TLP - CLEAR

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

SME CRA Survey Report

Survey Results and Analysis

JUNE 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.

AUTHORS

European Union Agency for Cybersecurity (ENISA)

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-793-1, DOI 10.2824/0994553, Catalogue Number TP-01-26-010-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 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 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, as part of the European Commission's SME cybersecurity strategy, is working on practical guidance, tools and support activities tailored to the realities and needs of smaller organisations.

This report presents the findings of the ENISA SME CRA Survey, conducted in February and March 2026. The survey aimed to better understand:

- how familiar SMEs are with the CRA;
- how well they understand the practical requirements of the regulation;
- what they are currently doing in terms of cybersecurity;
- what challenges they expect to face when working towards compliance.

The survey also gathered feedback on the support SMEs need and established a baseline for their maturity in product security practices.

A total of **194** ([2]) organisations responded from **31** countries / geographical groupings.

The sample includes SMEs, covering microcompanies (1–9 employees), small companies (10–49 employees) and medium-sized companies (50–249 employees), in line with the European Commission definition of SMEs ([3]).

Key findings

- **There is a clear gap between awareness and practical readiness.** The results showed that awareness of the existence of the CRA is relatively high, with 66 % of respondents stating that they had heard of it before the survey. However, the results indicate that this does not translate into a strong understanding of what the regulation requires in practice. The levels of understanding

([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]) There were 194 responses in total, with 174 being in the scope of the CRA. Percentages throughout are of the 194 responses. "No Answer" responses (n = 20, 10.31%) are excluded from all figures.

([3]) Commission Recommendation 2003/361/EC 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).

drop in more detailed areas, for example in the conformity assessment and compliance topic, where 54 % of the replies indicated limited or no understanding. Understanding is also low in relation to the required documentation, with 42 % indicating limited or no understanding.

- **The size of the enterprise is the most consistent factor influencing the level of maturity.** Across all five domains ([4]) in the survey, medium-sized companies scored about 1 point higher than microcompanies on average. At the same time, about half of microcompanies are still at level 1 or 2 ([5]), meaning they either do not have formal processes in place or are handling product security in a more improvised way.
- **Incident response and product life cycle management is the weakest area overall.** The average score is 2.6 out of 5. More than a third of microcompanies have no incident response plan. No microcompany reported a formally enforced product life cycle policy.
- **Practical templates are the most requested form of support.** Technical documentation templates and secure development templates were each requested by more than 70 % of respondents. Only 3 out of all respondents said they needed none of the listed templates.
- **The challenge for SMEs is not only understanding the CRA requirements, but also managing the time and resources needed to implement them and the cost involved.** Financial support was selected by 142 of the respondents who answered the open support question, the joint highest figure for any single item in the support needs section alongside support in terms of templates and checklists for required technical documentation.
- **SMEs do not rely on a single source of CRA information.** SMEs prefer different channels to get information about the CRA. This means that effective outreach will require a combination of communication formats and platforms.

Domain	At risk (L1 + L2)			Avg maturity score			On track (L4 + L5)		
	Micro	Small	Medium	Micro	Small	Medium	Micro	Small	Medium
Governance and Documentation	49%	19%	36%	2.5	3.0	3.5	9%	41%	53%
Risk Management and Secure-by-Design	49%	36%	26%	2.4	2.8	3.2	9%	23%	40%
Vulnerability and Patch Management	40%	30%	19%	2.6	3.0	3.3	8%	25%	44%
Inicident Response and Lifecycle	49%	38%	36%	2.2	2.6	2.9	4%	19%	25%
Awareness, Competence and Skills	49%	35%	26%	2.5	2.9	3.3	6%	22%	43%

Table 1: Maturity scorecard: average score (1–5) by domain and company size
NB: Scores in red indicate values below 2.5, reflecting ad hoc practices or no established process. Amber scores range from 2.5 to 3.4 and reflect processes that are only partly in place or applied inconsistently. Green scores start at 3.5 and indicate practices that are managed and applied consistently. None of the domains were fully in the green category. Microcompanies scored either in the red range or at the lower end of the amber range across all five domains. (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

([4]) Governance and documentation; risk management and security by design; vulnerability and patch management; incident response and life-cycle management; and awareness, competence and skills.
([5]) The maturity questions had five levels.

Introduction

Background on the Cyber Resilience Act

Microcompanies and small and medium-sized enterprises (SMEs) ([6]) make up the majority of manufacturers, distributors and importers of products with digital elements in Europe. Manufacturers, large and small, also rely on SMEs as their suppliers. 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]).

It is essential to understand the perspective of SMEs to ensure appropriate support and make sure that the guidelines being developed are practical and usable.

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 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.

This report presents the results of a survey conducted among SMEs to assess their awareness of and preparedness for the CRA. The objective of the report is to understand how SMEs interpret the requirements of the regulation in practice, where they feel confident and where challenges are emerging.

Scope and methodology

The report is based on responses collected through a structured survey of SMEs across different countries, sectors and company sizes. The survey covers awareness of the CRA, understanding of its requirements, existing cybersecurity practices, organisational responsibilities and anticipated challenges related to compliance. It also includes an assessment of maturity across **five domains** ([9]).

Maturity is assessed through a set of questions for each domain, scored on a **scale from 1 to 5**. The scale reflects levels of development, from ad hoc or non-existent practices to structured and

([6]) In this report, SMEs refer to microcompanies and small and medium-sized companies, as defined in Commission Recommendation 2003/361/EC 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).

([7]) 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).

([8]) For more information, please visit the Commission's web page on the implementation of the CRA: https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation

([9]) Governance and documentation; risk management and security by design; vulnerability and patch management; incident response and life-cycle management; and awareness, competence and skills.

consistently applied processes. Domain scores are calculated as the average of the scores for the relevant questions.

The survey received 194 responses. For multi-select questions, counts reflect how many respondents selected each option, so totals may exceed 194. As participation was voluntary and limited to professionally engaged respondents, the **results should not be considered representative of the wider EU SME population.**

The report begins with an overview of the respondent profile, followed by an assessment of respondents' awareness and understanding of the CRA. It then explores current practices and levels of preparedness before examining the key challenges SMEs expect and the types of support they require. The analysis also considers organisational maturity levels and preferred communication channels. The report concludes with a set of recommendations based on the findings.

Where relevant, qualitative input has been used to complement the survey results and provide additional context.

Limitations. As **participation was voluntary**, the sample is likely to reflect a more engaged group of SMEs. This should be considered when interpreting the findings, as overall levels of awareness and preparedness across the broader SME population may be lower.

1. Survey population

The following section describes the SMEs that responded to the survey. This population is an important factor in interpreting the results, since gaps in maturity and support needs may differ significantly depending on company size, market reach and role in the supply chain.

1.1 Geographical coverage and company profiles

The survey received responses from 31 countries and geographical groupings. In total, **25 EU Member States** are represented, alongside Norway, Switzerland and the United Kingdom. In addition, respondents reported operating EU-wide and EEA-wide. Two respondents indicated that they operate globally outside Europe.

The largest shares of responses were from companies operating across multiple Member States, with 30 responses (15 %), and in Germany, with 29 (also 15 %). France, Poland and Sweden each contributed 11 responses, while Austria provided 10. Belgium and Finland are represented by 8 responses each.

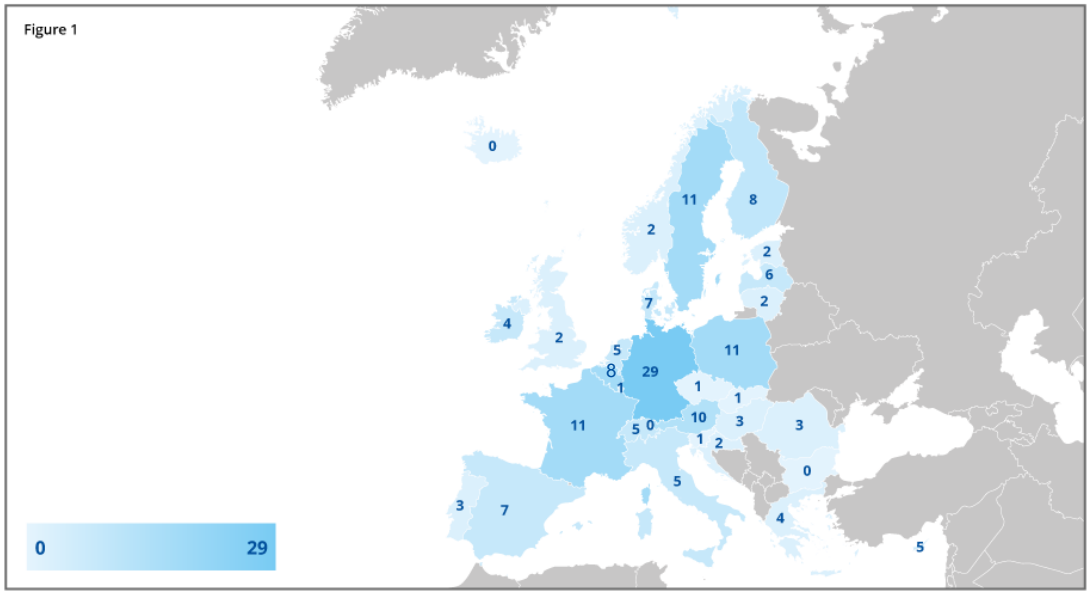

Figure 1. Geographical distribution of survey responses (Q1.1) (n = 194). Countries are shaded according to the number of respondents indicating operations in that country. In total, 25 EU Member States are represented. Respondents operating EU-wide (n = 30), EEA-wide (n = 3) or globally (n = 2) are included in the survey total (n = 194) but are not assigned to a specific country and are therefore not shown on the map. EEA = European Economic Area.

All SME sizes were represented in the results. There were 72 medium-sized companies (37 %), 69 small companies (36 %) and 53 microcompanies (27 %). In terms of turnover, smaller SMEs are highly represented in the results, as 63 % of respondents report annual revenues of below EUR 10 million. Most respondents operate either across several Member States (41 %) or within a single country (33 %). A smaller share, around a quarter (26 %), report operating on a global scale.

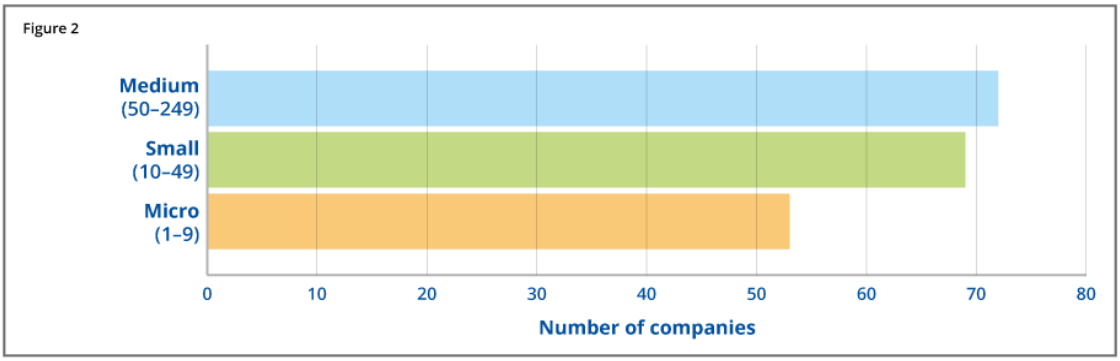

Figure 2: Company size (Q1.2)
NB: Numbers in brackets are numbers of employees.

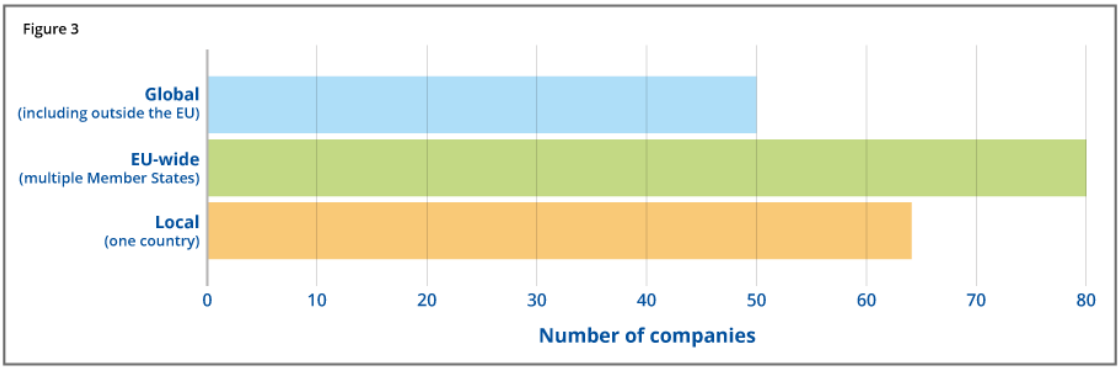

Figure 3: Annual turnover (Q1.3)

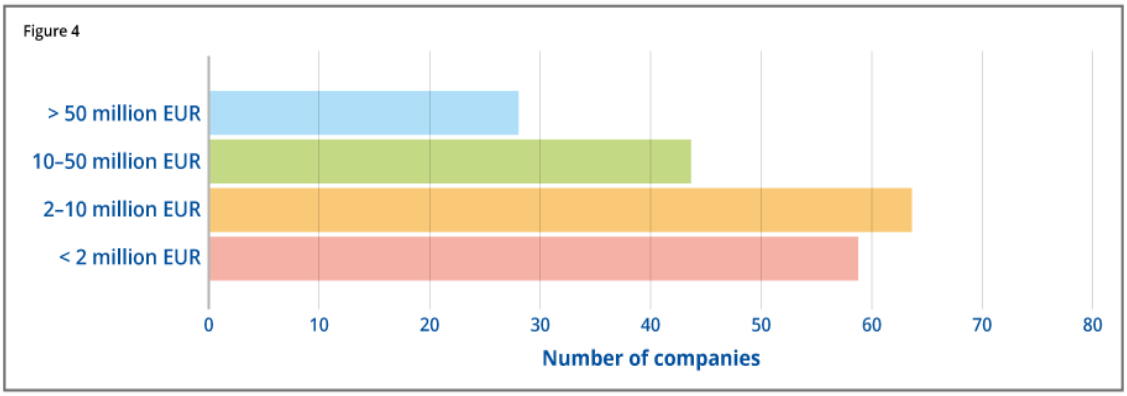

Figure 4: Main market (Q1.4)

Regarding the companies' roles, software developers had the largest group of responses (80 respondents, 41 %). Service providers and integrators were second (53, 27 %) and product manufacturers were third (39, 20 %). Importers, distributors and authorised representatives together provided about 26 % of responses. These roles have different obligations under the CRA. Importers, distributors and authorised representatives are subject to specific requirements that differ from those applying to manufacturers, particularly regarding documentation and conformity assessment for products they place on the EU market without modification.

1.2 Scope of the Cyber Resilience Act

One of the aims of the survey was to gain an understanding of the overall awareness of the CRA – that is, whether SMEs know the regulation exists and if they consider themselves to fall within the scope of the regulation.

In total, 135 respondents (70 %) replied that they are in the scope of the CRA. At the same time, there is still some uncertainty: 39 respondents (20 %) were not sure and 20 (10 %) believed that the CRA does not apply to them.

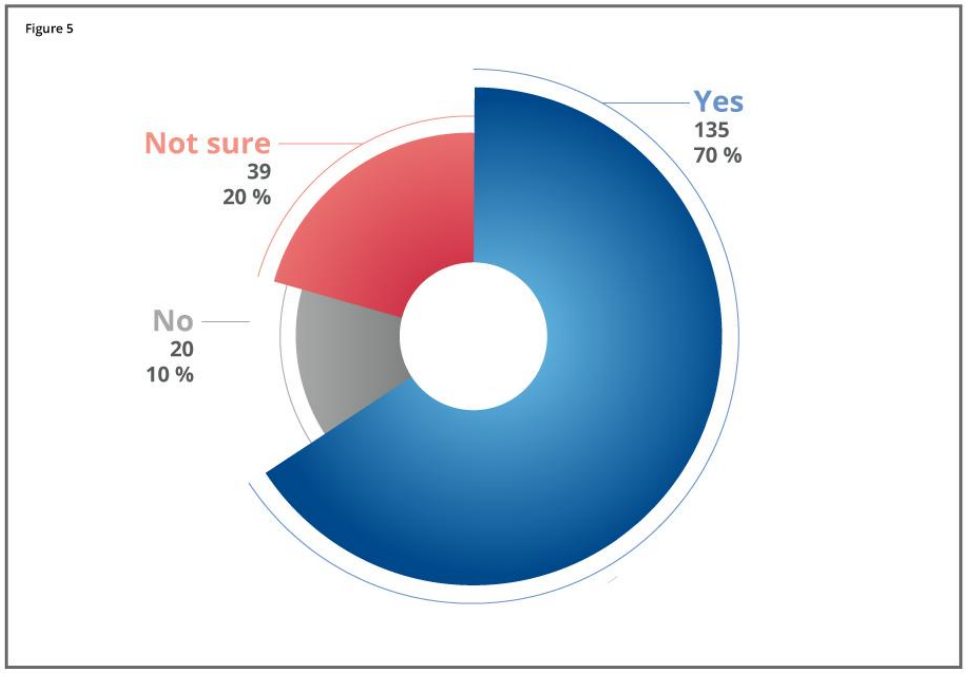

Figure 5: CRA scope (Q1.6: Do you fall under the CRA scope?)

The results suggest that, although there is general awareness of the CRA, there is still some confusion among SMEs when it comes to determining whether and how the regulation applies to them in practice.

> Approximately one in five respondents were not sure whether the CRA actually applies to their products. This uncertainty exists most often among the importers, distributors and service providers, for whom understanding whether they are within the scope depends heavily on how the supply chain is set up.

2. Cyber Resilience Act awareness and understanding

This section analyses how SMEs rate their understanding of what the CRA requires in practice in terms of product security. The responses have a consistent pattern. SMEs' awareness of the regulation does not necessarily translate into confidence about what they need to do to comply with it.

2.1 Prior awareness of the Cyber Resilience Act

Some level of prior awareness of the CRA was reported by the SMEs. In total, 128 out of 194[10] respondents (66 %) indicated that they were aware of the regulation before taking the survey. However, this primarily reflects general awareness of its existence rather than a detailed understanding of its requirements.

ANSWER OPTION	ANSWERS	RATIO
Yes	128	65.98%
No	16	8.25%
Not sure	30	15.46%

Table 2: Prior awareness of the CRA (Q2.1: Before this survey, were you aware of the CRA?) (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

Awareness varies by company size. It is highest among medium-sized companies (94 %), followed by small companies (74 %) and microcompanies (62 %). In the microcompany segment, 38 % said they either were unsure or had not heard of the CRA.

([10]) Overall responses 194; 174 responses within the scope of the CRA. "No Answer" responses (n = 20, 10.31%) are excluded from all figures

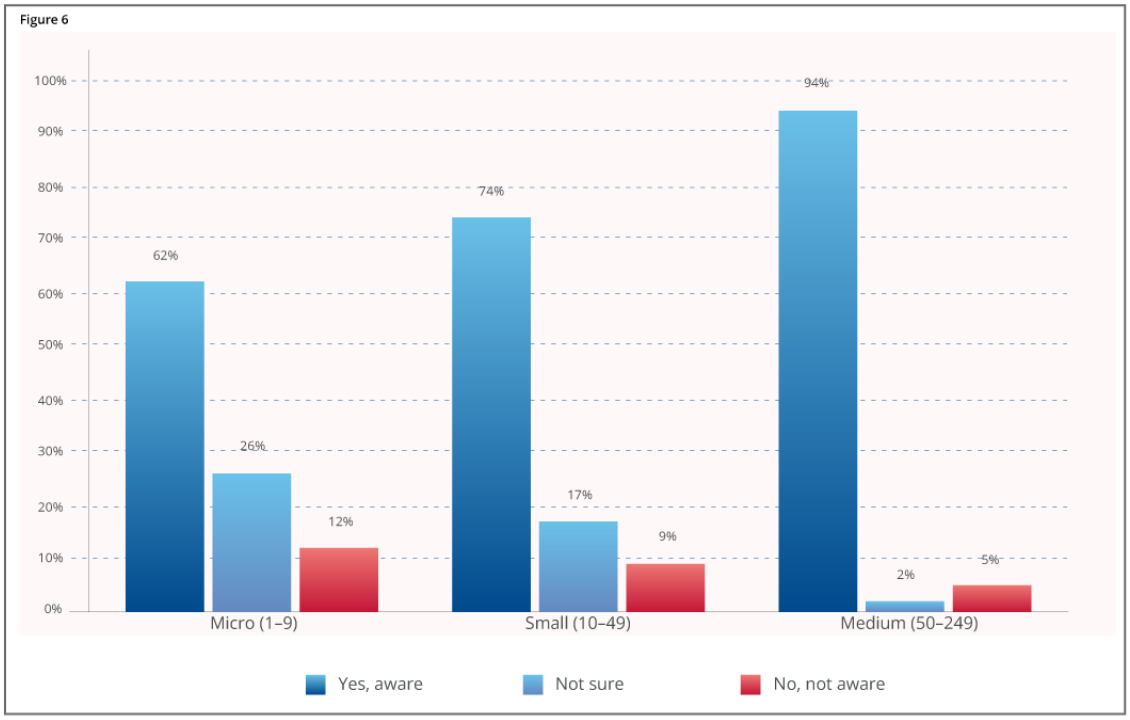

Figure 6: Prior awareness of the CRA by company size (percentage of respondents)
NB: Numbers in brackets are numbers of employees. (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

2.2 Understanding of Cyber Resilience Act obligations

Responses about SMEs' understanding of specific CRA topics were more mixed. Across all areas, most SMEs rated their knowledge as moderate or limited. Higher ratings were more common for broader topics. Understanding of essential cybersecurity requirements and of obligations in relation to vulnerability handling were assessed as good or very good by 31 % and 28 % of respondents, respectively. Understanding of obligations in relation to secure development followed at 29 %.

> Even among the SMEs that reported already being familiar with the CRA, most still rated their understanding of documentation and conformity assessment as limited or moderate. A similar trend can be observed across companies of all sizes, suggesting that this is not limited to a specific group of SMEs. While many organisations are aware of the regulation, this awareness does not necessarily translate into preparedness for its more detailed and operational requirements.

Understanding is lower when it comes to documentation and conformity assessment. Only 13 % of respondents report a good or very good understanding of documentation requirements, and 14 % for conformity assessment.

CRA TOPIC AREA	NONE	LIMITED	MODERATE	GOOD	VERY GOOD
Essential cybersecurity requirements	7%	24%	28%	25%	6%
Vulnerability handling obligations	10%	22%	29%	23%	5%
Secure development and security by design	7%	25%	29%	20%	9%
Required documentation	13%	29%	35%	9%	4%
Conformity assessment and compliance	14%	40%	22%	10%	4%

Table 3: Understanding of the CRA (percentage of respondents) (Q2.2: How would you rate your understanding of the CRA?) (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

3. Current practices and compliance readiness

This section brings together three elements: responsibility for cybersecurity within the organisation, steps already taken towards compliance and the technical practices currently in place. Taken together, they show the SMEs' starting point as they begin to work towards CRA compliance.

3.1 Cybersecurity responsibility

Having a person responsible for cybersecurity is strongly linked to company size and aligns closely with higher maturity scores across all five domains covered in the survey.

93 % of medium-sized companies reported having an internal staff member responsible for cybersecurity. In contrast, 57 % of microcompanies said that they have no designated responsibility for cybersecurity at all.

Cybersecurity responsibility	Micro (1-9)	Small (10-49)	Medium (50-249)
Internal staff member	38%	52%	93%
External provider	5%	9%	3%
No one responsible	57%	39%	5%

Table 4: Cybersecurity responsibility by company size (percentage of respondents) (Q3.1: Do you have a person responsible for cybersecurity (internal or external)?) (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

This gap helps explain many of the maturity differences seen in Sections 4 and 5. For microcompanies in particular, guidance needs to be designed for organisations that may not have any in-house cybersecurity expertise. It should avoid assuming prior knowledge of security frameworks or specialised terminology.

3.2 Prior compliance activity and technical practices

Most respondents report some level of prior compliance activity. Ensuring compliance with International Organization for Standardization standard 27001 is the most common, mentioned by 101 respondents (52 %), followed closely by measures related to the General Data Protection Regulation (94 respondents, 48 %) and internal security audits (86 respondents, 44 %). European Community conformity (CE) marking has been undertaken by 62 respondents (32 %), and product-specific

certification such as under Common Criteria or the EU cybersecurity certification (EUCC) scheme has been undertaken by 44 respondents (23 %). 32 respondents (16 %) have undertaken no formal compliance activity whatsoever. The rate of no prior compliance is significantly higher among microcompanies (25 %) and small companies (22 %) than among medium-sized ones (6 %).

> Threat modelling and software bills of materials stand out as the areas with the biggest gaps between current SME practices and what the CRA expects. Practical, easy-to-follow guidance, especially for organisations without dedicated security teams, would help address one of the clearest needs identified in the survey.

Answer option	Answers	Ratio
ISO/IEC 27001 (information security management)	101	52.06%
CE marking for EU product regulations	62	31.96%
GDPR compliance measures	94	48.45%
NIS2 related security requirements	29	14.95%
Sector-specific regulations (e.g. medical devices, automotive, payments)	15	7.73%
Internal security audits or self-assessments	86	44.33%
Certification schemes for products (e.g. Common Criteria, EUCC)	44	22.68%
We have not followed any cybersecurity certification or regulatory compliance process before	32	16.49%
Other	10	5.15%

Table 5: Implementation of certifications, compliance measures or audits (Q3.2: Have you previously implemented any formal cybersecurity certifications, regulatory compliance measures or audits for your organisation or products?)
NB: GDPR, General Data Protection Regulation; IEC, International Electrotechnical Commission; ISO, International Organization for Standardization; NIS2, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj). (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

On the technical practice side, most respondents implement at least one recognised security practice. Secure software development practices are the most common (99 respondents, 51 %), followed by secure coding guidelines (84, 43 %) and code review processes (82, 42 %). Vulnerability management processes are implemented by 80 respondents (41 %). Two practices stand out for their low level of adoption despite being explicit CRA requirements: threat modelling is used by only 47 respondents (24 %) and software bills of materials are used by 67 (35 %). Both are required for most in-scope products under the CRA.

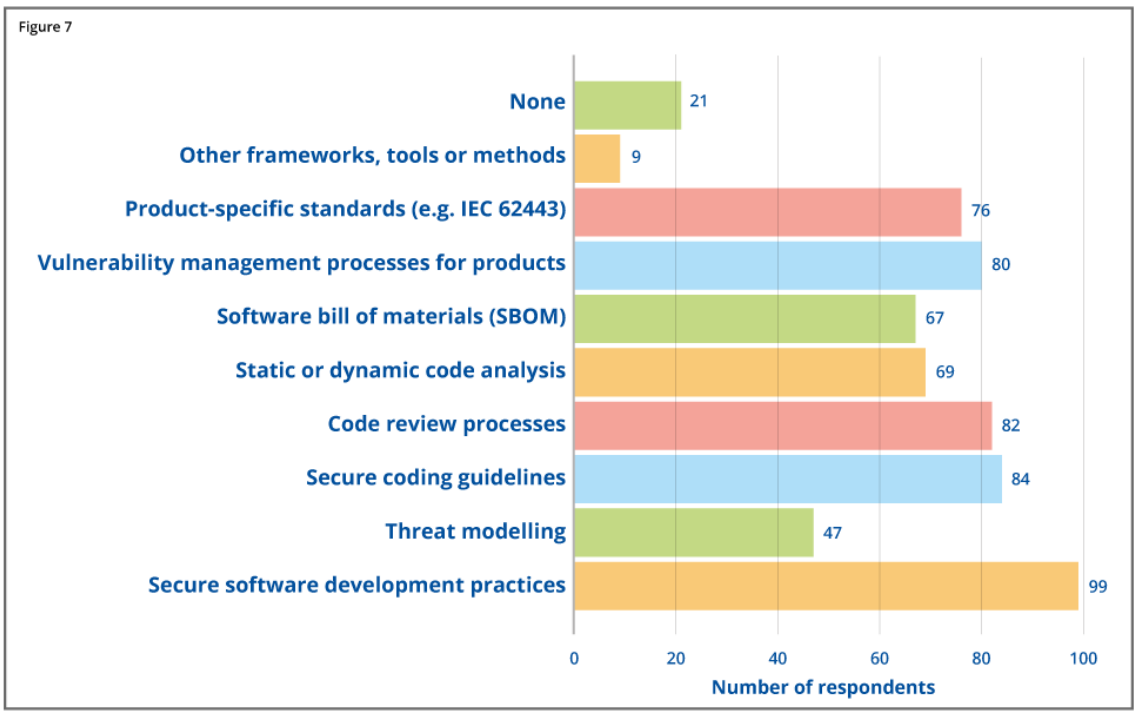

Figure 7: Technical practices and standards (Q3.3: Which of the following technical practices or standards do you currently implement for your products with digital elements?) (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

4. Compliance challenges and support needs

This section analyses where companies expect to have the most difficulties, especially when it comes to integrating security by design into their products. It also highlights the areas that companies consider the most challenging and the types of support they would find most useful. These insights provide an indication of where guidance could be most effectively targeted.

4.1 Anticipated challenges

Only 21 of respondents (11 %) said they are confident they will not face difficulties when integrating security by design into their products and processes. The majority are not that confident. Nearly half (91, 47 %) expect to face challenges, while 62 (32 %) remain unsure. This indicates that overall confidence in current readiness is low.

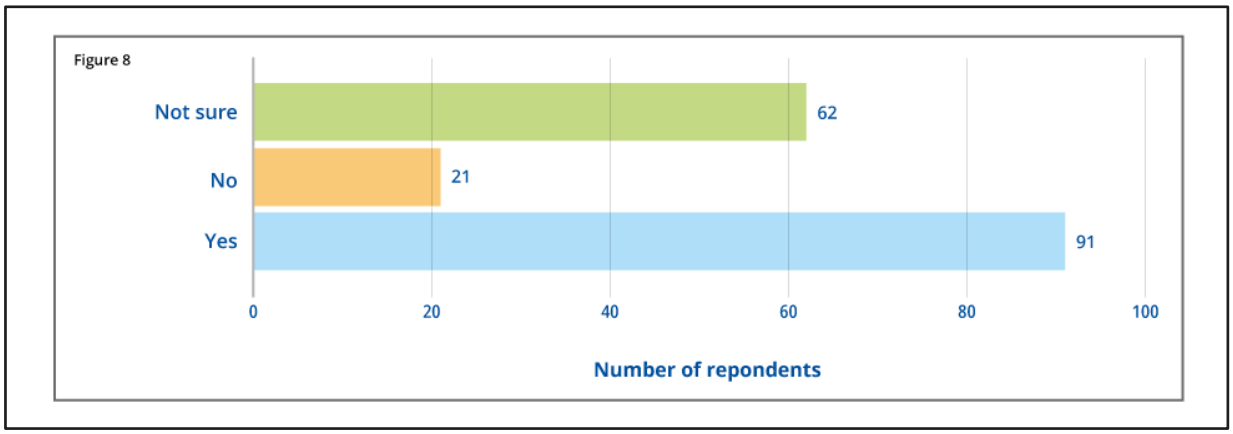

Figure 8: Difficulties integrating cybersecurity by design/default principles (Q4.1: Do you expect any difficulties integrating cybersecurity by design/default principles into your products or systems? Ensuring security is included in the design of products and activated by default) (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

Documentation requirements and conformity assessment procedures are the most commonly reported challenges, with each selected 128 times by respondents. Resource constraints and financial impact also emerge as major concerns, together accounting for more than 200 selections. This suggests that the expected cost and resource burden of compliance is a significant issue for SMEs, regardless of their current level of technical maturity. In addition, product classification was identified as a challenge by 73 respondents, reinforcing earlier findings that many SMEs remain uncertain about whether and how the CRA applies to their products or services.

Answer option	Answers	Ratio
Understanding CRA obligations	119	61.34%
Understanding how to classify products (default, important, critical)	73	37.63%
Understanding the required documentation	128	65.98%
Understanding conformity assessment processes	128	65.98%
Technical expertise related to cybersecurity	75	38.66%
Established development processes that integrate cybersecurity requirements	67	34.54%
Vulnerability handling and patching	73	37.63%
Resource limitations (staff or time)	119	61.34%
Financial impact (cost of implementation)	109	56.19%
Other	9	4.64

Table 6: Challenge areas (Q4.1.a: In which areas do you expect challenges?) (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

The overall results in this area suggest that SMEs are facing challenges not only in implementing technical measures, but also in navigating the complexity of the regulatory requirements.

4.2 Demand for support measures

The survey results indicate a consistently high demand for support across all areas, with very few respondents stating that they do not need additional assistance. Overall, SMEs appear to prioritise practical and easy-to-apply forms of support over general or purely theoretical guidance.

Templates were selected as the most requested form of support. In particular, respondents highlighted the need for templates related to technical documentation (73 %), secure development practices (71 %) and vulnerability-handling processes (56 %). There is also significant demand for technical tools that could assist with compliance assessments, identified by 68 % of respondents. At the same time, many SMEs are seeking clearer and more structured explanations of regulatory requirements. Step-by-step guidance for CRA documentation was requested by 66 % of respondents, while explanations of obligations, explanations of organisational roles and guidance on conformity assessment procedures were each selected by approximately 59 %.

Answer option	Answers	Ratio
for required technical documentation	142	73.2%
for risk assessment	100	51.55%
for vulnerability handling processes	108	55.67%
for documenting secure development practices in line with the CRA	138	71.13%
None of the above	3	1.55%

Table 7: Templates and checklists to support compliance with the CRA (Q4.2.a: What type of support would be most useful to support your efforts to comply with the CRA?) (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

Answer option	Answers	Ratio
Simple guidelines on how to establish development processes that integrate cybersecurity requirements (security by design/default)	111	57.22%
Practical guides on risk assessment methodologies	108	55.67%
Step-by-step guide for CRA documentation	128	65.98%
Guidance on CRA product classification (default, important, critical)	98	50.52%
Guidance on conformity assessment and CE marking	114	58.76%
None of the above	4	2.06%

Table 8: Guidance materials to support compliance with the CRA (Q4.2.b: What type of support would be most useful to support your efforts to comply with the CRA?) (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

Answer option	Answers	Ratio
Access to test environments or sandboxes	66	34.02%
Examples or use cases relevant to your sector	103	53.09%
Technical tools that help assess compliance	132	68.04%
None of the above	19	9.79%

Table 9: Operational or technical support to support compliance with the CRA (Q4.2.c: What type of support would be most useful to support your efforts to comply with CRA?) (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

Answer option	Answers	Ratio
Explanation of CRA obligations	115	59.28%
Explanation of roles and responsibilities for importers, distributors, or authorised representatives	115	59.28%
Clarification on lifecycle requirements	106	54.64%
None of the above	10	5.15%

Table 10: Regulatory or legal explanations to support compliance with the CRA (Q4.2.d: What type of support would be most useful to support your efforts to comply with CRA?) (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

Financial support was selected by the largest number of respondents. This reinforces the earlier finding that cost and resource challenges are major concerns for SMEs. Companies are looking not only for clarity around the CRA requirements, but also for ways to make compliance more manageable, less time-consuming and more affordable in practice.

Answer option	Answers	Ratio
Financial support	142	73.2%
Other	6	3.09%

Table 11: Other forms of support for compliance with the CRA (Q4.2.e: What type of support would be most useful to support your efforts to comply with CRA?) (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

The results suggest that SMEs are looking for support that is practical, accessible and easy to apply in their day-to-day work.

5. Product security maturity

This section assesses initial maturity levels using a five-point scale based on 17 questions. These cover governance and documentation; risk management and security by design; vulnerability and patch management; incident response and product life cycle management; and awareness, competence and skills. The scale had five values, from level 1, where no processes are in place, to level 5, where processes are optimised, integrated and continuously improved.

Maturity levels:
1 – processes are not implemented;
2 – processes are informal or ad hoc (inconsistent, dependent on individuals);
3 – processes are documented but not consistently applied;
4 – processes are consistently applied and regularly reviewed;
5 – processes are measured, monitored and continuously improved.

Table 12 shows where respondents currently stand. It shows the shares of organisations operating at the lowest two levels (no formal process or ad hoc practices) and the highest two levels (managed and optimised), along with average scores for each domain by company size group. This serves as a useful reference point before moving into the more detailed findings that follow.

Domain	At risk (L1 + L2)			Avg maturity score			On track (L4 + L5)		
	Micro	Small	Medium	Micro	Small	Medium	Micro	Small	Medium
Governance and Documentation	49%	19%	36%	2.5	3.0	3.5	9%	41%	53%
Risk Management and Secure-by-Design	49%	36%	26%	2.4	2.8	3.2	9%	23%	40%
Vulnerability and Patch Management	40%	30%	19%	2.6	3.0	3.3	8%	25%	44%
Inicident Response and Lifecycle	49%	38%	36%	2.2	2.6	2.9	4%	19%	25%
Awareness, Competence and Skills	49%	35%	26%	2.5	2.9	3.3	6%	22%	43%

Table 12: Maturity by domain: lowest and highest scores (percentage of respondents) and average maturity score by company size(N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

In terms of average maturity score, the weakest area across companies of all sizes is incident response and product life-cycle management. Governance and documentation shows the largest gap between microcompanies and medium-sized companies. For microcompanies, risk management and security by design has the second-lowest average score of any domain, at 2.4. It is also notable that none of the microcompanies have reached level 5 in incident response, product life cycle management or staff training.

5.1 Governance and documentation

This topic covers four main areas: written cybersecurity rules related to product security, clearly defined responsibilities for security, maintenance of product-level technical documentation, and regularly reviewed product security and documentation quality.

The most visible aspect in this area is the difference between company sizes. 64 % (level 4 and 5) of medium-sized companies report having written rules that are also followed in practice. Microcompanies are less developed in this area: more than half of respondents are at the lower two maturity levels, meaning that formal processes are either missing or handled in a more informal and ad hoc way.

The results also show lower maturity around technical documentation topics. Many SMEs indicated that their documentation is not yet fully complete or consistently maintained across products. At the same time, the level of detail required under CRA Annex VII appears to go beyond what most SMEs currently have in place.

Maturity level	Micro (1-9)	Small (10-49)	Medium (50-249)
Level 1 - None / No process	17%	9%	8%
Level 2 - Ad hoc / Informal	36%	15%	8%
Level 3 - Documented	29%	35%	21%
Level 4 - Managed / Consistent	12%	35%	51%
Level 5 - Optimised / Integrated	7%	5%	13%

Table 13: Distribution across maturity levels for the governance domain by company size (percentage of respondents) (Q5.1: Do you have written rules or guidelines in your organisation covering cybersecurity, product security and CRA-related obligations (risk assessment, secure by design, updates, documentation)?) (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure, percentages are rounded to the nearest whole number)

5.2 Risk management and security by design and default

Practices related to risk assessment and secure development vary across respondents. The survey examined whether risk assessments inform design decisions, whether security is considered early in development and whether security checks are carried out before release.

Risk assessment has lower levels of maturity, especially among smaller organisations. Many microcompanies either do not assess risks in a structured way or rely on informal approaches, and none have reached level 5. Similar gaps appear in development practices. Security is not consistently built in from the beginning, and in some cases is introduced later in the process. Around 24 % of microcompanies report addressing cybersecurity risks at a later stage despite the security by design approach of the CRA. This suggests that security is often still treated as a separate step rather than an integral part of product development.

Around 24 % of microcompanies report addressing security by design at a later stage despite the security by design approach of the CRA. This suggests that security is often still treated as a separate step rather than an integral part of development.

Maturity level	Micro (1-9)	Small (10-49)	Medium (50-249)
Level 1 - None / No process	7%	2%	6%
Level 2 - Ad hoc / Informal	24%	22%	15%
Level 3 - Documented	48%	37%	30%
Level 4 - Managed / Consistent	17%	35%	36%
Level 5 - Optimised / Integrated	5%	5%	13%

Table 14: Distribution across maturity levels for the use of security-by-design principles by company size (percentage of respondents) (Q6.2: Are your products designed with cybersecurity in mind from the beginning (secure configurations, minimal exposure, strong default settings)?) (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure, percentages are rounded to the nearest whole number)

Medium-sized companies generally report more-developed practices in terms of using security by default principles, with 49 % reaching maturity level 4 or 5. At the same time, organisations operating with regularly reviewed and consistently maintained processes remain in the minority. This suggests that, while many companies have started introducing relevant measures, these practices are not yet consistently integrated into day-to-day operations.

5.3 Vulnerability and patch management

The survey identified noticeable differences in how organisations manage vulnerabilities and software security updates. Questions focused on vulnerability tracking, update distribution, and the recording of identified issues and remediation activities.

The largest differences appear in vulnerability tracking. Many microcompanies still rely on informal or reactive methods, and formal processes are often missing altogether. Consequently, a large share of respondents remain concentrated in the lower maturity categories. Medium-sized companies show a more balanced distribution across maturity levels and are more likely to report established and structured procedures. Nearly half (48 %) fall within level 4 or 5.

Maturity level	Micro (1-9)	Small (10-49)	Medium (50-249)
Level 1 - None / No process	17%	6%	6%
Level 2 - Ad hoc / Informal	36%	25%	12%
Level 3 - Documented	36%	37%	34%
Level 4 - Managed / Consistent	10%	26%	30%
Level 5 - Optimised / Integrated	2%	6%	18%

Table 15: Distribution across maturity levels for vulnerability tracking by company size (percentage of respondents) (Q7.1: Do you have a process to receive, record and track vulnerabilities in your products if they are reported by customers, researchers or internal staff?) (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

The findings show a gap between smaller and larger SMEs. Microcompanies are more often positioned at lower maturity levels, where processes are still informal or only partly established, while medium-sized organisations generally demonstrate more structured and mature practices. At the same time, fully integrated and consistently applied practices remain relatively uncommon across the sector overall.

Software update management shows higher maturity overall, although differences between smaller and larger SMEs remain visible. Medium-sized companies more often report structured and well-established update management practices, while microcompanies are still more likely to rely on less mature or only partially formalised approaches. Fully mature practices remain uncommon among the smallest organisations.

- Vulnerability management within smaller SMEs often remains informal or reactive.
- Significant differences persist between microcompanies and medium-sized organisations in the use of structured processes.
- Documentation and records are often not consistently maintained.

A similar pattern can also be seen in record-keeping practices. Many respondents reported that formal record-keeping processes either are missing or rely on informal and scattered documentation. Even in organisations where procedures exist, records are not always maintained in a fully consistent or systematic way.

5.4 Incident response and product life cycle management

This area received the lowest average score (2.61). It covers practices related to incident response planning, product life-cycle management policies and the use of lessons learned from past incidents.

The findings show particularly low levels of maturity among microcompanies. More than one third (36 %) reported having no incident response plan in place, while only 2 % indicated that their plans are tested and regularly reviewed.

Medium-sized companies demonstrate comparatively stronger practices, with 43 % reporting the existence of a documented incident response plan and 21 % indicating that their processes are either regularly tested or integrated into broader governance structures. However, even among these organisations, consistent testing and ongoing operational use remain relatively limited.

> One takeaway is the potential for practical support to improve the situation. A simple incident response plan template for small organisations could be a useful support measure, especially if combined with clear guidance on when and how to report vulnerabilities, including how to use ENISA's Single Reporting Platform.

Product life cycle management shows similar patterns. Among microcompanies, 58 % either lack a formal policy or manage it informally, and none has reached level 5. This means that many microcompanies will need to introduce a formal policy where none currently exists, including provisions for support periods and end-of-life timelines.

Lifecycle policy	Micro (1-9)	Small (10-49)	Medium (50-249)
Level 1 - No lifecycle policy	29%	19%	18%
Level 2 - Information shared informally	29%	22%	16%
Level 3 - Policy documented	33%	37%	34%
Level 4 - Policy clear and communicated	10%	19%	24%
Level 5 - Enforced, periodically updated	0%	5%	8%

Table 16: Distribution across maturity levels for product life cycle policy by company size (percentage of respondents) (Q8.2: Is there a defined product life-cycle policy for your products, including support periods, update timelines and end-of-support or end-of-life information?) (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

5.5 Awareness, competence and skills

People-related factors play an important role in product security. The survey covered training, security culture, threat awareness and engagement with the wider cybersecurity community.

Training remains a weak area. None of the microcompanies or small companies reported having formal, role-specific and documented training in place. Among medium-sized companies, only 12 % have reached that level. In practice, knowledge is most often shared informally, particularly in microcompanies.

Maturity level	Micro (1-9)	Small (10-49)	Medium (50-249)
Level 1 - None / No process	12%	2%	5%
Level 2 - Ad hoc / Informal	45%	29%	19%
Level 3 - Documented	29%	49%	30%
Level 4 - Managed / Consistent	14%	20%	34%
Level 5 - Optimised / Integrated	0%	0%	12%

Table 17: Distribution across maturity levels for staff training by company size (percentage of respondents) (Q9.1: Are relevant staff in your organisation trained or informed about secure development practices and vulnerability-handling requirements?) (N = 194. "No Answer" responses (n = 20, 10.31%) are excluded from this figure)

6. Communication and information channels

The survey also explored how SMEs access information and the role of industry associations. The sample included 90 members and 84 non-members of industry associations, indicating that a substantial share of SMEs operate outside formal association networks.

The findings show a strong preference for practical and directly applicable support. Hands-on guidance and templates were identified by 134 respondents (69 %), making them the most requested form of assistance. Training sessions and webinars followed closely, selected by 116 respondents (60 %), while 110 respondents (57 %) highlighted the importance of clear information on timelines and implementation deadlines. In addition, 109 respondents (56 %) expressed interest in sector-specific examples and good practices. Taken together, the results suggest that SMEs are primarily seeking support that can be easily translated into practical action within their organisations.

Which of the following types of information would you be interested in related to the CRA?	Answers	Ratio
Updates on CRA implementation, e.g. regulatory deadlines or regulatory changes	110	56.7%
Training or webinars on CRA compliance	116	59.79%
Practical CRA guidance, templates or checklists for documentation and risk assessment	134	69.07%
Examples of sector-specific good practices or use cases related to CRA	109	56.19%
Technical tools to support compliance (for example test environments or sandboxes)	81	41.75%
Other	3	1.55%

Table 18: Information preferences by company size (Q10.2: Which of the following types of information would you be interested in related to the CRA?) (N = 194, multiple responses were permitted. Percentages are calculated based on all respondents)

The survey results show that SMEs rely on a range of different information channels rather than one clearly preferred source. Webinars and online sessions are used most frequently, selected by 111 respondents (57 %). EU-level websites and helpdesks were mentioned almost as often, by 109 respondents (56 %), followed closely by national cybersecurity authorities, selected by 106 respondents (55 %). Industry associations are used by 90 respondents (46 %), while ENISA channels were identified by 72 respondents (37 %). Overall, usage is fairly evenly distributed across the different channels, with no single source standing out as dominant.

The findings further indicate that most respondents use multiple information sources at the same time rather than relying on a single communication channel. National authorities, industry associations and EU-level platforms are commonly consulted in parallel. This suggests that outreach efforts are likely to be more effective when information is distributed across several channels rather than confined to a single central source.

7. Findings and recommendations

Around two thirds of SMEs (66 %) stated that they were familiar with the CRA before participating in the survey, suggesting a relatively broad level of general awareness among the respondents. However, this awareness does not yet seem to translate into a deeper understanding of what the CRA will actually require. Across the topics covered in the survey, respondents most often described their knowledge as moderate or limited, with the lowest confidence levels reported in areas such as conformity assessment and technical documentation.

The following sections examine these findings in more detail and present recommendations aimed at addressing the identified gaps and support needs.

7.1 Documentation and conformity assessment

Around two thirds of respondents (66 %) reported that they were familiar with the CRA before taking the survey.

Despite this, the results show that SMEs' understanding of specific requirements is limited. Lower levels of understanding are reported in areas such as conformity assessment and technical documentation. These are the areas with the most clearly defined procedural requirements, yet more than half of respondents described their understanding as limited. The same pattern appears across all company size groups and is most pronounced among small companies, with 62 % reporting limited understanding of conformity assessment.

The same trend emerges in several parts of the survey. Documentation and conformity assessment rank lowest in terms of understanding, while also appearing at the top of both anticipated challenges and requested support. This points to a clear priority. General guidance on topics like risk assessment or vulnerability handling is useful, but on its own it is often not enough. Many SMEs are looking for more practical support, especially around how to create the documentation and processes required for CRA compliance in practice.

7.2 Microcompanies as a distinct audience

Among microcompanies, 57 % report that no-one in the organisation is specifically responsible for cybersecurity. Across all domains measured, the maturity gap between microcompanies and medium-sized companies is roughly one full point on a five-point scale. This is not a single issue that can be addressed with one targeted measure. It reflects a more structural constraint.

In many microcompanies, the person expected to deal with CRA requirements is also responsible for development, customer management and day-to-day operations. They need practical tools that help non-specialists get started without reading the full document upfront.

7.3 Templates for technical documentation

73 % of respondents requested templates for required technical documentation, and 71 % requested templates for documenting secure development practices. Both figures are higher than the demand for written guidance materials, tools or regulatory explanations. When given a list of potential outputs and asked to select what would actually help, the respondents chose templates by a clear margin. The four

types listed in the survey with the highest demand, covering technical documentation, secure development practices, vulnerability-handling processes and risk assessment, were each selected by more than half of all respondents. Only 3 of the respondents said they needed none of the listed templates.

7.4 Threat modelling and software bills of materials

Only 24 % of respondents report using threat modelling and 35 % maintain a software bill of materials. These are less widely used than more familiar practices such as code review (42 %) and secure coding guidelines (43 %). Neither practice fits easily into the typical workflow of a small team. Addressing this is less about further explaining their importance and more about showing how they can be applied in practice. Simple, practical examples based on realistic product scenarios, using freely available tools, would probably make adoption easier for SMEs without adding significant cost.

7.5 Incident response and product life cycle management

This is the lowest-scoring area across all SME size groups in the survey, with an average of 2.6 out of 5. Among microcompanies, 36 % said they do not have an incident response plan at all. CRA compliance may therefore be facilitated by means of a simple and practical incident response template tailored to small organisations. This should be accompanied by clear guidance on when and how to use ENISA's Single Reporting Platform.

7.6 Financial support

Out of all respondents who answered the open question on support needs, 142 identified financial support as a priority. This is the highest figure reported for any single item in this section. The responses indicate that SMEs are working with limited time and resources. As a result, requests for guidance appear to be driven more by regulatory obligations than by organisational capacity. This has implications for how guidance should be designed. It should provide a practical, step-by-step roadmap that companies can realistically follow. It also needs to be easy to use, without requiring companies to rely on additional tools, external support or consultants, and it should be freely accessible.

7.7 Guidance for small and medium-sized enterprises

50 % of respondents are not members of any industry association, so the distribution of guidance through association networks alone would miss roughly half the target audience. ENISA's own channels reach 37 % directly. Webinars and online sessions ranked first among the preferred information channels (111 respondents, 57 %), followed closely by EU-level websites (109, 56 %) and national cybersecurity authorities (106, 55 %). The three leading channels are almost equal in reach, which confirms that national authorities and industry associations need to be treated as active distribution partners rather than secondary audiences. An initial webinar or online session should accompany each major guidance publication and sector-specific examples should be built into guidance materials wherever possible; 109 respondents explicitly asked for use cases relevant to their sector.

Annex A: Questionnaire and results

1.1: Geographical region / economic area

Answer option	Answers	%
Belgium	8	4.12
Bulgaria	0	0
Czechia	1	0.52
Denmark	7	3.61
Germany	29	14.95
Estonia	2	1.03
Ireland	4	2.06
Greece	4	2.06
Spain	7	3.61
France	11	5.67
Croatia	2	1.03
Italy	5	2.58
Cyprus	5	2.58
Latvia	6	3.09
Lithuania	2	1.03
Luxembourg	1	0.52
Hungary	3	1.55
Malta	0	0
Netherlands	5	2.58
Austria	10	5.15
Poland	11	5.67
Portugal	3	1.55
Romania	3	1.55
Slovenia	1	0.52
Slovakia	1	0.52
Finland	8	4.12
Sweden	11	5.67
Iceland	0	0

Answer option	Answers	%
Liechtenstein	0	0
Norway	2	1.03
Switzerland	5	2.58
United Kingdom	2	1.03
EU-wide (operations in multiple Member States)	30	15.46
EEA-wide (operations in multiple EEA countries)	3	1.55
Global / outside Europe	2	1.03

NB: EEA, European Economic Area.

1.2: Company size (number of employees)

Answer option	Answers	%
Micro (1–9)	53	27.32
Small (10–49)	69	35.57
Medium (50–249)	72	37.11

1.3: Annual turnover

Answer option	Answers	%
< EUR 2 million	59	30.41
EUR 2–10 million	63	32.47
EUR 10–50 million	44	22.68
> EUR 50 million	28	14.43

1.4: Main market

Answer option	Answers	%
Local (within one country)	64	32.99
EU-wide (more than one Member State)	80	41.24
Global (also countries outside the EU)	50	25.77

1.5: Your company's role (select all that apply)

Answer option	Answers	%
Manufacturer of ICT hardware or connected devices	28	14.43
Software developer	80	41.24
Component manufacturer	28	14.43
Final product manufacturer	39	20.10
Importer or distributor of hardware or software products	33	17.01
Service provider or integrator	53	27.32

Answer option	Answers	%
Authorised representative of one of the companies mentioned above	17	8.76
Other	8	4.12

1.6: Do you develop or sell hardware or software products that are likely to fall under the scope of the CRA? The CRA applies to products with digital elements meaning any hardware or software that is connected or can communicate with other devices or networks.

Answer option	Answers	%
Yes	135	69.59
No	20	10.31
Not sure	39	20.10

2.1: Before this survey, were you aware of the CRA?

Answer option	Answers	%
Yes	128	65.98
No	16	8.25
Not sure	30	15.46
No Answer	20	10.31

2.2: How would you rate your understanding of the CRA?

Essential cybersecurity requirements for products with digital elements

Answer option	Answers	%
None	14	7.22
Limited	46	23.71
Moderate	54	27.84
Good	48	24.74
Very good	12	6.19
No Answer	20	10.31

Obligations on vulnerability handling and management

Answer option	Answers	%
None	19	9.79
Limited	43	22.16
Moderate	57	29.38
Good	45	23.20
Very good	10	5.15
No Answer	20	10.31

Secure development / security by design – ensuring security is included in the design of products and activated by default

Answer option	Answers	%
None	13	6.70
Limited	49	25.26
Moderate	57	29.38
Good	38	19.59
Very good	17	8.76
No Answer	20	10.31

Required documentation, including technical documentation

Answer option	Answers	%
None	25	12.89
Limited	57	29.38
Moderate	67	34.54
Good	18	9.28
Very good	7	3.61
No Answer	20	10.31

Necessary conformity assessment and compliance procedures

Answer option	Answers	%
None	27	13.92
Limited	78	40.21
Moderate	42	21.65
Good	20	10.31
Very good	7	3.61
No Answer	20	10.31

3.1: Do you have a person responsible for cybersecurity (internal or external)?

Answer option	Answers	%
Yes, internal staff	112	57.73
Yes, external service provider	10	5.15
No	52	26.80
No Answer	20	10.31

3.2: Have you previously implemented any formal cybersecurity certifications, regulatory compliance measures or audits for your organisation or products? (Select all that apply)

Answer option	Answers	%
ISO/IEC 27001 (information security management)	101	52.06
CE marking for EU product regulations	62	31.96
GDPR compliance measures	94	48.45
NIS2-related security requirements	29	14.95
Sector-specific regulations (e.g. medical devices, automotive, payments)	15	7.73
Internal security audits or self-assessments	86	44.33
Certification schemes for products (e.g. Common Criteria, EUCC)	44	22.68
We have not followed any cybersecurity certification or regulatory compliance process before	32	16.49
Other	10	5.15
No Answer	20	10.31

NB: GDPR, General Data Protection Regulation; IEC, International Electrotechnical Commission; ISO, International Organization for Standardization; NIS2, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

3.3: Which of the following technical practices or standards do you currently implement for your products with digital elements? (Select all that apply)

Answer option	Answers	%
Secure software development practices	99	51.03
Threat modelling	47	24.23
Secure coding guidelines	84	43.30
Code review processes	82	42.27
Static or dynamic code analysis	69	35.57
Software bill of materials (SBOM)	67	34.54
Vulnerability management processes for products	80	41.24
Product-specific standards (e.g. IEC 62443)	76	39.18
Other frameworks, tools or methods	9	4.64
None	21	10.82
No Answer	20	10.31

NB: IEC, International Electrotechnical Commission.

4.1: Do you expect any difficulties integrating cybersecurity-by-design/default principles into your products or systems? Ensuring security is included in the design of products and activated by default

Answer option	Answers	%
Yes	91	46.91
No	21	10.82
Not sure	62	31.96
No Answer	20	10.31

4.1.a: In which areas do you expect challenges? (Select all that apply)

Answer option	Answers	%
Understanding CRA obligations	119	61.34
Understanding how to classify products (default, important, critical)	73	37.63
Understanding the required documentation	128	65.98
Understanding conformity assessment processes	128	65.98
Technical expertise related to cybersecurity	75	38.66
Established development processes that integrate cybersecurity requirements	67	34.54
Vulnerability handling and patching	73	37.63
Resource limitations (staff or time)	119	61.34
Financial impact (cost of implementation)	109	56.19
Other	9	4.64
No Answer	20	10.31

4.2: What type of support would be most useful to support your efforts to comply with the CRA? (Select all that apply)

4.2.a: Templates and checklists

Answer option	Answers	%
For required technical documentation	142	73.20
For risk assessment	100	51.55
For vulnerability-handling processes	108	55.67
For documenting secure development practices in line with the CRA	138	71.13
None of the above	3	1.55
No Answer	20	10.31

4.2.b: Guidance materials

Answer option	Answers	%
Simple guidelines on how to establish development processes that integrate cybersecurity requirements (security by design/default)	111	57.22
Practical guides on risk assessment methodologies	108	55.67
Step-by-step guide for CRA documentation	128	65.98
Guidance on CRA product classification (default, important, critical)	98	50.52
Guidance on conformity assessment and CE marking	114	58.76
None of the above	4	2.06
No Answer	20	10.31

4.2.c: Operational or technical support

Answer option	Answers	%
Access to test environments or sandboxes	66	34.02
Examples or use cases relevant to your sector	103	53.09
Technical tools that help assess compliance	132	68.04
None of the above	19	9.79
No Answer	20	10.31

4.2.d: Regulatory or legal explanations

Answer option	Answers	%
Explanation of CRA obligations	115	59.28
Explanation of roles and responsibilities for importers, distributors or authorised representatives	115	59.28
Clarification on life-cycle requirements	106	54.64
None of the above	10	5.15
No Answer	20	10.31

4.2.e: Other

Answer option	Answers	%
Financial support	142	73.20
Other	6	3.09
No Answer	20	10.31

Maturity related questions

5.1: Do you have written rules or guidelines in your organisation covering cybersecurity, product security and CRA-related obligations (risk assessment, secure by design, updates, documentation)?

Answer option	Answers	%
No rules or guidelines exist	18	9.28
Some very basic ad hoc guidelines exist	30	15.46
Some basic guidelines exist but are not formalised	49	25.26
Written rules exist and are generally followed	62	31.96
Written rules exist, are formally approved, applied consistently and regularly reviewed	15	7.73
No Answer	20	10.31

5.2: Are responsibilities clearly defined in your organisation for cybersecurity, secure development, vulnerability handling, product updates?

Answer option	Answers	%
No responsibilities are defined	14	7.22
Responsibilities exist only informally or ad hoc	44	22.68
Responsibilities exist but are not consistently applied	48	24.74
Responsibilities are defined, documented and generally followed	46	23.71
Responsibilities are clearly defined, documented, communicated, applied consistently and periodically reviewed	22	11.34
No Answer	20	10.31

5.3: Do you maintain product-level technical documentation describing security features, risk assessments, design decisions and update procedures?

Answer option	Answers	%
No product security documentation exists	10	5.15
Some very basic documentation exists	44	22.68
Product security documentation is maintained for most products	55	28.35
Product security documentation is complete and generally updated for most products	46	23.71
Product security documentation is complete, regularly updated and formally approved for all products	19	9.79
No Answer	20	10.31

5.4: Is there a process or management mechanism in your organisation to review product security and documentation quality?

Answer option	Answers	%
No review process exists	18	9.28
Reviews happen informally and ad hoc	51	26.29

Answer option	Answers	%
Reviews are documented but inconsistently applied	51	26.29
Reviews are systematic and lead to improvements	39	20.10
Reviews are systematic, documented, tracked and result in continuous improvements	15	7.73
No Answer	20	10.31

6.1: Do you assess cybersecurity risks for your products with digital elements and use the results to guide your design or development decisions?

Answer option	Answers	%
No risk assessments are performed	39	20.10
Risk assessments are informal or occasional	48	24.74
Risk assessments are documented for most products	60	30.93
Risk assessments are systematic and regularly reviewed	22	11.34
Risk assessments are systematic, formally approved, documented, applied to all products and continuously improved	5	2.58
No Answer	20	10.31

6.2: Are your products designed with cybersecurity in mind from the beginning (secure configurations, minimal exposure, strong default settings)?

Answer option	Answers	%
Cybersecurity is not considered during design	8	4.12
Security is considered only late in development	34	17.53
Security is considered during design for most products	64	32.99
Security by design is standard practice	54	27.84
Security by design is fully integrated, documented, reviewed and continuously improved	14	7.22
No Answer	20	10.31

6.3: Do you perform security checks or testing before releasing or updating a product (for example code review, basic testing or threat analysis)?

Answer option	Answers	%
No security checks are performed	14	7.22
Some basic checks are performed occasionally	51	26.29
Security checks are part of most releases	54	27.84
Security checks are standard and consistently applied	37	19.07
Security checks are comprehensive, standard, systematically documented and continuously improved	18	9.28
No Answer	20	10.31

7.1: Do you have a process to receive, record and track vulnerabilities in your products if they are reported by customers, researchers or internal staff?

Answer option	Answers	%
No vulnerability tracking exists	15	7.73
Vulnerabilities are handled informally	39	20.10
Vulnerabilities are documented and tracked	62	31.96
Vulnerabilities are systematically tracked and reviewed	41	21.13
Vulnerabilities are systematically tracked, reviewed, and lessons learned are integrated into products and processes	17	8.76
No Answer	20	10.31

7.2: Do you have a defined process for creating, testing and delivering security updates for supported products?

Answer option	Answers	%
No update process exists	10	5.15
Updates are created on an ad hoc basis	42	21.65
Updates follow a documented process	52	26.80
Updates follow a defined process and timelines are monitored	50	25.77
Updates follow a defined process, are documented, monitored, and continuously improved	20	10.31
No Answer	20	10.31

7.3: Do you document vulnerabilities, fixes and update history for each product or product version?

Answer option	Answers	%
No documentation exists	15	7.73
Some information is recorded informally	50	25.77
Vulnerability and update information is documented	64	32.99
Documentation is complete and maintained over time	27	13.92
Documentation is complete, maintained, reviewed and formally approved	18	9.28
No Answer	20	10.31

8.1: Do you have a plan for handling security incidents in relation to your products, including how to inform customers or authorities when necessary?

Answer option	Answers	%
No incident response plan exists	37	19.07
A basic, informal plan exists	58	29.90
An incident response plan is documented	57	29.38
The plan is tested, reviewed and improved	13	6.70

Answer option	Answers	%
The plan is documented, tested, reviewed, continuously improved and integrated into governance	9	4.64
No Answer	20	10.31

8.2: Is there a defined product life-cycle policy for your products, including support periods, update timelines and end-of-support or end-of-life information?

Answer option	Answers	%
No life-cycle policy exists	36	18.56
Life-cycle information is shared informally	37	19.07
Life-cycle policy is documented for products	61	31.44
Life-cycle policy is clear, communicated and reviewed	32	16.49
Life-cycle policy is documented, communicated, enforced and periodically updated based on feedback	8	4.12
No Answer	20	10.31

8.3: Do you use lessons learned from incidents, vulnerabilities or customer feedback to improve the security of your product(s)?

Answer option	Answers	%
No structured improvement process exists	22	11.34
Improvements happen occasionally	52	26.80
Improvements are documented and planned	56	28.87
Continuous improvement is part of regular practice	35	18.04
Continuous improvement is systematic, documented, measured and embedded in governance	9	4.64
No Answer	20	10.31

9.1: Are relevant staff in your organisation trained or informed about secure development practices and vulnerability-handling requirements?

Answer option	Answers	%
No training or awareness activities exist	9	4.64
Some informal knowledge sharing exists	51	26.29
Training or guidance is provided occasionally	64	32.99
Training is regular and role-specific	42	21.65
Training is formal, role-specific, documented and continuously updated	8	4.12
No Answer	20	10.31

9.2: Does your organisation encourage cybersecurity culture including, for example, secure behaviour, responsible disclosure and proactive security thinking?

Answer option	Answers	%
Cybersecurity culture is not actively promoted	7	3.61
Security is discussed informally	57	29.38
Security expectations are documented	52	26.80
Security culture is actively promoted and reinforced	46	23.71
Security culture is formally embedded, monitored and continuously improved	12	6.19
No Answer	20	10.31

9.3: Does your organisation actively monitor external cybersecurity information (alerts, advisories, authorities)?

Answer option	Answers	%
No external information is monitored	12	6.19
Information is monitored occasionally	50	25.77
Relevant sources are monitored regularly	59	30.41
Monitoring is systematic and well established	35	18.04
Monitoring is systematic and integrated into governance	18	9.28
No Answer	20	10.31

9.4: Does your organisation engage with external cybersecurity communities (industry groups, peers, authorities)?

Answer option	Answers	%
No engagement or information sharing	8	4.12
Ad hoc or informal engagement	66	34.02
Regular engagement when relevant	61	31.44
Systematic engagement and information sharing	26	13.40
Systematic engagement, information sharing and active contribution integrated into governance	13	6.70
No Answer	20	10.31

10.1: Are you part of an industry association, SME cluster or chamber of commerce?

Answer option	Answers	%
Yes	90	46.39
No	84	43.30
No Answer	20	10.31

10.2: Which of the following types of information would you be interested in related to the CRA? (Select all that apply)

Answer option	Answers	%
Updates on CRA implementation, e.g. regulatory deadlines or regulatory changes	**110**	**56.70**
Training or webinars on CRA compliance	**116**	**59.79**
Practical CRA guidance, templates or checklists for documentation and risk assessment	**134**	**69.07**
Examples of sector-specific good practices or use cases related to the CRA	**109**	**56.19**
Technical tools to support compliance (for example test environments or sandboxes)	**81**	**41.75**
Other	**3**	**1.55**
No Answer	**20**	**10.31**

10.3: Do you have a preferred channel for getting information related to the CRA?

Answer option	Answers	%
National cybersecurity authority	**106**	**54.64**
Industry association or cluster	**90**	**46.39**
EU-level website or helpdesk	**109**	**56.19**
Webinars or online sessions	**111**	**57.22**
ENISA web page and social media	**72**	**37.11**
Other	**2**	**1.03**
No Answer	**20**	**10.31**

Annex B: Abbreviations

CE	European Community conformity
CRA	Cyber Resilience Act (Regulation (EU) 2024/2847)
EEA	European Economic Area
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUCC	European Common Criteria-based cybersecurity certification scheme (EUCC)
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
NIS2	Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (Network and Information Systems Directive 2)
SME	Small and medium-sized enterprise

TP-01-26-010-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