Cyber Resilience Stakeholder Survey

Help shape the next generation of cyber resilience tools for 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 small and medium-sized enterprises (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 3–7 minutes to complete. All responses are anonymous and will be treated confidentially.

Thank you for your contribution.

Co-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 21 questions in this survey.

Stakeholder's characteristic

1 Which stakeholders’ group do you belong to and what type of products do you offer? *

Select all that apply

Please choose **all** that apply:

□ Hardware product

□ Software product

□ Manufacturer

□ Importer

□ Distributor

□ Open-source software steward - providing support, not a manufacturer - Article 3 (14) of CRA

□ Other: ▭

Select all that apply according to EU Cyber Resilience Act (CRA) regulations.

Inventory / labelling

2 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 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 or other relevant standards, SBOM files, etc., please input details in comment)

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

Make a comment on your choice here:

SBOM - Software Bill of Material

3 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: ____________________

4 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: ____________________

Risk management

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

Comment only when you choose an answer.
Please choose all that apply and provide a comment:

□ 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)

6 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:

○ No

○ Yes (please put names or details in comments)

Make a comment on your choice here:

Vulnerability management

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

Comment only when you choose an answer.
Please choose all that apply and provide a comment:

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

8 Is vulnerability classification implemented (how)? *

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

○ No

○ Own (internal) classification

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

○ Other (please put details in comments)

Make a comment on your choice here:

9 Notification Channels of detected / registered / fixed vulnerabilities? *

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:

10 Information Format of detected / registered / fixed vulnerabilities? *

Comment only when you choose an answer.

Please choose all that apply and provide a comment:

□ 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

11 Do You use any vulnerability disclosure / handling supporting tools? *

Select all that apply

Please choose **all** that apply:

□ Nmap

□ Nessus

□ ZAP

□ BurpSuite

□ None/No

□ Other: □

Incident management

12 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)

Make a comment on your choice here:

13 Is incident classification implemented (how)? *

Choose one of the following answers

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

○ No

○ Own (internal) classification

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

○ Other if so, please provide details in comment

Make a comment on your choice here:

14 Who is notified of detected incidents carried out? *

Select all that apply
Please choose **all** that apply:

□ None
□ Internal Security Team
□ Affected Customers
□ Regulatory Authorities
□ Public Disclosure
□ Other: □

15 Notification Channels of detected incidents carried out? *

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: □

16 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

17 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:

○ No

○ 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 27001 or other relevant standards, etc., please provide names or details in comment)

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

Make a comment on your choice here:

18 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
□ None/No
□ Other: □

19 Do you use any building sytems / compilations tools *

Select all that apply

Please choose **all** that apply:

□ GitLab CI/CD
□ Ansible
□ Jenkins
□ Maven
□ None/No
□ Other: □

Needs and expectations

Which elements of the planned OSCRAT framework interest you the most?

20 How important to you is:

Please choose the appropriate response for each item:

	Unimportant	Important	Very important
CL - Checklist Automation (CRA self-assessment checklist)	○	○	○
SBOM - Software Bill of material – preparing/analysis supporting tool	○	○	○
VUL – vulnerability management supporting tool	○	○	○
INC – incident management supporting tool	○	○	○
DOC – documentation tool (central repository)	○	○	○

21 Are you interested in participating in the validation of the tool developed within the project? *

Choose one of the following answers

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

○ Yes

○ No

○ I am not sure

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: https://oscrat.eu

Submit your survey and send it to
the following email address:

info@unicis.tech

Thank you for completing this survey.