Cyber Resilience Stakeholder Survey v2

Help shape the next generation of cyber resilience tools for small and medium-sized enterprises (SMEs). Your insights will directly influence the development of solutions that align with the Cyber Resilience Act (CRA) and support trusted, secure operations for businesses like yours.

Welcome, and thank you for participating!

This survey is part of a broader initiative to enhance cyber resilience for SMEs. The tools we're developing are designed to meet the core requirements of the Cyber Resilience Act (CRA), helping businesses strengthen their defenses and maintain stakeholder trust.

Your feedback is vital. By sharing your needs and perspectives, you'll help ensure these tools are practical, effective, and aligned with the real challenges faced by SMEs.

The survey will take approximately 10–15 minutes to complete. All responses are anonymous and will be treated confidentially.

Thank you for your contribution.

Funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180

There are 37 questions in this survey.

Organization profile

Hint:

The main factors determining whether an enterprise is an SME are

- **number of employees**
- either **turnover** or **balance sheet total**

Type of Enterprise	Number of Employees	Annual Turnover (EUR)	Balance Sheet Total (EUR)
Microenterprise	< 10	< 2 million	< 2 million
Small Enterprise	< 50	< 10 million	< 10 million
Medium Enterprise	< 250	< 50 million	< 43 million

What is the type of enterprise within the meaning of European Union regulations?

Choose one of the following answers

Please choose **only one** of the following:

○ Microenterprise

○ Small Enterprise

○ Medium Enterprise

○ I do not know

○ Other

What type of products with digital elements do you offer?

Select all that apply

Please choose **all** that apply:

□ Hardware product

□ Software product

□ Other:

Which stakeholders’ group do you belong?

Select all that apply

Please choose **all** that apply:

□ Manufacturer

□ Importer

□ Distributor

□ Open-source software steward - providing support, not a manufacturer

□ Other:

What is your position in the company?

Choose one of the following answers
Please choose **only one** of the following:

○ Owner

○ IT Director

○ IT Specialist

○ Compliance Specialist

○ Prefer not to say

○ Other

CRA readiness

Are you familiar with the CRA requirements?

Choose one of the following answers
Please choose **only one** of the following:

○ Yes

○ No

○ Partially

Are your products subject to CRA conformity assessment?

Choose one of the following answers
Please choose **only one** of the following:

○ Yes

○ No

○ I'm not sure

Respondents' experience

Inventory/ labelling (SBOM - Software Bill of Materials)

How are you currently handling the labelling (tagging), identifying products, components, and libraries processes in your organization?

Choose one of the following answers
Please choose **only one** of the following:

○ We are using a tool / automated process for this (input tools name or details in comments)

○ We are doing it on an informal basis, with no records kept

○ We are doing it using manual processes and written / informal records

○ We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC or other relevant standards, SBOM files, etc., please input details in comment)

○ We are not doing it

○ Other ______________________

Do you use any SBOM preparing / analysis of SBOM supporting tool?

Select all that apply

Please choose **all** that apply:

□ OWASP dependency-check

□ cve-bin-tool

□ Grype

□ Trivy

□ None/No

□ Other:

If you use solutions that support SBOM, what types of standards do you use or would like to use?

Select all that apply

Please choose **all** that apply:

□ None (we have no solutions to support SBOM)

□ SPDX® (Software Package Data Exchange) – Linux Foundation format, ISO/IEC 5962 standard

□ CycloneDX – OWASP Foundation ECMA-424 standard

□ SWID (Software Identification Tagging) – ISO/IEC 19770-2

□ Other:

Risk management

How are you currently handling the Risk Management processes in your organization?

Choose one of the following answers

Please choose **only one** of the following:

○ We are not doing it

○ We are doing it on an informal basis, with no records kept

○ We are doing it using manual processes and written / informal records

○ We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC 27005, 31000, etc., please list standards in comments)

○ We are using a tool / automated process for this (please input tool name or description in comments)

○ Other (please describe in comments)

Make a comment on your choice here:

Do you use any governance, risk management, and compliance (GRC) supporting tools?

Choose one of the following answers

Please choose **only one** of the following:

○ Yes (list in comments)

○ No

Make a comment on your choice here:

Vulnerability management

How are you currently handling the Vulnerability management processes in your organization?

Choose one of the following answers

Please choose **only one** of the following:

○ We are not doing it

○ We are doing it on an informal basis, with no records kept

○ We are doing it using manual processes and written / informal records

○ We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC 30111, 29147, etc., list in comments)

○ We are using a tool / automated process for this (please input tool name or description in comments)

○ Other (please describe in comments)

Make a comment on your choice here:

Is vulnerability classification implemented in your organization?

Choose one of the following answers

Please choose **only one** of the following:

○ Own (internal) classification

○ Compliant with standard / guideline / regulation (e.g. CVSS, please list them in comments)

○ No

○ Other (please describe in comments)

Make a comment on your choice here:

What types of notification channels does your organization provide for reporting and communicating detected, registered, and resolved vulnerabilities?

Select all that apply

Please choose **all** that apply:

- □ None
- □ E-mail
- □ Dashboard / Internal System / Incident Response Platform
- □ Public Advisory / Website / Vulnerability Disclosure Policy
- □ Automated Alerts (e.g., SIEM, Monitoring tools)
- □ Other:

What is the information format for detected, registered, and fixed vulnerabilities used in your organization?

Choose one of the following answers

Please choose **only one** of the following:

○ Internal (Proprietary Format)

○ Standard-Compliant (e.g., CVE, ISO, NIST, EUVD) if so, which provide in comments)

○ Other (if so, which provide in comments)

○ None/No

Make a comment on your choice here:

Do You use any vulnerability disclosure / handling supporting tools?

Select all that apply

Please choose **all** that apply:

- □ None
- □ Nmap
- □ Nessus
- □ ZAP
- □ BurpSuite
- □ Other: ______

Incident management

How are you currently handling the incident management processes in your organization?

Choose one of the following answers

Please choose **only one** of the following:

○ We are not doing it

○ We are doing it on an informal basis, with no records kept

○ We are doing it using manual processes and written / informal records

○ We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC 27035, etc., please list standards or practices in comments)

○ We are using a tool / automated process for this (please provide tool name or description in comments)

○ Other (please describe in comments)

Make a comment on your choice here:

Is incident classification implemented in your organization?

Choose one of the following answers
Please choose **only one** of the following:

○ Own (internal) classification

○ Compliant with standard / guideline / regulation (e.g. NIS 2 directive) if so, which provide in comment

○ No

○ Other if so, please provide details in comment

Make a comment on your choice here:

Who is notified of detected incidents?

Select all that apply

Please choose **all** that apply:

□ None

□ Internal Security Team

□ Affected Customers

□ Regulatory Authorities

□ Public Disclosure

□ Other:

What notification channels are used to report and communicate detected and handled incidents?

Select all that apply

Please choose **all** that apply:

□ None

□ E-mail

□ Dashboard / Internal System

□ Public Advisory / Website

□ Automated Alerts (e.g., SIEM, Monitoring tools)

□ Other:

Do you use any incident detection / analysis, reporting supporting tools?

Select all that apply

Please choose **all** that apply:

□ No

□ Wazuh

□ Snort

□ Suricata

□ Other: ______________________

Security management, documentation, workflow

Have you implemented any documentation management or security management processes in your organization?

Choose one of the following answers

Please choose **only one** of the following:

○ We are using a tool / automated process for this (please provide names or details in comment)

○ We are doing it using formal processes, defined according to best practices (e.g. ISO/IEC 27001 or other relevant standards, etc., please provide names or details in comment)

○ We are doing it using manual processes and written / informal records

○ No

○ We are doing it on an informal basis, with no records kept

○ Other (please describe in comments)

Make a comment on your choice here:

Do you use any tools for documents / source code / data repository tools (internal for developers, managers and public for customers)?

Select all that apply

Please choose **all** that apply:

□ GIT

□ SVN

□ One Drive

□ Google Drive

□ Windows shared folders/Samba

□ Sharepoint

□ iCloud

□ Confluence

□ ISO/ISMS

□ Jira

□ None/No

□ Other:

Do you use any building systems / compilations tools

Select all that apply

Please choose **all** that apply:

□ GitLab CI/CD

□ Ansible

□ Jenkins

□ Maven

□ GitHub

□ None/No

□ Other:

User needs and expectations

What kind of convenience or feature would you expect from a tool that supports inventory or SBOM management?

Please write your answer here:

What do you expect from a tool designed to support vulnerability handling?

Please write your answer here:

What do you expect from a tool designed to support incident handling?

Please write your answer here:

What would you like a tool for risk management to help you with?

Please write your answer here:

What are your requirements for a security management support tool?

Please write your answer here:

What do you expect from a tool supporting documentation and workflow?

Please write your answer here:

Participation in workshops and training sessions on the OSCRAT platform

Are you interested in participating in training sessions or workshops conducted on the OSCRAT platform (selected case studies)?

Choose one of the following answers

Please choose **only one** of the following:

○ Yes

○ No

Contact e-mail

Only answer this question if the following conditions are met:

G4Q1 == "Y"

Please write your answer here:

Thank you for your time and valuable input!

Your responses will help guide the development of cyber resilience tools that truly meet the needs of stakeholders like you. Together, we can make a meaningful impact on the security and trustworthiness of digital operations in SMEs.

If you would like to stay informed about the project or receive a summary of the findings, please indicate so in the optional follow-up section or contact us directly.

We appreciate your support.

For more details please visit project website:

Submit your survey.
Thank you for completing this survey.