as documented. Evidence on process implementation is available for all activities. Reviews (e.g. audits) reveal inconsistencies between planned capacity and real needs in less than 1% of the cases. Identified inconsistencies lead to improvement actions that contribute to continuous process improvement. Process performance is reported as described in the applicable process documentation.

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

Documentation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	The process to appropriate actions when unauthorized access and activities is detected, is not documented or not formally approved by management.
2	Controlled process documentation (version control, approved) exists that frame the taking of appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorized access and activities, including data leakage, but this documentation hasn’t been reviewed in the past 2 years.
3	Controlled process documentation (version control, approved) exists to make sure that appropriate actions are taken when unauthorized access and activities, including data leakage, happen. Exceptions on the monitoring of its critical systems at external borders and critical internal points are documented, approved and limited to less than 5% of the total of the organization’s critical systems at external borders and critical internal points.
4	Controlled process documentation (version control, approved) exists to make sure that appropriate actions are taken when unauthorized access and activities, including data leakage, happen. Exceptions on the monitoring of its critical systems at external borders and critical internal points are documented, approved and limited to less than 3% of the total of the organization’s critical systems at external borders and critical internal points.
5	Controlled process documentation (version control, approved) exists to make sure that appropriate actions are taken when unauthorized access and activities, including data leakage, happen. Exceptions on 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 quasi no exceptions) of the total of the organization’s critical systems at external borders and critical internal points.

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

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	There are no usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization’s critical systems environment.
2	Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization’s critical systems environment are implemented on an ad hoc basis and managed informally.
3	The organization takes appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorized access and activities, including data leakage, is detected as documented in the relevant documentation. Evidence is available for most activities. Review (e.g. through audits) reveals less than 10% cases of unauthorized access and activities that are inconsistently handled in comparison with what is prescribed in the process documentation.

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

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
4	The organization takes appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorized access and activities, including data leakage, is detected as documented in the relevant documentation. Evidence is available for all activities. Review (e.g. through audits) reveals less than 5% cases of unauthorized access and activities that are inconsistently handled in comparison with what is prescribed in the process documentation. Detailed metrics of the process, for which minimal targets for metrics have been established, are captured and reported.
5	The organization takes appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorized access and activities, including data leakage, is detected as documented in the relevant documentation. Evidence is available for all activities. Review (e.g. through audits) reveals less than 1% cases of unauthorized access and activities that are inconsistently handled in comparison with what is prescribed in the process documentation. Detailed metrics of the process, for which minimal targets for metrics have been established, are captured, reported, and show continuous improvement of process performance.

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

Documentation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	The organisation has no process documentation, or a by management approved documentation, how to establish and maintain a configuration baseline for the its business-critical systems.
2	The organisation has a controlled process documentation (version controlled and approved) on how to establish and maintain a configuration baseline for the 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)on how to establish and maintain a configuration baseline for the its business-critical systems. For less than 5% of the business-critical systems there is a documented and approved exception for the reason 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.), 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…).

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

Documentation Maturity

IMPORTANT

Maturity	Evidence to be considered
4	The organisation has a controlled process documentation (version controlled and approved)on how to establish and maintain a configuration baseline for the its business-critical systems. For less than 3% of the business-critical systems there is a documented and approved exception for the reason 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.), 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…).
5	The organisation has a controlled process documentation (version controlled and approved)on how to establish and maintain a configuration baseline for the its business-critical systems. For less than 0,5% (which practically comes on no exceptions) of the business-critical systems there is a documented and approved exception for the reason why the configuration information does not exist or is incomplete.

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

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	There is no baseline configuration for the organisation’s business-critical systems identified nor 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	Baseline configuration for the organisation’s business-critical systems is identified and maintained on an ad hoc basis and managed informally.
3	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. through audits) show that for less than 10% of the business-critical systems, the baseline configuration deviates from reality.
4	Baseline configuration for the organisation’s business-critical systems is identified and maintained. Evidence is available for all activities. Reviews (e.g. through 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 minimal targets for metrics have been established, are captured and reported.
5	Baseline configuration for the organisation’s business-critical systems is identified and maintained. Evidence is available for all activities. Reviews (e.g. through 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 minimal targets for metrics have been established, are captured, reported, and show continuous improvement of process performance.

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

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

BASIC

Maturity	Evidence to be considered
1	No controlled (version controlled and approved) documentation exists to ensure that backups for organization's business-critical data are performed and stored on a system different from the device on which the original data resides.
2	Controlled (version controlled and approved) documentation exists to ensure that backups for organization's business-critical data are performed and stored on a system different from the device on which the original data resides, but this documentation hasn't been reviewed in the previous 2 years.
3	Controlled (version and approved) documentation that ensures that backups for business-critical data of the organisation are performed and stored on another system is available and up to date. Process is applicable for more than 95% of the organization's business critical data; exceptions are documented and approved.
4	Controlled (version and approved) documentation that ensures that backups for business-critical data of the organisation are performed and stored on another system is available, regularly reviewed and updated. The back-up process documentation prescribes applicability for more than 97% of the organization's business critical data; exceptions are documented and approved.
5	Controlled (version and approved) documentation that ensures that backups for business-critical data of the organisation are performed and stored on another system is available, regularly reviewed and updated. The back-up process documentation prescribes applicability for more than 99,5% of the organization's business critical data; exceptions are documented and approved.

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
1	There is no process implemented to ensure that backups for organization's business-critical data are performed and stored on a system different from the device on which the original data resides.
2	Backup of business-critical data of the organisation is demonstrable. Back-ups are taken and stored on a system different from the device on which the original data resides on an ad-hoc basis and informally managed.
3	Back-ups of organization's business-critical data and storage on a system different from the device on which the original data resides are done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of the implemented process reveals less than 10% failed back-up jobs.

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
4	Back-ups of organization's business-critical data and storage on a system different from the device on which the original data resides are done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of the implemented process reveals less than 5% failed back-up jobs. Metrics, including targets, are in place to monitor the process. Process performance is reported as described in the applicable process documentation.
5	Back-ups of organization's business-critical data and storage on a system different from the device on which the original data resides are done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of the implemented process reveals less than 1% failed back-up jobs. Metrics, including targets, are in place to monitor the process. Process performance results are translated in process improvements. Process performance is reported as described in the applicable process documentation.

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

BASIC

Documentation Maturity

Maturity	Evidence to be considered
1	Critical system components and operating systems that are essential for the performance of the business (both production as services) are not defined nor is there a controlled (version controlled and approved) patching process in place.
2	Critical system components and operating systems that are essential for the performance of the business (both production as services) are defined and a patching process has been put in place in a controlled manner (formally approved and under version control), though this documentation and/or the patching process are outdated (e.g. not reviewed in the previous 2 years).
3	Critical system components and operating systems that are essential for the performance of the business (both production as services) are defined and a patching process has been put in place in a controlled manner (formally approved and under version control). Documentation is regularly reviewed (e.g. yearly or earlier when needed). Exemptions to the patch management schedule are documented and limited to those cases that can be operationally explained.

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

BASIC

Documentation Maturity

Maturity	Evidence to be considered
4	Critical system components, operating systems and a patching process are formally documented and regularly reviewed, including a reporting mechanism. Exemptions and exceptions to the patch management schedule are documented and limited to those cases that can be operationally explained; the patch management schedule includes priority for critical- and security patches.
5	Critical system components, operating systems and a patching process are formally documented and regularly reviewed, including a reporting mechanism. Exemptions to the patch management schedule are documented, limited to those cases that can be operationally explained and prioritizing critical- and security patches. Exemptions and exceptions are limited to a minimum by using documented patch management tools (e.g. vendor supported scanning tools) .

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

BASIC

Implementation Maturity

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

PR.MA-1.5 The organization shall prevent the unauthorized removal of maintenance equipment containing organization's critical system information.

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	No controlled (version controlled and approved) documentation on preventing the unauthorized removal of maintenance equipment containing critical system information exists.
2	Controlled (version and approved) documentation (policy, process, SOP…) on preventing the unauthorized removal of maintenance equipment containing critical system information is available but hasn't been reviewed in the previous 2 years.
3	Controlled (version and approved) documentation (policy, process, SOP…) on preventing the unauthorized removal of maintenance equipment containing critical system information is available and regularly reviewed. Controlled (version and approved) documentation (policy, process, SOP…) of situations where maintenance equipment containing critical system information may be removed without prior authorisation is limited to less than 5% of identified cases.

PR.MA-1.5 The organization shall prevent the unauthorized removal of maintenance equipment containing organization's critical system information.

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	Controlled (version and approved) documentation (policy, process, SOP…) on preventing the unauthorized removal of maintenance equipment containing critical system information is available and regularly reviewed. Controlled (version and approved) documentation (policy, process, SOP…) of situations where 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 unauthorized removal of maintenance equipment containing critical system information is available and regularly reviewed. There are no situations where maintenance equipment containing critical system information may be removed without prior authorisation.

PR.MA-1.5 The organization shall prevent the unauthorized removal of maintenance equipment containing organization's critical system information.

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	Unauthorized removal of maintenance equipment containing organization's critical system information is not prevented.
2	Unauthorized removal of maintenance equipment containing organization's critical system information is prevented informally and on an ad hoc basis. The practices are not covered by a standard organisation-wide policy.
3	Formal process for preventing the unauthorized removal of maintenance equipment containing critical system information is present and implemented. Evidence is available for most activities. Regular reviews (e.g. audits) show less then 10% inconsistencies between what is documented and what is implemented in the field.

PR.MA-1.5 The organization shall prevent the unauthorized removal of maintenance equipment containing organization's critical system information.

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	Unauthorized removal of maintenance equipment containing organization's critical system information is prevented formally through the implementation of the respective process. Evidence is available for all activities. Regular reviews (e.g. audits) show less then 5% inconsistencies between what is documented and what is implemented in the field. Minimal process performance targets are established. Process performance is measured and reported.
5	Unauthorized removal of maintenance equipment containing organization's critical system information is prevented formally through the implementation of the respective process. Evidence is available for all activities. Regular reviews (e.g. audits) show less then 1% inconsistencies between what is documented and what is implemented in the field. Minimal 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 organization's systems.

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	There is no process documentation or formally approved documentation by management ensuring that maintenance tools and portable storage devices are inspected when 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.
2	Controlled (versioned, approved) process documentation ensuring that maintenance tools and portable storage devices 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 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 protected by anti-malware solutions so that they are scanned for malicious code before being used on the organisation's systems, and this 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 over a predefined period.

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

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
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 this 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 over a predefined period.
5	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 this 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 over a predefined period.

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

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	There is no standard process ensuring that maintenance tools and portable storage devices are inspected when 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.
2	Maintenance tools and portable storage devices are ad hoc inspected when they enter the facility and ad hoc protected by anti-malware solutions so that they are scanned for malicious code before being used on the organisation's systems. This is all 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 exist and is implemented. Evidence is available for most maintenance tools and portable storage devices that enter the organisation over a predefined period. Regular reviews (e.g. audits) show less then 10% inconsistencies between what is documented, including the exceptions, and what is implemented.

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

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
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 exist 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 less then 5% inconsistencies between what is documented, including the exceptions, and what is implemented. Detailed process performance metrics, including minimal 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 exist 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 less then 1% inconsistencies between what is documented, including the exceptions, and what is implemented. Detailed process performance metrics, including minimal process performance targets, are measured, reported and show continuous improvement.

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

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	There is no process documentation or formally approved documentation by management that ensures that security controls are carried out after hardware and software maintenance, or repairs/patching and appropriate actions are taken consequently.
2	Controlled (versioned, approved) process documentation ensuring that security checks after hardware and software maintenance or repairs/patching are carried out with the required actions as a consequence exists, but has not been reviewed in the past 2 years.
3	Controlled (versioned, approved) process documentation exists to ensure that security checks after hardware and software maintenance or repairs/patching are carried out with the required actions as a consequence, and this 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 hardware and software maintenance or repairs/patching over a predefined period.

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

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	Controlled (versioned, approved) process documentation exists to ensure that security checks after hardware and software maintenance or repairs/patching are carried out with the required actions as a consequence, and this 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 hardware and software maintenance or repairs/patching over a predefined period.
5	Controlled (versioned, approved) process documentation exists to ensure that security checks after hardware and software maintenance or repairs/patching are carried out with the required actions as a consequence, and this 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 hardware and software maintenance or repairs/patching over a predefined period.

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

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	There is no standard process ensuring that security controls are carried out after hardware and software maintenance and repairs/patching and appropriate actions are taken consequently.
2	Security controls are carried out ad hoc after hardware and software maintenance and repairs/patching and appropriate actions are taken ad hoc. This is all managed informally.
3	A formal process exist and is implemented to carry out security controls after hardware and software maintenance, or repairs/patching and appropriate actions are taken as a result of these controls. Evidence is available for most hardware and software maintenance and repairs/patching over a predefined period. Regular reviews (e.g. audits) show less then 10% inconsistencies between what is documented, including the exceptions, and what is implemented.

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

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	A formal process exist and is implemented to carry out security controls after hardware and software maintenance, or repairs/patching and appropriate actions are taken as a result of these controls. Evidence is available for all hardware and software maintenance and repairs/patching over a predefined period. Regular reviews (e.g. audits) show less then 5% inconsistencies between what is documented, including the exceptions, and what is implemented. Detailed process performance metrics, including minimal process performance targets, are measured and reported.
5	A formal process exist and is implemented to carry out security controls after hardware and software maintenance, or repairs/patching and appropriate actions are taken as a result of these controls. Evidence is available for all hardware and software maintenance and repairs/patching over a predefined period. Regular reviews (e.g. audits) show less then 1% inconsistencies between what is documented, including the exceptions, and what is implemented. Detailed process performance metrics, including minimal process performance targets, are measured, reported and show continuous improvement.

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

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

BASIC

Maturity	Evidence to be considered
1	No controlled (version controlled and approved) documentation exists to identify the types of logs (non-exhaustive list: Audit Logs, Event Logs, Application Logs, Security Logs, System Logs, Maintenance Logs) that are enabled, documented and reviewed.
2	Controlled (version controlled and approved) documentation exists to identify the types of logs that are enabled, documented and reviewed, but this documentation hasn't been reviewed in the previous 2 years.
3	Controlled (version and approved) documentation that identifies the logs that the organisation has enabled is available, regularly reviewed and updated. Exceptions on the enabling of logging, where it is identified the logging should be enabled, are documented and approved and may not exceed more than 4% of the total of logs the entity has identified to maintain.

NEW IN THIS VERSION

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

Documentation Maturity

BASIC

Maturity	Evidence to be considered
4	Controlled (version and approved) documentation that identifies the logs that the organisation has enabled is available, regularly reviewed and updated. Exceptions on the enabling of logging, where it is identified the logging should be enabled, are documented and approved and may not exceed more than 2% of the total of logs the entity has identified to maintain.
5	Controlled (version and approved) documentation that identifies the logs that the organisation has enabled is available, regularly reviewed and updated. Exceptions on the enabling of logging, where it is identified the logging should be enabled, are documented and approved and may not exceed more than 0,5% of the total of logs the entity has identified to maintain.

NEW IN THIS VERSION

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
1	Logging identified in the documentation is not enabled in the entity.
2	Logging identified in the documentation is deployed, the review of the logs is done on an ad hoc basis and is managed informally.
3	Logging functionalities are enabled, and logs are reviewed on a frequency as documented in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of the implemented process reveals less than 10% inconsistencies between what is documented and what is implemented in the field.

NEW IN THIS VERSION

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
4	Logging functionalities are enabled, and logs are reviewed on a frequency as documented in the relevant process documentation, and the review of the logs is done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) show less then 5% cases where the process is not followed. Metrics, including targets, are in place to monitor the process. Process performance is reported as described in the applicable process documentation.

NEW IN THIS VERSION

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

Implementation Maturity

BASIC

Maturity	Evidence to be considered
5	Logging functionalities are enabled, and logs are reviewed on a frequency as documented in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) show less then 1% cases where the process is not followed. Metrics, including targets, are in place to monitor the process. Process performance results are translated in opportunities for improvement. Process performance is reported as described in the applicable process documentation.

NEW IN THIS VERSION

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

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	There is no process documentation or formally approved documentation by management that ensures that portable storage devices containing system data are controlled and protected while in transit and in storage.
2	Controlled (versioned, approved) process documentation ensuring that portable storage devices containing system data are controlled and protected while in transit and in storage exists, but has not been reviewed in the past 2 years.
3	Controlled (versioned, approved) process documentation ensuring that portable storage devices containing system data are controlled and protected while in transit and in storage exists, and this documentation is reviewed regularly. Portable storage devices containing system data that are in transit and in storage are known and exceptions on 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 and in storage over a predefined period.

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

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	Controlled (versioned, approved) process documentation ensuring that portable storage devices containing system data are controlled and protected while in transit and in storage exists, and this documentation is reviewed regularly. Portable storage devices containing system data that are in transit and in storage are known and exceptions on 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 and in storage over a predefined period.
5	Controlled (versioned, approved) process documentation ensuring that portable storage devices containing system data are controlled and protected while in transit and in storage exists, and this documentation is reviewed regularly. Portable storage devices containing system data that are in transit and in storage are known and exceptions on 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 and in storage over a predefined period.

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

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	There is no standard process ensuring that portable storage devices containing system data are controlled and protected while in transit and in storage.
2	Control and protection of portable storage devices containing system data while in transit and in storage is carried out ad hoc and managed informally.
3	A formal process exist and is implemented to control and protect portable storage devices containing system data while in transit and in storage. Evidence is available for most portable storage devices containing system data over a predefined period. Regular reviews (e.g. audits) show less then 10% inconsistencies between what is documented, including the exceptions, and what is implemented.

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

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	A formal process exist and is implemented to control and protect portable storage devices containing system data while in transit and in storage. Evidence is available for all portable storage devices containing system data over a predefined period. Regular reviews (e.g. audits) show less then 5% inconsistencies between what is documented, including the exceptions, and what is implemented. Detailed process performance metrics, including minimal process performance targets, are measured and reported.
5	A formal process exist and is implemented to control and protect portable storage devices containing system data while in transit and in storage. Evidence is available for all portable storage devices containing system data over a predefined period. Regular reviews (e.g. audits) show less then 1% inconsistencies between what is documented, including the exceptions, and what is implemented. Detailed process performance metrics, including minimal process performance targets, are measured and reported and show continuous improvement.

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

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	There is no process documentation or formally approved documentation by management that ensures 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 ensuring 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 ensuring that a baseline of network operations and expected data flows for the critical systems is developed, documented and maintained to track events exists, and this documentation is reviewed regularly. For less than 5% of the critical systems exceptions on the baseline (development, depth of documentation and maintenance) are allowed, documented and approved.

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

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	Controlled (versioned, approved) process documentation ensuring that a baseline of network operations and expected data flows for the critical systems is developed, documented and maintained to track events exists, and this documentation is reviewed regularly. For less than 3% of the critical systems exceptions on the baseline (development, depth of documentation and maintenance) are allowed, documented and approved.
5	Controlled (versioned, approved) process documentation ensuring that a baseline of network operations and expected data flows for the critical systems is developed, documented and maintained to track events exists, and this documentation is reviewed regularly. For less than 0,5% (which practically amounts to no exceptions) of the critical systems exceptions on the baseline (development, depth of documentation and maintenance) are allowed, documented and approved.

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

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	There is no standard process ensuring 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 exist and is implemented to develop, document and maintain a baseline of network operations and expected data flows for the critical systems so events can be tracked. Evidence is available for most critical systems. Regular reviews (e.g. audits) show less then 10% events over a predefined period that cannot be tracked because of inconsistent baselines (e.g. incomplete logging, logs that contain insufficient information).

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

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	A formal process exist and is implemented to develop, document and maintain a baseline of network operations and expected data flows for the critical systems so events can be tracked. Evidence is available for all critical systems. Regular reviews (e.g. audits) show less then 5% events over a predefined period that cannot be tracked because of inconsistent baselines (e.g. incomplete logging, logs that contain insufficient information). Detailed process performance metrics, including minimal process performance targets, are measured and reported.
5	A formal process exist and is implemented to develop, document and maintain a baseline of network operations and expected data flows for the critical systems so events can be tracked. Evidence is available for all critical systems. Regular reviews (e.g. audits) show less then 1% events over a predefined period that cannot be tracked because of inconsistent baselines (e.g. incomplete logging, logs that contain insufficient information). Detailed process performance metrics, including minimal process performance targets, are measured and reported and show continuous improvement.

DE.AE-3.1 The activity logging functionality of protection / detection hardware or software shall be enabled, backed-up and reviewed.

Documentation Maturity

BASIC

Maturity	Evidence to be considered
1	No controlled (version controlled and approved) documentation exists to ensure that activity logging is enabled, backed-up and reviewed.
2	Controlled (version controlled and approved) documentation exists to ensure that activity logging is enabled, backed-up and reviewed, but this documentation hasn't been reviewed in the previous 2 years.
3	Controlled (version and approved) documentation that ensures that activity logging is enabled, backed-up and reviewed is available and up-to-date. Exceptions on the enabling and back-up of activity logging and review of the logs are documented and approved and may not exceed more than 4% of the total of protection/detection hardware and software deployed in the entity.

DE.AE-3.1 The activity logging functionality of protection / detection hardware or software shall be enabled, backed-up and reviewed.

Documentation Maturity

BASIC

Maturity	Evidence to be considered
4	Controlled (version and approved) documentation that ensures that activity logging is enabled, documented and reviewed is available, regularly reviewed and updated. Exceptions on the enabling and back-up of activity logging and review of the logs are documented and approved and may not exceed more than 2% of the total of protection/detection hardware and software deployed in the entity.
5	Controlled (version and approved) documentation that ensures that activity logging is enabled, documented and reviewed is available, regularly reviewed and updated. Exceptions on the enabling and back-up of activity logging and review of the logs are documented and approved and are limited to less than 0,5% of the total of protection/detection hardware and software deployed in the entity.

DE.AE-3.1 The activity logging functionality of protection / detection hardware or software shall be enabled, backed-up and reviewed.

Implementation Maturity

BASIC

Maturity	Evidence to be considered
1	Activity logging is not enabled for any of the protection/detection hardware and software deployed in the entity.
2	The enabling of the activity logging functionality of the protection/detection hardware and software deployed in the entity, the back-up and review of the logs is done on an ad hoc basis and is managed informally.
3	The enabling of the activity logging functionality of the protection/detection hardware and software deployed in the entity, the back-up and review of the logs is done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of the implemented process reveals less than 10% inconsistencies between what is documented and what is implemented in the field.

DE.AE-3.1 The activity logging functionality of protection / detection hardware or software shall be enabled, backed-up and reviewed.

Implementation Maturity

BASIC

Maturity	Evidence to be considered
4	The enabling of the activity logging functionality of the protection/detection hardware and software deployed in the entity, the back-up and review of the logs is done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) show less then 5% cases where the process is not followed. Metrics, including targets, are in place to monitor the process. Process performance is reported as described in the applicable process documentation.

DE.AE-3.1 The activity logging functionality of protection / detection hardware or software shall be enabled, backed-up and reviewed.

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

BASIC

Maturity	Evidence to be considered
5	The enabling of the activity logging functionality of the protection/detection hardware and software deployed in the entity, the back-up and review of the logs is done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits)show less then 1% cases where the process is not followed. Metrics, including targets, are in place to monitor the process. Process performance results are translated in opportunities for improvement. Process performance is reported as described in the applicable process documentation.

DE.AE-4.1 Negative impacts to organization’s operations, assets, and individuals resulting from detected events shall be determined and correlated with risk assessment outcomes.

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	There is no controlled (version-controlled and approved) documented process that ensures that negative impacts to organization’s operations, assets, and individuals resulting from detected events are determined and correlated with risk assessment outcomes.
2	There is a controlled (version controlled and approved) documented process on the communication of recovery activities to predefined stakeholders, executive and management teams, which, however, have not been reviewed in the past 2 years.
3	There is a controlled (version-controlled and approved) documented process that ensures that negative impacts to organization’s operations, assets, and individuals resulting from detected events are determined and correlated with risk assessment outcomes. The process does allow exceptions on what negative impacts from detected events don’t have to be determined and thus 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 that ensures that negative impacts to organization’s operations, assets, and individuals resulting from detected events are determined and correlated with risk assessment outcomes. The process does allow exceptions on what negative impacts don’t have to be determined and thus 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 that ensures that negative impacts to organization’s operations, assets, and individuals resulting from detected events are determined and correlated with risk assessment outcomes. The process doesn’t allow exceptions.

DE.AE-4.1 Negative impacts to organization’s operations, assets, and individuals resulting from detected events shall be determined and correlated with risk assessment outcomes.

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	Negative impacts to organization’s operations, assets, and individuals resulting from detected events are not determined and thus not correlated with risk assessment outcomes..
2	Negative impacts to organization’s operations, assets, and individuals resulting from detected events are determined and correlated with risk assessment outcomes on an ad hoc basis and informally managed.
3	Negative impacts to organization’s operations, assets, and individuals resulting from detected events are determined and correlated with risk assessment outcomes as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits, exercises) of the implemented process reveal less than 10% inconsistencies between what is documented and reality.

DE.AE-4.1 Negative impacts to organization’s operations, assets, and individuals resulting from detected events shall be determined and correlated with risk assessment outcomes.

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	Negative impacts to organization’s operations, assets, and individuals resulting from detected events are determined and correlated with risk assessment outcomes as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) of the implemented process reveal less than 5% inconsistencies between what is documented and reality. Metrics, including targets, are in place to monitor the process. Process performance is reported as described in the applicable process documentation.
5	Negative impacts to organization’s operations, assets, and individuals resulting from detected events are determined and correlated with risk assessment outcomes as specified in the relevant process documentation. Evidence on process implementation is available for all activities. Reviews (e.g. audits) of the implemented process reveal less than 1% inconsistencies between what is documented and reality. Metrics, including targets, are in place to monitor the process. Process performance results are translated in process improvements. Process performance is reported as described in the applicable process documentation.

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

Documentation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	No controlled (version controlled and approved) documentation on monitoring and identifying unauthorized use of business-critical systems through the detection of unauthorized local connections, network connections and remote connections exists.
2	Controlled (version and approved) documentation (policy, process, SOP…) on monitoring and identifying unauthorized use of business-critical systems through the detection of unauthorized local connections, network connections and remote connections exists, hasn't been reviewed in the previous 2 years.
3	Controlled (version and approved) documentation (policy, process, SOP…) on monitoring and identifying unauthorized use of business-critical systems through the detection of unauthorized local connections, network connections and remote connections exists and is regularly reviewed. Exceptions on the monitoring and identifying of unauthorized use of business-critical systems are documented, approved and limited to less than 5% of the business-critical systems.

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

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

IMPORTANT

Maturity	Evidence to be considered
4	Controlled (version and approved) documentation (policy, process, SOP…) on monitoring and identifying unauthorized use of business-critical systems through the detection of unauthorized local connections, network connections and remote connections exists, is up-to-date and regularly reviewed. Exceptions on the monitoring and identifying of unauthorized use of business-critical systems are documented, approved and limited to less than 3% of the business-critical systems.
5	Controlled (version and approved) documentation (policy, process, SOP…) on monitoring and identifying unauthorized use of business-critical systems through the detection of unauthorized local connections, network connections and remote connections exists for all business-critical systems, is up-to-date and regularly reviewed. Eventual exceptions are kept to a strict minimum (less than 0,5% of the business-critical systems) and are documented and approved.

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

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	The organization doesn’t monitor nor identifies unauthorized use of its business-critical systems.
2	The organization monitors and identifies unauthorized use of its business-critical systems through the detection of unauthorized local connections, network connections and remote connections on an ad hoc basis but without a supporting policy.
3	The organization performs the monitoring and identifying of unauthorized use of its business-critical systems through the detection of unauthorized local connections, network connections and remote connections as documented in policies, processes, SOPs etc.). Evidence on process implementation is available for most activities. Reviews (e.g. audits) show less then 10% inconsistencies between what is documented and what is implemented in the field.

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

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
4	The organization performs the monitoring and identifying of unauthorized use of its business-critical systems through the detection of unauthorized local connections, network connections and remote connections as documented in policies, processes, SOPs etc.). Evidence on process implementation is available for all activities. Reviews (e.g. audits) show less then 5% inconsistencies between what is documented and what is implemented in the field. Minimal process performance targets are established. Process performance is measured and reported.
5	The organization performs the monitoring and identifying of unauthorized use of its business-critical systems through the detection of unauthorized local connections, network connections and remote connections as documented in policies, processes, SOPs etc.). Evidence on process implementation is available for all activities. Reviews (e.g. audits) show less then 1% inconsistencies between what is documented and what is implemented in the field. Minimal process performance targets are established. Process performance is measured, reported and continually improving.

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

BASIC

Documentation Maturity

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

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

CENTRE FOR CYBERSECURITY BELGIUM

BASIC

Implementation Maturity

Maturity	Evidence to be considered
1	No malware protection policy nor process is in place.
2	A process to manage malware protection is applied on an ad hoc basis without a clear definition on responsibilities and authorities.
3	The malware protection process is rolled out as documented. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of the malware protection process reveal less than 10% cases where the process is not followed (e.g. endpoints where the malware protection is not up to date).
4	The malware protection process is rolled out as documented. Evidence on process implementation is available for all activities. Reviews (e.g. audits) of the malware protection process reveal less than 5% cases where the process is not followed. Metrics, including targets, are in place to monitor the implementation of the malware protection process. Performance of malware protection is reported as described in the malware protection process.
5	The malware protection process is rolled out as documented. Evidence on process implementation is available for all activities. Reviews (e.g. audits) of the malware protection process reveal less than 1% cases where the process is not followed. Metrics, including targets, are in place to monitor the implementation of the malware protection process. Malware protection monitoring (e.g. analysis of effectiveness of malware protection) is translated in opportunities for improvement. Performance of malware protection is reported as described in the malware protection process.

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

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

IMPORTANT

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, are 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, are incorporated into the detection process, but it hasn’t 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, are incorporated into the detection process. The process does not consider all improvements that facilitate the continuous improvement of the detection process (e.g. test results, lessons learned… are not considered). The reason for exclusion of improvements 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, are incorporated into the detection process. The process does not consider lessons learned as a source for improvements that are to be incorporated in the detection process revisions. 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, are incorporated into the detection process. The documented process does consider all improvements derived from the monitoring, measurement, assessment, testing, review, and lessons learned.

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

Implementation Maturity

IMPORTANT

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, are incorporated into the detection process.
2	The process that provides that improvements are incorporated into the detection process is implemented on an ad hoc basis and managed informally.
3	The process that provides that improvements are incorporated into the detection process is implemented, including the documented exceptions. Evidence on process implementation is available for most improvements. Reviews (e.g. audits) of the implemented process reveal less than 10% inconsistencies between the identified improvements and what is incorporated into detection process revisions.

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

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
4	The process that provides that improvements derived from the monitoring, measurement, assessment, testing, review, and lessons learned, are incorporated into the detection process, is implemented considering the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) of the implemented process reveal less than 5% inconsistencies between the identified improvements and what is incorporated into detection process revisions. 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, are incorporated into the detection process, is implemented considering the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits) of the implemented process reveal less than 1% inconsistencies between the identified improvements and what is incorporated into detection process revisions. Metrics, including targets, are in place to monitor the implementation of the process. Process performance results are translated in process improvements. Process performance is reported as described in the applicable process documentation.

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

Documentation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	No controlled (version controlled and approved) documentation regarding performing specialized assessments on the organization's critical systems exists.
2	Controlled (version and approved) documentation (policy, process, SOP…) regarding performing specialized assessments on the organization's critical systems is available but hasn't been reviewed in the previous 2 years.
3	Controlled (version and approved) documentation regarding performing specialized assessments on the organization's critical systems is available and regularly reviewed. Exceptions on the performance of specialized assessments on the organization's critical systems are documented, approved and limited to less than 5% of the total number of identified critical systems.
4	Controlled (version and approved) documentation regarding performing specialized assessments on the organization's critical systems is available and regularly reviewed. Exceptions on the performance of specialized assessments on the organization's critical systems are documented, approved and limited to less than 3% of the total number of identified critical systems.
5	Controlled (version and approved) documentation regarding performing specialized assessments on the organization's critical systems is available and regularly reviewed. There are no exceptions on the performance of specialized assessments on the organization's critical systems.

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

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
1	No specialized assessments, e.g. in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, performance/load testing, and verification and validation testing, on the organization's critical systems are performed.
2	Specialized assessments on the organization's critical systems are performed in an ad hoc and informal manner and without a clear policy or process.
3	Formal process for performing specialized assessments on the organization's critical systems is present and implemented. Evidence is available for most activities. Regular reviews (e.g. assessment reports, assessment calendar) show less then 10% inconsistencies between what is documented and what is implemented in the field.

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

CENTRE FOR CYBERSECURITY BELGIUM

Implementation Maturity

ESSENTIAL

Maturity	Evidence to be considered
4	Specialized assessments on the organization's critical systems are performed formally through the implementation of the respective process. Evidence is available for all activities. Regular reviews (e.g. assessment reports, assessment calendar) show less then 5% inconsistencies between what is documented and what is implemented in the field. Minimal process performance targets are established. Process performance is measured and reported.
5	Specialized assessments on the organization's critical systems are performed formally through the implementation of the respective process. Evidence is available for all activities. Regular reviews (e.g. assessment reports, assessment calendar) show less then 1% inconsistencies between what is documented and what is implemented in the field. Minimal process performance targets are established. Process performance is measured, reported and shows continuous improvement.

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

CENTRE FOR CYBERSECURITY BELGIUM

IMPORTANT

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. not reviewed in the previous 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.

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

CENTRE FOR CYBERSECURITY BELGIUM

IMPORTANT

Implementation Maturity

Maturity	Evidence to be considered
1	No vulnerability management policy, including processing, analysing and remedying vulnerabilities from internal and external sources, nor process is in place.
2	Vulnerability management is done ad hoc, without clear responsibilities and authorities.
3	The vulnerability management process is rolled out as documented. Evidence on process implementation is available for most activities. Reviews (e.g. audits) of the vulnerability management process reveal less than 10% cases where the process is not followed (e.g. vulnerabilities identified but not remediated as prescribes in the vulnerability management process, information from internal and/or external sources that are neglected).

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

IMPORTANT

Implementation Maturity

Maturity	Evidence to be considered
4	The vulnerability management process is rolled out as documented. Evidence on process implementation is available for all activities. Reviews (e.g. audits) of the vulnerability management process reveal less than 5% cases where the process is not followed. 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 of vulnerability management is reported as described in the vulnerability management process.
5	The vulnerability management process is rolled out as documented. Evidence on process implementation is available for all activities. Reviews (e.g. audits) of the vulnerability management process reveal less than 1% cases where the process is not followed. 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. through KPI analysis) is translated in opportunities for improvement. Performance of vulnerability management is reported as described in the vulnerability management process.

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

CENTRE FOR CYBERSECURITY BELGIUM

Documentation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	There is no controlled (version-controlled and approved) documented process that ensures that recovery activities are communicated to predefined stakeholders, executive and management teams.
2	There is a controlled (version controlled and approved) documented process on the communication of recovery activities to predefined stakeholders, executive and management teams, which, however, has not been reviewed in the past 2 years.
3	There is a controlled (version controlled and approved) regularly reviewed and up-to-date documented process on 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) regularly reviewed and up-to-date documented process on 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) regularly reviewed and up-to-date documented process on the communication of recovery activities to predefined stakeholders, executive and management teams. Communications are made to all (internal& external) stakeholders. There are no exceptions.

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

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
1	There is no communication of recovery activities to predefined stakeholders, executive and management teams.
2	Communication of recovery activities to predefined stakeholders, executive and management teams is done on an ad hoc and informal basis.
3	Communication of recovery activities to predefined stakeholders, executive and management teams is done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for most activities. Reviews (e.g. audits, exercises) of the implemented process reveal less than 10% inconsistencies between what is documented and reality.

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

Implementation Maturity

IMPORTANT

Maturity	Evidence to be considered
4	Communication of recovery activities to predefined stakeholders, executive and management teams is done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits, exercises) of the implemented process reveal less than 5% inconsistencies between what is documented and reality. Metrics, including targets, are in place to monitor the process. Process performance is reported as described in the applicable process documentation.
5	Communication of recovery activities to predefined stakeholders, executive and management teams is done as specified in the relevant process documentation, including the documented exceptions. Evidence on process implementation is available for all activities. Reviews (e.g. audits, exercises) of the implemented process reveal less than 1% inconsistencies between what is documented and reality. Metrics, including targets, are in place to monitor the process. Process performance results are translated in process improvements. Process performance is reported as described in the applicable process documentation.

CENTRE FOR
CYBERSECURITY
BELGIUM

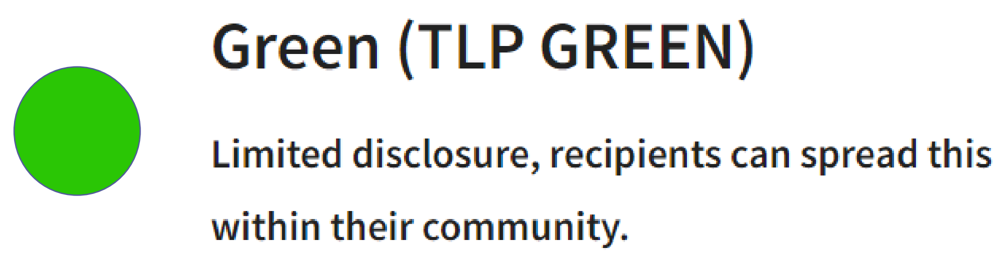
CCB Certification Authority (NCCA)
certification@ccb.belgium.be

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister
Rue de la Loi / Wetstraat 18 - 1000 Brussels
www.ccb.belgium.be

.be

What does TLP Green mean?

TRAFFIC LIGHT PROTOCOL (TLP)



🟢 **Green (TLP GREEN)**

Limited disclosure, recipients can spread this within their community.

Sources may use **TLP:GREEN** when information is useful to increase awareness within their wider community.

Recipients may share **TLP:GREEN** information with peers and partner organizations within their community, but not via publicly accessible channels (e.g. websites, LinkedIn…). **TLP:GREEN** information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.