TLP - CLEAR

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

SME Cyber Resilience Maturity Assessment Model

JULY 2026

About ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

To contact the authors, use product_security@enisa.europa.eu.
For media enquiries about this paper, use press@enisa.europa.eu.

AUTHOR

European Union Agency for Cybersecurity (ENISA)

ACKNOWLEDGEMENTS

ENISA would like to thank colleagues and reviewers whose insights contributed to the development of this model: Davide Iaccarino from Digital SME Alliance, Tudor Pitulac from OpenSky Data Systems, Bruno Banelli from NOVARQ, Sabine Dellaitre from GuardedBox and Advanced Cyber Security.

LEGAL NOTICE

Luxembourg: Publications Office of the European Union, 2026

COPYRIGHT NOTICE

ISBN 978-92-9204-799-3, DOI 10.2824/1676704, Catalogue Number TP-01-26-014-EN-N

Table of Contents

Executive summary

The Cyber Resilience Act (CRA) ([1]) introduces new cybersecurity requirements for products with digital elements placed on the EU market. With the regulation entering into application in December 2027, manufacturers, distributors and importers, including micro, small and medium-sized enterprises (SMEs), will need to ensure that their products meet cybersecurity requirements throughout the product life cycle.

Since SMEs make up a large part of the EU´s digital ecosystem, their ability to understand and implement the CRA will play an important role in the overall success of the regulation. At the same time, many smaller organisations face practical challenges related to resources, expertise, time and implementation capacity. To help address this, the European Union Agency for Cybersecurity, ENISA is working on practical guidance, tools and support activities tailored to the realities and needs of smaller organisations.

The SME Cyber Resilience Maturity Assessment Model provides a structured approach for micro, small and medium-sized enterprises ([2]) (SMEs) to evaluate and strengthen their overall cyber resilience, while taking into account the requirements of the Cyber Resilience Act (CRA).

The model is primarily intended for organisations that manufacture and place products with digital elements on the market, as these are directly subject to CRA requirements. However, it can also be used by other organisations involved in the product life cycle, such as integrators or service providers, to assess and improve their product security practices.

SMEs may not have dedicated security teams and expertise ([3]). This model is therefore designed to be simple and practical. The aim of this guidance is to help SMEs understand their current situation and identify the improvements that should be implemented first. Over time, these steps support stronger cyber resilience practices.

This model focuses on five domains:

- governance and documentation,
- risk management and security by design and by default,
- vulnerability and patch management,
- product life cycle management,
- awareness, competence and skills.

Each domain is divided into five maturity criteria that reflect expected practices under the CRA and product security approaches. By scoring their responses to questions related to each domain, SMEs

([1]) Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([2]) Commission recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

([3]) For a more general overview of cybersecurity challenges faced by SMEs, see ENISA, *Cybersecurity for SMEs – Challenges and recommendations*, 2021, https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes.

can evaluate their current practices in a structured way. The results highlight areas that are functioning well and those that may require attention. This also provides insight on whether policies and processes are not only defined, but also consistently applied in everyday operations.

The model suggests three maturity profiles: **basic**, **intermediate** and **advanced**. These profiles are intended to show how consistently product-related risks are managed in the organisation. The aim is to provide organisations with a clear view of where they stand and what they may need to address next. Although it reflects practices supporting the implementation of the CRA, having an advanced maturity level does not replace legal obligations and **should not be considered evidence of compliance**. Instead, it supports organisations in strengthening their product security and cyber resilience over time in a structured and manageable way.

Introduction

Background on the Cyber Resilience Act

Micro, small and medium-sized companies (SMEs) ([6]) make up the majority of manufacturers, distributors and importers of products with digital elements in Europe. With the Cyber Resilience Act (CRA) ([7]) entering into application in December 2027, manufacturers of products with digital elements, including SMEs, will need to ensure the cybersecurity of their products. The European Commission and the European Union Agency for Cybersecurity, ENISA, aim to support the implementation of the CRA by SMEs ([8]).

The CRA is a new EU regulation that introduces cybersecurity requirements for all products with digital elements placed on the EU market. Its aim is to ensure that software and hardware are designed securely, include proper vulnerability management and that they receive necessary security updates throughout their life cycle. The CRA affects manufacturers, importers and distributors of software and hardware products of all sizes, including SMEs.

ENISA supports the European Commission and EU Member States in strengthening cybersecurity across Europe. As part of the Commission's SME strategy on cybersecurity, ENISA provides practical guidance, tools and expertise to help smaller companies understand and meet new cybersecurity requirements, including those introduced by the CRA.

Objectives

The Model was developed to support micro, small and medium-sized enterprises (SMEs) ([4]) in systematically addressing the requirements of the Cyber Resilience Act (CRA) ([5]). Many SMEs do not operate with dedicated security teams, and responsibilities are often shared across roles. For this reason, the model has been designed for practical use in real-world scenarios, rather than as a theoretical guide.

The purpose of the model is to guide SMEs in planning their activities and thinking about product security in a structured way. It can support the implementation of security practices and provide a roadmap for improvement activities. Although the model is aligned with the main requirements of the CRA, having an advanced maturity level should not be seen as proof of compliance.

Using this model, SMEs can conduct a self-check of their cybersecurity practices, identify areas of weakness and develop plans to strengthen them. After the responses to the questions in Annex A have been scored, SMEs can see which maturity profile best matches their current level: basic, intermediate or advanced. The checklist in Annex B helps SMEs to decide which activities should be undertaken first and where improvement efforts should be directed.

([4]) Commission recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

([5]) Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

Scope, target audience and methodology

Organisations rely more and more on digital technologies, connected products and digital services to run their operations, support innovation and remain competitive ([6]). These products introduce specific cybersecurity risks, as vulnerabilities may arise from software components, third-party dependencies or design and configuration choices. If not addressed in a timely manner, such weaknesses can be exploited and affect both the organisation and its customers.

For manufacturers and organisations placing products on the market, this creates a responsibility to ensure that products are designed, developed and maintained with security in mind throughout their life cycle. Strengthening product security and cyber resilience is therefore essential to protect operations, reduce risk exposure and maintain customer trust.

This model is primarily intended for SMEs acting as manufacturers, importers or distributors of products with digital elements. It recognises that these organisations often operate with limited resources and may find it challenging to implement complex frameworks in practice.

At the same time, the model can be used by organisations of any size as a structured approach to assess and improve product security.

The CRA requires that security is considered throughout the entire product life cycle. In practice, this means that organisations should have processes in place for assessing risks, integrating the results into product development, managing vulnerabilities, maintaining necessary documentation, applying updates and reporting exploited vulnerabilities when they occur. Smaller organisations may still face challenges due to limited staff and legal expertise ([7]), which can make regulatory requirements more difficult to interpret and apply.

The model is built around five main domains: governance and documentation; risk management and security by design and by default; vulnerability and patch management; product life cycle management; and awareness, competence and skills. Each of these domains contains criteria that can be assessed across five maturity levels, ranging from informal practices to structured and regularly reviewed processes. The checklist provided helps organisations to link their self-check results from the assessment to specific actions and helps them to plan improvement activities.

([6]) Calderon-Monge, E. and Ribeiro-Soriano, D., 'The role of digitalization in business and management: A systematic literature review', *Review of Managerial Science*, Vol. 18, No 2, 2024, pp. 449–491, https://link.springer.com/article/10.1007/s11846-023-00647-8.

([7]) For a more general overview of cybersecurity challenges faced by SMEs, see ENISA, *Cybersecurity for SMEs – Challenges and recommendations*, 2021, https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes.

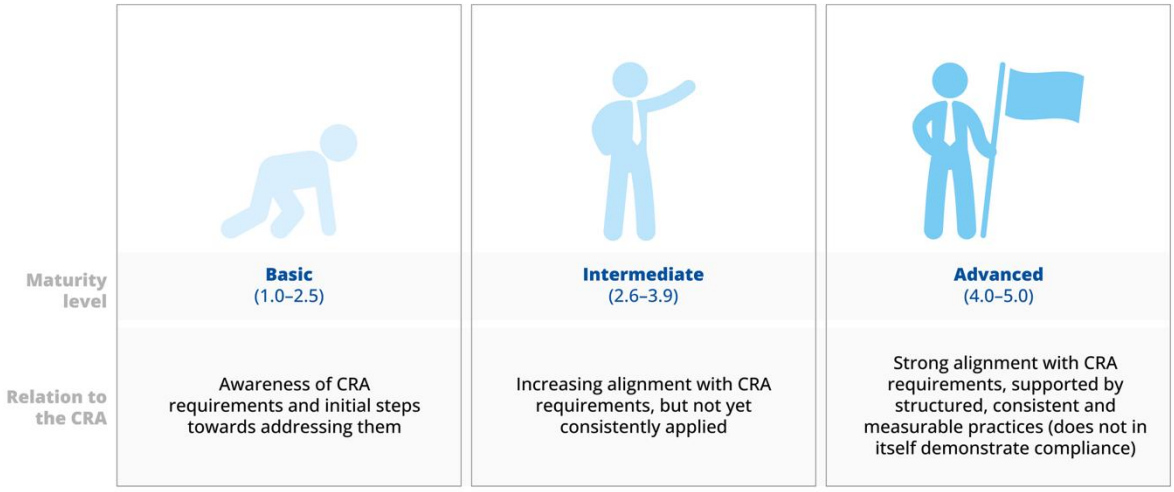

Figure 1. Maturity levels

The five domains reflect the main areas addressed by the cybersecurity requirements set out in the CRA. While they do not correspond directly to specific provisions in all cases, they support a comprehensive approach to cybersecurity across the product life cycle, rather than focusing only on individual technical measures.

Using this model helps organisations:

- identify gaps in their product security practices;
- prioritise improvements based on risk;
- prepare for regulatory requirements in a structured way.

This assessment applies to products with digital elements as defined in the CRA. Before completing the assessment, organisations should:

- Identify which of their products fall within the scope of the CRA.
- Determine the category into which each product falls (for example, default, important or critical products).
- Assess which conformity assessment procedures are applicable to the relevant products.

The level of assurance and regulatory obligations may vary depending on product classification. While this model does not distinguish between different product categories, organisations should be aware that the product type and risk level may influence which obligations apply.

The model has been developed to be practical and flexible, while recognising the capabilities of smaller organisations. It supports the gradual improvement of cybersecurity without creating unnecessary processes or administrative overheads. The model is aligned with the CRA and builds on existing ENISA maturity and assessment frameworks.

1. Model structure

SMEs can use this maturity model to carry out a self-check of their product related cybersecurity policies and practices in line with the CRA. Each criterion across the five domains is evaluated against maturity levels from 1 to 5. Scoring should be based on objective evidence such as documented procedures, implemented practices or observable behaviours rather than assumptions or informal impressions.

The goal of the self-check is not to get the highest score in every area but to gain a realistic view of the organisation's current maturity, identify gaps and make informed decisions. By reviewing results across all domains, SMEs can build an overall maturity profile and see which areas may need attention as a priority.

Five domains. The model covers five areas that can be assessed using the questionnaire in Annex A: governance and documentation, risk management and security by design and by default; vulnerability and patch management; product life cycle management; and awareness, competence and skills. Together, these areas provide a structured overview of product security practices and support organisations in assessing and improving their approach to cyber resilience.

Assessment criteria. Each domain is broken down into specific criteria that describe practices relevant to product security in the context of the CRA. These criteria help SMEs assess whether their product-security-related processes, policies and activities are in place and functioning effectively.

Maturity levels. Each criterion is scored from 1 (none or ad hoc) to 5 (governed and continuously improved). This helps organisations see how advanced their practices are, from informal or reactive to fully structured, monitored and continuously improved.

Overall maturity profile. Results are added together across all domains to provide an overall maturity profile. Organisations can then classify their maturity profile as one of the following:

- **Basic maturity.** Practices are non-existent or limited, reactive and dependent on individuals.
- **Intermediate maturity.** Foundational practices are documented but inconsistently applied.
- **Advanced maturity.** Practices are formalised, embedded, actively managed and continuously improved.

2. Domains and assessment criteria

2.1 Governance and documentation

Product security practices benefit from having structured approaches to managing cybersecurity risks, supported by clear internal responsibilities and appropriate documentation. While the CRA focuses on ensuring that products meet essential cybersecurity requirements, organisations typically need such practices to implement and demonstrate compliance with these requirements effectively. In particular, the CRA requires manufacturers to draw up technical documentation that demonstrates how products meet the essential cybersecurity requirements. Maintaining clear and consistent documentation supports this objective.

Ensuring product security starts with capturing the essential elements in written form. Maintaining documentation is not about creating unnecessary paperwork but about capturing essential practices, responsibilities and controls so that they can be consistently applied and repeated when needed. It gives a clear, consistent overview of security across the organisation, helps manage risks effectively and helps ensure that improvements can be made in a structured way.

This domain looks at how SMEs assign cybersecurity responsibilities, keep track of decisions and manage product security-related information at both the organisational and product levels. These elements form the basis of how security is managed in practice. When ownership is unclear or documentation is missing, activities tend to become inconsistent and more difficult to sustain, particularly when roles or priorities change.

In practice, governance does not need to be complex. What matters is that responsibilities are clear, records are kept and documentation stays up to date. This makes it easier to manage day-to-day work, respond to audits and meet requirements such as those set by the CRA, where being able to show what has been done is part of what is expected.

The main assessment criteria include:

- clearly defined roles and responsibilities for product security;
- management-approved cybersecurity and product security policies;
- product-level documentation describing security features, assumptions and limitations;
- defined cybersecurity expectations for suppliers and third parties;
- regular management review of cybersecurity risks and compliance status.

The maturity levels are as follows:

- **Level 1.** No defined roles, policies or documentation exist.
- **Level 2.** Roles and responsibilities are generally understood but not formally documented.
- **Level 3.** Policies and product documentation exist, but they are not always approved or used consistently.
- **Level 4.** Policies are approved, documentation is maintained, and processes are consistently followed.
- **Level 5.** Policies and processes are regularly reviewed, monitored, and continuously improved.

At the first maturity level, roles may be informal and documentation limited. At the higher levels, responsibilities are more defined, policies are documented and management reviews become routine.

2.2 Risk management and security by design and by default

This section focuses on how product security risks are considered and addressed during design and development. The CRA requires that products meet essential cybersecurity requirements, including protection against known risks and vulnerabilities. In practice, this is typically supported by identifying relevant risks and addressing them early in the product design process.

Rather than treating security as something to address later, organisations are expected to take potential risks into account from the outset. This includes considering how design choices, components and configurations may affect the overall security of the product.

For smaller organisations, this does not require complex processes. It involves ensuring that product security risks are taken into account when designing features, selecting components and making decisions that reduce exposure before the product is placed on the market.

The main assessment criteria include:

- considering product-specific cybersecurity risks;
- identifying relevant threats, misuse scenarios and potential attack surfaces;
- considering risks related to third-party components and supply chain dependencies;
- integrating security considerations into design and development activities;
- applying secure by default configurations and reducing unnecessary exposed functionality.

The maturity levels are as follows.

- **Level 1.** Security risks are not systematically considered, and secure design practices are not applied.
- **Level 2.** Security and risk considerations are addressed on an ad hoc basis, often in response to issues. Practices are informal and depend on individuals.
- **Level 3.** Risk-related and secure design practices are defined or documented but are not consistently applied across products or teams.
- **Level 4.** Security considerations are systematically integrated into product design and development. Risk-related and secure design practices are applied consistently.
- **Level 5.** Security and risk management practices are proactively monitored, regularly reviewed and continuously improved to address changing risks and organisational needs.

As organisations grow in maturity, they tend to move away from simply reacting to risks as they arise and instead adopt structured, repeatable risk management practices that are embedded in the way that they design, build and release products.

2.3 Vulnerability and patch management

The vulnerability and patch management domain looks at how an organisation identifies, manages and addresses vulnerabilities throughout a product's life cycle. The CRA requires manufacturers to ensure that known vulnerabilities are addressed, and to identify and fix vulnerabilities by providing updates quickly and transparently, including automatic security updates where applicable and clear user notifications ([8]).

This domain covers both internal activities and external inputs. It includes tracking known issues, reviewing external sources, such as vendor advisories and public vulnerability databases, and handling reports from researchers or customers.

Additionally, the CRA requires manufacturers to identify and document vulnerabilities and components, including by drawing up a software bill of materials (SBOM) for software products placed on the EU single market. A SBOM is a structured inventory of both proprietary and open-source components, libraries and dependencies within software, enabling manufacturers to understand the composition of their software products. By providing visibility into software components and dependencies, SBOMs support vulnerability management by helping manufacturers identify affected products and prioritise remediation activities based on exposure and criticality.

The main assessment criteria include:

- identifying, receiving and tracking vulnerabilities affecting products;
- using external sources of vulnerability information, such as advisories and public databases;
- prioritising vulnerabilities based on risk and potential impact;
- developing, testing and distributing security updates;
- communicating vulnerabilities and updates to users where appropriate.

The maturity levels are as follows.

- **Level 1.** No vulnerability or patch management process exists.
- **Level 2.** Vulnerabilities and patches are being handled on an ad hoc basis.
- **Level 3.** Vulnerability and patch management processes are not consistently followed.
- **Level 4.** Vulnerabilities are systematically tracked and prioritised, and patches are applied reliably.
- **Level 5.** Vulnerability and patch management processes are measured, reviewed and continuously improved.

When the maturity level increases, organisations move away from ad hoc vulnerability handling towards more structured, measurable and continuously improving processes that can reduce security risks and strengthen the trust of users.

([8]) Annex I, Part I(2)(c), of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

2.4 Product life cycle management

This domain aligns with the post-market aspects of the CRA. While the CRA does not define product life cycle management as a separate requirement, these elements imply that manufacturers are expected to maintain an appropriate level of cybersecurity during the declared support period of a product ([9]). Security therefore does not end at the moment that a product is placed on the market. This includes addressing and reporting vulnerabilities, and being transparent with customers about security updates and end-of-support timelines. In this way, security remains an ongoing responsibility throughout the entire product life cycle.

For SMEs, a clear and consistent approach to product life cycle management is particularly important to ensure the security of their product. Limited resources can make it tempting to handle security issues and vulnerabilities on a case-by-case basis, but without a defined structure this tends to result in inconsistent responses, unclear responsibilities and delays that can have real consequences for customers.

Effective life cycle management reduces these risks. When support periods are clearly defined, responsibilities are assigned and end-of-life transitions are planned in advance, organisations are better placed to respond to issues in a timely and coordinated way. Customers benefit from greater predictability and clearer communication, and the organisation is less likely to find itself managing avoidable problems under pressure.

Over time, consistent life cycle management also helps build and maintain customer trust. Organisations that handle security issues in a transparent way and follow through on their commitments are seen as more reliable. This kind of consistency is difficult to achieve with ad hoc approaches, regardless of the organisation's size.

The main assessment criteria include:

- defining and maintaining security support periods for products;
- ensuring security updates are provided throughout the declared support period;
- maintaining processes to support the security of products throughout their life cycle;
- communicating security support periods, end-of-support and end-of-life timelines to users;
- planning for the secure retirement or replacement of products where appropriate.

The maturity levels are as follows.

- **Level 1.** Product security is not actively managed after release. Support periods and responsibilities are not defined.
- **Level 2.** Product support, security updates and end-of-support decisions are handled on an ad hoc basis. Activities depend on individual effort.
- **Level 3.** Processes for product support, security updates and end-of-support are defined but are not applied consistently across products.

([9]) See Annex I, Part II, of the CRA, which requires manufacturers to address vulnerabilities and provide security updates for products with digital elements during the declared support period.

- **Level 4.** Products are actively managed throughout their declared support period. Security updates are provided as needed, and support periods and end-of-support timelines are clearly defined and communicated to users.
- **Level 5.** Product life cycle management is regularly reviewed and continuously improved. Support processes, update delivery and communication with users are monitored to ensure products remain secure throughout their supported life cycle.

As the maturity level increases, organisations show better preparedness, communicate more clearly with customers and manage life cycle transitions in a more predictable and structured way.

2.5 Awareness, competence and skills

The awareness, competence and skills domain focuses on the people and organisational capabilities needed to support cybersecurity practices in the context of the CRA. While the CRA primarily defines requirements for product security, their effective implementation depends on the knowledge, skills and awareness of the people involved throughout the product life cycle. Training can range from short internal briefings and online courses to more advanced, role-specific training, depending on the organisation's size and risk exposure.

This domain is especially important for SMEs, because staff, particularly at microenterprises with only a few employees, often perform multiple roles, and dedicated cybersecurity teams may not exist. In such environments, responsibilities related to product security may be shared across staff working in development, operations, management and support. The aim is not to introduce specialised roles, but to ensure that individuals have sufficient awareness and competence to carry out their responsibilities in a secure and reliable manner.

This domain covers both general product security awareness and role-specific competence. General product security awareness helps individuals understand basic security principles and common risks, while role-specific competence supports the application of security practices in areas such as design, development and maintenance. It also reflects the importance of information sharing ([10]), both within the organisation and externally. Access to relevant security information, such as vulnerability reports or lessons learned, can support more effective handling of product security issues.

The criteria in this domain support the implementation of CRA requirements but do not represent a direct regulatory obligation. The level of formal and structured practices should be proportionate to the size of the organisation and the complexity of its products.

The main assessment criteria include:

- ensuring basic awareness of product security principles among relevant staff;
- providing role-appropriate guidance or training where needed;

([10]) Articles 13 and 14 of and Annex I to Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

- supporting secure development and configuration practices for technical roles;
- sharing relevant lessons learned from vulnerabilities or security issues;
- making use of available external sources of security information where appropriate.

The maturity levels are as follows.

- **Level 1.** No awareness or training activities exist.
- **Level 2.** Basic awareness exists but is informal and depends on individual experience or initiative.
- **Level 3.** Relevant knowledge or guidance is available and used in some activities, but not consistently across all work.
- **Level 4.** Product security awareness and role-relevant knowledge are applied consistently in day-to-day activities.
- **Level 5.** Knowledge and skills are regularly updated and adapted based on experience, new risks and external information.

At lower maturity levels, awareness and training tends to be informal, irregular or driven by individual initiative. Training may only happen after incidents or due to external pressure, and security knowledge is not shared systematically across the organisation. As the maturity level increases, training becomes more structured, role based and regular.

3. How to use the SME Cyber Resilience Maturity Assessment Model

Estimated time to complete

The self-check questionnaire takes approximately two hours to complete, depending on the size of the organisation and the availability of information. It can be completed more quickly using operational knowledge or in more detail by reviewing documentation and evidence.

Product scope and CRA context

This assessment applies to products with digital elements as defined in the CRA. Before completing the assessment, organisations should identify which products are in scope and whether different product types should be considered separately.

The CRA distinguishes between categories of products, including default, important and critical products, which may be subject to different requirements and conformity assessment procedures. While this model does not distinguish between different product categories, organisations should be aware that the product type and risk level may influence which obligations apply.

Figure 2. Steps for completing the self-check.

Step 1. Score each response in all five domains (see questionnaire in Annex A)
Each question has five response options ranging from 'Not implemented' (Level 1) to 'Measured, monitored and continuously improved' (Level 5). Assign the numeric value that matches your answer. For example, if your answer corresponds to Level 2, give it a score of 2.

> Some questions combine multiple related practices. If your organisation performs well in some aspects but not others, select the score that best reflects the weakest area, or apply a conservative average judgement.

The maturity levels can be interpreted as follows:

- Level 1 – not implemented;
- Level 2 – informal or ad hoc;

- Level 3 – documented but inconsistently applied;
- Level 4 – consistently applied and regularly reviewed;
- Level 5 – measured, monitored and continuously improved.

The following are some examples to assist scoring:

- Level 1 – no defined practices exist or activities are not performed (e.g. vulnerabilities are not tracked or handled in a structured way);
- Level 2 – activities are performed occasionally and depend on individuals (e.g. vulnerabilities tracked in personal notes or emails);
- Level 3 – processes are defined (e.g. a documented procedure or template exists) but are not consistently followed across all products;
- Level 4 – processes are consistently followed for most or all products and evidence exists (e.g. logs, records, reports);
- Level 5 – practices are measured (e.g. using key performance indicators such as time taken to fix vulnerabilities), regularly reviewed and improved based on the results.

When selecting a level, it should be considered how practices are applied in practice, not only whether they are documented. For example:

- a documented process that is not followed in day-to-day activities should be considered Level 2 rather than Level 3;
- where practices are applied inconsistently across products or teams, Level 3 may be more appropriate than Level 4;
- where there is no clear evidence of review or improvement, Level 4 should be selected rather than Level 5.

Key distinction: Level 4 indicates that practices are consistently applied, while Level 5 requires evidence of measurement (e.g. metrics or key performance indicators) and active improvement based on the results.

Step 2. Calculate scores for each domain

The self-check is divided into five domains. For each domain, calculate the average score of all the responses. This gives a domain-specific maturity score between 1 and 5. For example, if in the ‘Governance and documentation’ domain the five responses score 2, 3, 2, 1 and 3, the average is 2.2, indicating that the maturity level for the domain is 2.2.

Step 3. Determine overall maturity

The overall organisational maturity score is calculated as the average of the five domain scores. For example, if the domain averages are 2.2 for governance and documentation, 3.0 for risk management and security by design and by default, 2.5 for vulnerability and patch management, 2.0 for product life cycle management and 1.8 for awareness, competence and skills, the combined score is 11.5. Dividing this by the five domains results in an overall maturity score of 2.3.

Step 4. Classify maturity profile

Use the overall score or the distribution of scores across domains to classify your organisation’s maturity, as follows.

- **Basic maturity (1.0–2.5).** Practices are informal or ad hoc, mostly reactive and require immediate attention.

- **Intermediate maturity (2.6–3.9).** Some processes are documented, but implementation is inconsistent.
- **Advanced maturity (4.0–5.0).** Practices are formalised, applied consistently and continuously improved.

Step 5. Identify gaps and plan improvements

The overall maturity score provides a general view of your organisation's readiness, but it should not be considered in isolation. An intermediate score does not mean that all areas are performing at the same level. Some domains may still fall within the basic maturity category and require focused attention. Areas with lower scores should be reviewed carefully, as weaknesses in a single domain can affect overall security.

Where gaps are identified, a structured improvement plan should be developed, with actions prioritised as follows.

- **High-risk gaps.** These are issues that create significant exposure if left unaddressed, such as untracked vulnerabilities, the absence of an incident response process or unclear regulatory responsibilities.
- **Easier improvements.** These are changes that can be implemented without significant time or resources, for example clarifying ownership, formalising existing practices or updating documentation.
- **Long-term actions.** These are changes that require time and continued effort to implement, such as strengthening the security culture, introducing structured training and developing processes that support ongoing improvement.

Step 6. Track progress over time

The self-check should be repeated periodically, for example annually or after major product updates. Comparing results over time allows your organisation to track progress in each domain, demonstrate continuous improvement and maintain evidence of increasing product security.

A Annex: self-check questionnaire

Each question in Annex A has five response options, corresponding to increasing levels of maturity:

- 1 corresponds to Level 1 (score = 1);
- 2 corresponds to Level 2 (score = 2);
- 3 corresponds to Level 3 (score = 3);
- 4 corresponds to Level 4 (score = 4);
- 5 corresponds to Level 5 (score = 5).

Guidance on composite questions

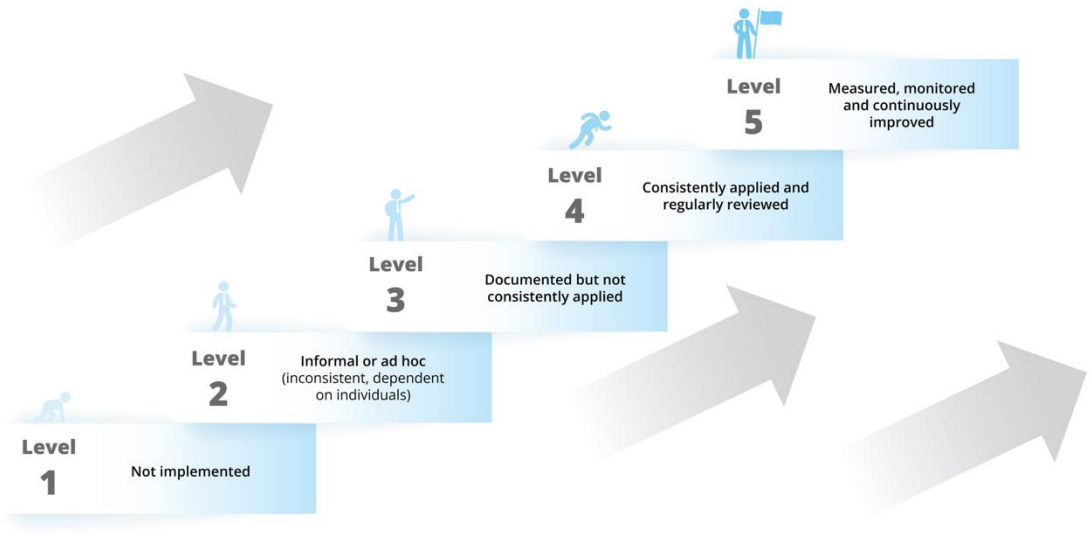

Figure 3. Maturity-level guidance

Some questions in this assessment cover multiple related practices (e.g. risk assessment, secure design and component management). This is intended to keep the questionnaire concise.

Where an organisation performs well in some aspects but not in others, the score should reflect the lowest level that is consistently achieved. If needed, organisations may use internal notes to assess each aspect separately before selecting an overall score. Where significant differences exist between aspects, organisations are encouraged to internally assess them separately before selecting an overall score. The descriptions of maturity levels and domains in Section 2 can be used as a reference when selecting responses.

1. Governance and documentation

1.1. Do you have written and approved product security policies?
1. No product security policies or guidelines exist.
2. Some basic guidelines exist but are informal or incomplete.
3. Documented policies or guidelines exist but are not formally approved or consistently used.
4. Policies are formally approved, documented and generally applied.
5. Policies are formally approved, consistently applied, regularly reviewed and continuously improved.

1.2. Are roles and responsibilities clearly defined for product security activities (e.g. development, vulnerability management, updates)?
1. No roles or responsibilities are defined.
2. Responsibilities exist informally but are unclear or inconsistently assigned.
3. Responsibilities are documented but not consistently applied in practice.
4. Responsibilities are clearly defined, documented and consistently applied.
5. Responsibilities are clearly defined, communicated, consistently applied, regularly reviewed and continuously improved.

1.3. Do you maintain product-level technical documentation describing implemented security features, risk assessments, design decisions and update procedures?
1. No product security documentation exists.
2. Limited or incomplete documentation exists covering only some aspects.
3. Documentation covering most required aspects exists but is incomplete or not consistently maintained.
4. Documentation is complete for most products and consistently maintained.
5. Documentation is complete for all products and is formally maintained, regularly reviewed and continuously improved.

1.4. Is there a process to regularly review product security and the quality of related documentation?
1. No review process exists.
2. Reviews happen informally or occasionally.
3. A documented review process exists but is not consistently applied.
4. Reviews are consistently performed and documented.
5. Reviews are measured, tracked and continuously improved.

1.5. Are you aware of the market surveillance authority responsible for enforcing the CRA, the conformity assessment procedure applicable to your products, and how to interact with relevant authorities if needed?
1. No awareness of authorities or obligations.
2. Limited awareness but no clear understanding of obligations.
3. Authorities and obligations are known but not formally documented.
4. Authorities, obligations and interaction processes are defined and followed.
5. Awareness and interaction processes are formalised, maintained and regularly reviewed.

2. Risk management and security by design and by default

2.1. Do you perform cybersecurity risk assessments and use the results to guide product design, development, configuration and component management decisions?

1. No risk assessments are performed.
2. Risk assessments are informal and rarely influence decisions.
3. Risk assessments are documented but not consistently used.
4. Risk assessments are systematically performed and guide decisions.
5. Risk assessments are formalised, integrated into processes and continuously improved.

2.2. Are products designed using security by design principles from the outset?

1. Security by design is not considered.
2. Security by design is considered occasionally or late in development.
3. Security by design is applied during design but not consistently.
4. Security by design is consistently applied across products and regularly reviewed.
5. Security by design is fully integrated into development and continuously improved.

2.3. Are products delivered with secure by default configurations and settings?

1. No secure defaults are defined.
2. Secure defaults exist but are inconsistent.
3. Secure defaults are defined but not consistently applied.
4. Secure defaults are consistently applied and reviewed.
5. Secure defaults are enforced, tested and continuously improved.

2.4. Do you perform security checks and testing before releasing or updating a product, and to what extent are automated tools used?

1. No security testing is performed.
2. Testing is occasional and mostly manual.
3. Testing is documented and includes some automated tools.
4. Testing is systematically integrated into development workflows and regularly reviewed.
5. Testing is risk based, automated where appropriate, monitored and continuously improved.

2.5. When risks change or new threats emerge, are risk assessments, configurations and third-party components reviewed and updated?

1. No structured review or update process exists.
2. Updates are informal or occasional.
3. Reviews are documented but not consistently applied.
4. Reviews and updates are consistently performed across products.
5. Continuous monitoring and structured updates are in place and continuously improved.

3. Vulnerability and patch management

3.1. Do you have a process to receive, acknowledge, record and track vulnerabilities reported by customers, researchers or internal staff?

1. No vulnerability tracking exists.
2. Vulnerabilities are handled informally.
3. A documented tracking process exists but is not consistently applied.
4. Vulnerabilities are consistently tracked and reviewed.
5. Tracking is measured, integrated and continuously improved.

3.2. Do you have a defined process for creating, testing and delivering security updates for supported products and communicating them to customers?

1. No update process exists.
2. Updates are handled informally.
3. A documented process exists but is not consistently followed.
4. Updates are consistently managed, tested and delivered.
5. The process is monitored, measured and continuously improved.

3.3. Do you maintain and use SBOMs to support vulnerability and dependency management?

1. No SBOMs are created or maintained.
2. SBOMs are created occasionally or manually.
3. SBOMs are documented for most products but not consistently maintained or used.
4. SBOMs are systematically maintained and used in vulnerability management.
5. SBOMs are integrated, automated where appropriate and continuously improved.

3.4. Are vulnerabilities and updates prioritised based on risk and potential impact?

1. No prioritisation is performed.
2. Prioritisation is informal.
3. A documented prioritisation approach exists but is not consistently applied.
4. Prioritisation is consistently risk based and applied.
5. Prioritisation is measured, reviewed and continuously improved.

3.5. Do you verify that security updates resolve reported vulnerabilities effectively and maintain evidence of this verification?

1. No verification is performed.
2. Verification is informal or occasional.
3. Verification is documented but not consistently applied.
4. Verification is consistently performed and documented.
5. Verification is measured, reviewed and continuously improved.

4.1. Is there a defined approach to managing product security during the operational phase?
1. No structured approach exists.
2. Some practices exist but are informal.
3. A documented approach exists but is not consistently applied.
4. The approach is consistently applied and reviewed.
5. The approach is monitored, measured and continuously improved.

4.2. Is the product life cycle management actively managed, including defined support periods, update responsibilities, end-of-life arrangements and communication with customers?
1. No life-cycle management exists.
2. Life-cycle activities are informal.
3. Life-cycle processes are documented but not consistently applied.
4. Life-cycle management is consistently applied and communicated.
5. Life-cycle management is monitored, reviewed and continuously improved.

4.3. Is experience from product operation, post-incident reviews and customer input used to improve products over time?
1. No structured improvement process exists.
2. Improvements are implemented occasionally and informally.
3. A documented improvement approach exists but is not consistently applied.
4. Improvements are consistently implemented and tracked.
5. Continuous improvement is measured and integrated into product management.

4.4. Is there a structured and tested way to address identified product security issues?
1. No defined method exists.
2. Issues are handled inconsistently.
3. A documented method exists but is not consistently applied or tested.
4. Issues are handled through a consistent and reviewed process.
5. The process is tested, measured and continuously improved.

4.5. Are products monitored during operation to identify security risks, vulnerabilities and emerging threats?
1. No monitoring exists.
2. Monitoring is informal or occasional.
3. Monitoring is documented but not consistently applied.
4. Monitoring is consistently performed and results are tracked.
5. Monitoring is integrated, risk based and continuously improved.

5. Awareness, competence and skills

5.1. Are sufficient skills available to design, develop and maintain products in a secure way, including through external expertise where internal capacity is limited?
1. No relevant expertise is available.
2. Limited expertise is available and applied informally.
3. Skills are documented but not consistently sufficient.
4. Skills are sufficient, applied and regularly reviewed.
5. Skills are assessed, developed and continuously improved.

5.2. Do staff receive appropriate training on cybersecurity practices relevant to their roles, including product risk management, vulnerability management, and security by design?
1. No training is provided.
2. Training is informal or occasional.
3. Training is documented but not consistently delivered.
4. Training is regularly delivered and reviewed.
5. Training effectiveness is assessed and continuously improved.

5.3. Does the organisation promote a culture of responsible product development, open reporting and awareness of product risks?
1. No promotion of responsible product development or product risk awareness.
2. Responsible practices and product risks are discussed informally.
3. Expectations are documented but not consistently applied.
4. Responsible practices are consistently encouraged and applied.
5. Culture is embedded, measured and continuously improved.

5.4. Do you follow relevant external product security information (e.g. advisories, alerts)?
1. No external information is followed.
2. Information is followed occasionally.
3. Sources are documented but not consistently used.
4. Information is consistently monitored and used.
5. Engagement is active, integrated and continuously improved.

5.5. Do you assess your team and validate that it has the required skills and competence to maintain secure products?
1. No assessment exists.
2. Assessment is informal.
3. Assessment is documented but not consistently applied.
4. Assessment is consistently performed and gaps are addressed.
5. Competence is measured, tracked and continuously improved.

B Annex: checklist – what to do after the self-check

When the organisation has finished the self-check, calculated their score and identified their maturity profile, they can use the checklist that matches their profile to create a roadmap for the next steps and actions to potentially focus on. Not everything needs to be completed at once. Start with the most important items and build up from that, step by step. The recommended actions should be applied proportionally, taking into account the size, resources and complexity of the organisation.

The following process is recommended:

- start with your current maturity level;
- prioritise actions in domains where scores are lowest, especially where scores are below 2.5;
- pick a small number of actions you can complete in the next 3–6 months;
- repeat the self-check regularly to track progress.

Domain	Actions if score is 1.0–2.5 (basic maturity)	Actions if score is 2.6–3.9 (intermediate maturity)	Actions if score is 4.0–5.0 (advanced maturity)
Governance and documentation	Prioritise **basic actions in Annex B**, such as defining policies, roles and documentation	Focus on **intermediate actions**, ensuring that governance is applied consistently	Maintain practices and consider **advanced actions**, such as improving review and traceability
Risk management and security by design and by default	Prioritise **basic actions**, such as introducing risk assessment and secure design practices	Focus on **intermediate actions**, integrating risk considerations into development processes	Maintain and refine practices, including **advanced actions** such as improving decision-making and efficiency
Vulnerability and patch management	Prioritise **basic actions**, such as tracking vulnerabilities and applying updates	Focus on **intermediate actions**, improving prioritisation and use of component information (e.g. SBOMs)	Maintain and enhance practices, including **advanced actions** such as improving response and automation where appropriate
Product life cycle management	Prioritise **basic actions**, such as defining support, monitoring and communication practices	Focus on **intermediate actions**, ensuring that life cycle processes are applied consistently	Maintain and improve practices, including **advanced actions** such as testing and feedback loops
Awareness, competence and skills	Prioritise **basic actions**, ensuring that relevant staff have sufficient awareness and guidance	Focus on **intermediate actions**, providing more structured knowledge sharing or training	Maintain and improve practices, including **advanced actions** such as reviewing and updating skills over time

Table 1. Maturity progress by domains.

The maturity level reflects how structured and consistent the organisation's approach to product security is. The recommendations outline practical steps that organisations can take to improve their

preparedness with the CRA. Following these steps does not guarantee compliance, but it helps establish a more organised and reliable approach to product security.

Proportionality guidance

The actions described in this annex should be applied proportionally, taking into account the size of the organisation, the type of product and the associated risks. For microenterprises, simpler approaches may be sufficient, provided that they enable consistent, traceable and timely management of product security. Examples include:

- using lightweight tools or processes, provided that they support tracking, prioritisation and follow-up of security issues;
- focusing on the most critical risks and components;
- using external expertise where internal capacity is limited.

The objective is to achieve an appropriate level of security and control, rather than to implement complex solutions that are not justified by the level of risk.

Maturity profiles checklist:

When the result is basic maturity (score of 1.0–2.5)

At this level: product cybersecurity is mostly informal and reactive.

Main goal: to set up a basic structure, visibility and responsibilities.

Documentation and governance

- Keep a basic record of key product security aspects (e.g. configurations, issues, updates).
- Assign responsibility for product security activities so that ownership is clear. Without a defined owner, important obligations are easier to overlook.
- Be clear about roles across product life cycle management, including development, maintenance and vulnerability management.
- From time to time, review documentation to check that it still reflects how things are actually done.
- Identify the relevant market surveillance authority and understand basic reporting expectations under the CRA ([11]).

Risk management and security by design and by default

- Carry out a basic risk assessment for products so that security measures are based on actual risks.
- Consider security during development, rather than later when the product has already been built.
- Record the main security risks for each product to avoid repeated rediscovery.
- Ensure that products are delivered with secure default settings.
- Perform basic security checks before release or update to identify issues early.

([11]) A market surveillance authority is a national authority responsible for monitoring the compliance of products placed on the market and for acting when products do not meet regulatory requirements. See European Commission, 'Market surveillance authorities', European Commission website, accessed 17 June 2026, https://webgate.ec.europa.eu/single-market-compliance-space/market-surveillance/ms-authorities.

Vulnerability and patch management

- Establish a clear contact point for reporting vulnerabilities so that issues can be recorded and handled without delay.
- Maintain a record of vulnerabilities for each product to ensure that they are tracked.
- Address vulnerabilities based on their potential impact, starting with the most serious ones.
- Before releasing an update, check that it actually fixes the reported vulnerability.
- Research and plan a SBOM strategy to support the identification of vulnerabilities in software products.
- Generate an inventory of components (SBOM), using a commonly used and machine-readable format where feasible. Start with key components and expand over time.
- Be aware of basic CRA reporting expectations for vulnerabilities and incidents.

Product life cycle management

- Put a simple process in place for handling product security issues so that teams can respond in a consistent way when something happens.
- Clarify how communication with customers would be handled if a serious security issue arose.
- Make product support periods clear so that customers know what to expect.
- Keep a record of product security issues so that they can be tracked and used for learning over time.
- Make sure that someone is responsible for product security during the support period.
- Use feedback from customers and operational experience to spot recurring issues.
- Perform basic monitoring of products on the market during their life cycle to identify potential security risks.

Awareness, competence and skills

- Identify the knowledge and skills needed to meet product security obligations.
- Consider using external expertise where internal capacity is limited.
- Make sure that security expectations are communicated so that staff understands their responsibilities.
- Follow relevant external sources of product security information.
- Periodically check that staff involved in product development and maintenance have the required competence.

Action planning and tracking

- ✓ Address the highest-risk gaps first, particularly in vulnerability management and regulatory obligations.
- ✓ Focus on a limited number of achievable actions to ensure that progress is made.
- ✓ Assign responsibility for vulnerability management, updates and product security tasks.

Examples of evidence: informal records such as spreadsheets, emails, meeting notes, ticketing system entries, basic product documentation, assigned responsibilities or other evidence showing that activities are performed in practice.

Outcome: basic structure and responsibilities are in place, and initial steps towards CRA alignment have been taken.

When the result is intermediate maturity (score of 2.6–3.9)

At this level: there is increasing alignment with CRA requirements, but practices are not yet consistently applied.

Main goal: to strengthen consistency and ensure that these practices are used regularly.

Governance and documentation

- Ensure that cybersecurity responsibilities are clearly assigned.
- Maintain product-level documentation covering design decisions, known issues and update procedures.
- Review documentation regularly to keep it accurate and aligned with current practices.
- Keep a clear record of interactions with relevant authorities and reporting points of contact with reporting responsibilities.
- Document regulatory incident reporting requirements, including when incidents must be reported, applicable deadlines, and responsible roles.
- Identify and document the conformity assessment procedure applicable to each product.

Risk management and security by design and by default

- Maintain documented risk assessments for each product and keep them up to date.
- Use risk assessment results to guide design and configuration decisions.
- Make security by design a consistent part of product development.
- Perform security checks before each release or update.
- Follow vulnerability sources and advisories for components used in products.
- Review security architecture periodically to ensure that controls remain appropriate.

Vulnerability and patch management

- Assign a severity rating to each vulnerability using a consistent approach.
- Set time frames for addressing vulnerabilities based on their severity.
- Notify customers about vulnerabilities and relevant security updates in a timely manner.
- Maintain a complete record of vulnerabilities and the actions taken to resolve them.
- Generate and maintain an inventory of components (a SBOM), using tools or simplified approaches appropriate to the organisation’s size.
- Research and plan how to integrate SBOMs into the vulnerability identification process.
- Use component information (a SBOM) to support vulnerability identification, where feasible.
- Verify that security updates resolve the reported vulnerability before release.

Product life cycle management

- Maintain a documented plan for handling product security issues, including roles and communication.
- Test the plan periodically using approaches appropriate to the organisation (e.g. simple walk-throughs or tabletop exercises).
- Provide clear information to customers on support timelines and end-of-life arrangements.
- Review product security incidents and customer feedback regularly.
- Monitor products consistently throughout their support period.

Awareness, competence and skills

- Ensure that product security training reflects the responsibilities of each role.
- Encourage teams to share lessons learned from product security issues.
- Follow relevant external sources of product security information.
- Periodically check that staff involved in product development and maintenance have the required level of security knowledge.

Action planning and tracking

- ✓ Define clear and realistic objectives for each area requiring improvement. Vague goals are difficult to measure and are more likely to be deprioritised when competing demands arise.
- ✓ Break down larger improvements into smaller, manageable steps. Gradual changes are easier to implement and more likely to be sustained over time.
- ✓ Track progress and update relevant policies or procedures as actions are completed. Improvements that are not reflected in documentation tend to fade from everyday practice.

Examples of evidence: documented procedures, risk assessments, vulnerability registers, training records, incident-handling plans, SBOMs, review records or evidence that security activities are performed consistently across products.

Outcome: practices are applied more consistently and support stronger alignment with CRA requirements.

When the result is advanced maturity (score of 4.0–5.0)

At this level: security practices are established and applied consistently.

Main goal: to maintain these practices and update them when necessary.

Governance and documentation

- Review cybersecurity arrangements on a regular basis using defined indicators (e.g. incidents, response times), for example through quarterly discussions that cover recent incidents, key indicators and any unresolved issues.
- Look at incident and monitoring data over time to spot recurring patterns and address underlying causes, rather than just looking at individual cases.

- Make sure that staffing and budget decisions reflect the level of risk associated with each product.
- Clearly assign responsibility for risk reviews and regulatory notifications, and make sure that the approach is documented so that it can be followed in practice.
- Keep records of cybersecurity activities, including risk assessments, testing and vulnerability management, in a way that is complete and easy to trace when needed.

Risk management and security by design and by default

- Include risk management in product planning and roadmaps so that security considerations influence decisions from the outset.
- Apply a consistent set of secure design principles across products to support more predictable and defensible outcomes.
- Record key threat scenarios along with the reasoning behind the selected security measures.
- Revisit the security architecture periodically to confirm that existing controls remain appropriate as the product evolves.
- Integrate security testing into the development workflow and ensure that results are addressed before release.
- Ensure that risk assessment results are clearly reflected in design, configuration and component management decisions.
- Measure the effectiveness of security controls and improve processes based on the results.

Vulnerability and patch management

- Use automated tools, where appropriate to the organisation's size and product complexity.
- Maintain a clear and consistent process for communicating vulnerabilities to customers and, where required, authorities.
- Keep complete and traceable records of vulnerabilities and how they were handled.
- Confirm that fixes resolve the underlying vulnerability and review how effectively the update process worked.
- Maintain and use component inventories (e.g. SBOMs) to support vulnerability management, where appropriate.
- Assess the exploitability of vulnerabilities where relevant, to support prioritisation of fixes.
- Track indicators such as time taken to detect and resolve vulnerabilities to support improvement, where feasible.

Product life cycle management

- Maintain a structured product security management plan with clear roles, responsibilities and escalation paths.
- Test and review the plan regularly and address any gaps that are identified.
- Carry out structured follow-ups after security incidents to capture lessons learned.
- Review product support periods and life cycle commitments to ensure that they remain realistic.
- Ensure that processes support the coordinated handling of vulnerabilities, including communication with external parties where relevant.
- Measure the effectiveness of incident handling and improve processes based on the results.

Awareness, competence and skills

- Provide role-appropriate training, using approaches suitable for the organisation and that reflect the level of risk and responsibility involved.
- Maintain accessible reporting channels and encourage staff to raise security concerns.
- Review competence levels regularly and address gaps through training, recruitment or specialist support.
- Follow external product security information in a structured way and engage with relevant communities where appropriate.
- Assess staff skills on an ongoing basis and use the results to guide training and product security improvements.
- Track training effectiveness and improve processes based on the results.

Action planning and tracking

- ✓ Review improvement plans at regular intervals, for example alongside annual product roadmap reviews, to ensure that they remain relevant.
- ✓ Update planned actions when new risks, vulnerabilities or weaknesses are identified so that efforts reflect the current situation.
- ✓ Keep key records such as policies, risk assessments, component inventories, vulnerability logs and test results up to date and easy to access when needed.
- ✓ Use measurable indicators, where feasible, to track product security performance (e.g. time taken to resolve vulnerabilities).

Examples of evidence: governance reports, security metrics, management reviews, automated monitoring outputs, audit trails, effectiveness measurements, trend analyses, lessons learned records and evidence of continuous improvement based on the results.

Outcome: the organisation is able to manage product risks in a structured way and respond effectively to changing requirements.

Ongoing improvement for all maturity levels

Regardless of the maturity level:

- ✓ repeat the self-check at regular intervals (e.g. once per year);
- ✓ compare results over time to identify progress or gaps;
- ✓ keep documentation and supporting records up to date;
- ✓ treat product risk management as an ongoing activity rather than a one-time exercise.

C Annex: glossary of key terms

The following terms are used throughout this document.

Attack surface – the set of all points within a system or product where an attacker could attempt to exploit vulnerabilities.

Conformity assessment procedure – a process used to demonstrate that a product complies with applicable regulatory requirements before being placed on the market. The applicable procedure depends on the type and classification of the product. Source: European Commission, 'Cyber Resilience Act', European Commission website, accessed 17 June, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

Market surveillance authority – a national authority responsible for monitoring compliance of products placed on the market and acting where products do not meet regulatory requirements. Source: European Commission, 'Market surveillance authorities', European Commission website, accessed 17 June, https://webgate.ec.europa.eu/single-market-compliance-space/market-surveillance/ms-authorities.

Security by default – a principle ensuring that products are configured with secure settings by default, reducing exposure to risks without requiring user intervention.

Security by design – an approach where security considerations are integrated into the design and development of a product from the outset, rather than added later.

Software bill of materials (SBOM) – a structured list of software components, libraries and dependencies included in a product. It supports vulnerability management by helping organisations identify affected components. Source: European Commission, 'Cyber Resilience Act', European Commission website, accessed 17 June, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

Vulnerability – a weakness in a system, component or process that can be exploited to compromise security.

D Annex: mapping to Cyber Resilience Act requirements

The table below provides an indicative mapping between the assessment domains and relevant provisions of the CRA, including Annex I (essential cybersecurity requirements), related to vulnerability handling, reporting and communication obligations.

The mapping focuses on Annex I to the CRA, which defines the essential cybersecurity requirements for products with digital elements.

Some domains in this model, such as governance and documentation, product life cycle management and awareness, competence and skills, are not explicitly defined as separate requirements in the CRA. However, they represent organisational capabilities that support the effective implementation and maintenance of the requirements set out in Annex I. As a result, not all assessment criteria can be directly mapped to specific CRA provisions.

The mapping supports traceability and understanding of how the assessment relates to the CRA.

Domain	CRA requirements	CRA provisions (supporting obligations)
Governance and documentation	Not explicitly addressed as a stand-alone requirement in the CRA	Supports compliance with Article 13, Article 31 and Annex VII through cybersecurity risk assessment, technical documentation and conformity assessment activities
Risk management and security by design and by default	Annex I, Part I(1) and (2): risk assessment, secure design, protection against vulnerabilities and secure configuration	Article 13
Vulnerability and patch management	Annex I, Part II: vulnerability handling, remediation, security updates and coordinated vulnerability disclosure	Articles 13 and 14
Product life cycle management	Annex I, Part II: security updates throughout the support period Annex II: information on support period and security updates	Article 13
Awareness, competence and skills	Not explicitly addressed in the CRA	Indirectly supports compliance with Article 13 and implementation of Annex I requirements

References

1. **Calderon-Monge, E. and Ribeiro-Soriano, D**., 'The role of digitalization in business and management: A systematic literature review', *Review of Managerial Science*, Vol. 18, No 2, 2024, pp. 449–491, https://link.springer.com/article/10.1007/s11846-023-00647-8.

2. Commission recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

3. **ENISA.** Cybersecurity for SMEs – Challenges and Recommendations. 2021

4. . Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act),

Abbreviations

CRA	Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)
MSA	Market Surveillance Authority
SBOM	software bill of materials
SMEs	micro, small and medium-sized enterprises

TP-01-26-014-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union

978-92-9204-799-3