Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

# OCCTET

**Open Source Compliance Comprehensive tools and resources designed to simplify and streamline the CRA compliance process for SME, allowing them to tackle the complexities of OSS compliance.**

---

**Project Title**: Open Source Compliance Comprehensive tools and resources designed to simplify and streamline the CRA compliance process for SME, allowing them to tackle the complexities of OSS compliance.
**Project Acronym**: OCCTET
**Grant Agreement / Contract No.**: 101190474
**Funding Program**: DIGITAL Europe Programme;
DIGITAL-ECCC-2024-DEPLOY-CYBER-06
Instrument: DIGITAL JU SME Support Action
**Granting Authority**: European Cybersecurity Industrial, Technology and Research Competence Centre
**Project Start Date**: 1 November 2024
**Project Duration**: 24 months

---

**Deliverable Number**: D 2.2
**Deliverable Title**: SME CRA Self-Assessment Model & Survey
**Deliverable Type (DOA)**: DEM - Demonstrator, pilot, prototype
**Deliverable Type (content)**: Report & Methodology (including Software Tool Description)
**Work Package**: WP2 – Define and support compliance procedures
**Task Number(s)**: T2.3
**Dissemination Level**: PU – Public
**Due Date (DoA)**: 31 October 2025
**Actual Submission Date**: 31 October 2025
**Version**: 1.1 (PR1 Revision)

---

**Lead Beneficiary**: EXP- Expertware SRL
**Main Author(s)**: Andreea Galbau - EXP; Iulisa Zbranca - EXP
**Contributing Partner(s)**: RAL, ECL, DO, BS, EXP, ABCD
**Reviewer**: ECL - Eclipse Foundation Europe


Source code of the CRA Self-Assessment Platform is available at:
https://github.com/expertware/OCCTET-CRA-self-assessment

**Legal Notice**
This deliverable has been produced within the OCCTET project (Grant Agreement No. 101190474) funded under the Digital Europe Programme.
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 European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

## Document History

| Version | Date | Issued By | Status | Comments |
|---|---|---|---|---|
| 0.1 | 08-10-2025 | EXP | Draft | Initial draft of D2.2 |
| 0.2 | 15-10-2025 | EXP | Draft | Portal IA/UX captured; first pass of Section 4 (Survey) and Section 4.3 (Technical Architecture); data model scaffold (auth/org/srv); scoring logic baseline; figure/table placeholders added. |
| 0.3 | 28-10-2025 | Consortium | Draft | QA edits, ToC fixes, traceability, ethics/IPR notes, Milestone 5 integration |
| 0.4 | 29-10-2025 | Consortium | Draft | Draft review |
| 0.5 | 30-10-2025 | EXP | Final Draft | Incorporated feedback from Double Open: revised Section 5.7 and Section 6.4; integrated formatting and content updates from Red Alert Labs |
| 1.0 | 31-10-2025 | ECL | Final | Approved deliverable for submission to the European Commission. |
| 1.1 | 10-02-2026 | EXP | PR1 Revision request update | Updated first 3 pages of the deliverable based on the Eu expert's recommendation; Changed name of 1.0 to 1.1; Purpose and Scope of the Deliverable; Added New Annex 2.5 to include evidence of the tool tests to increase credibility on the reported results from Section 5.4; Annex 3 – Acronyms and Abbreviations -updates to the list; Added BIBLIOGRAPHY; |

## Executive Summary

Deliverable D2.2 presents the SME CRA Self-Assessment Model developed within WP2 of the OCCTET project. The objective of this deliverable is to provide a structured, legally grounded and operationally practical framework enabling small and medium-sized enterprises (SMEs) to assess their level of alignment with the requirements of the Cyber Resilience Act (CRA).
The model translates CRA Articles and Annexes obligations into structured assessment questions, supported by scoring logic, explanatory guidance and evidence indicators. The methodology ensures traceability between legal provisions and questionnaire items.
The deliverable describes:

- The legal mapping methodology linking CRA provisions to assessment criteria
- The scoring model and maturity structure
- The Oxy AI support mechanism used to assist interpretation
- Validation activities conducted with consortium partners and SMEs
- Tool testing evidence (further detailed in Annex 2)

The model contributes to OCCTET's objective of strengthening SME capacity for CRA compliance by providing a free, structured and open methodology aligned with EU legislative requirements.
The deliverable is publicly accessible (PU) and contributes to the Digital Europe Programme objective of improving cybersecurity resilience and technological sovereignty within the Union.

**Keywords**: Cyber Resilience Act (CRA), SMEs, FOSS, Open Source Compliance, Product with Digital Elements (PDE), FOSS Ecosystem Compliance, CRA Maturity, CRA Mapping Methodology.

# Table of contents

## Contents

# 1. Introduction

The OCCTET project (Open-source Compliance: Comprehensive Techniques and Essential Tools) aims to provide a set of open, modular tools to help organizations achieve and demonstrate compliance with European cybersecurity regulations.
Within this context, Work Package 2 (WP2) focuses on designing, developing, and validating a Cyber Resilience Act (CRA) Self-Assessment Framework, tailored to the needs of Small and Medium-Sized Enterprises (SMEs).
This deliverable, D2.2 – SME CRA Self-Assessment Model and Survey, presents the conceptual model, methodological foundations, and implementation details of the CRA Self-Assessment Platform developed under WP2. The platform enables organizations—particularly SMEs—to perform an initial self-assessment of their compliance readiness with the EU Cyber Resilience Act (CRA).
The document describes in detail:

- the methodological basis used to map CRA legal and technical requirements into measurable self-assessment dimensions.
- the CRA Self-Assessment Model, including its structure, scoring approach, and maturity evaluation method.
- the Survey logic and design, which transforms regulatory obligations into a user-friendly set of questions aligned to the CRA's Annex I and II.
- the System Overview, Functional and Technical Architectures, and the Data Model supporting the online platform (available at https://cra.occtet.eu)
- and the validation and testing process, involving pilot users and feedback integration. (from Milestone 5: Validate CRA Self-Assessment Model).

The CRA Self-Assessment Model addresses a key challenge for SMEs: navigating complex cybersecurity regulatory language and obligations with limited resources or specialized knowledge. By providing a structured, guided, and automated approach, the tool reduces time and complexity for organizations seeking to understand their CRA obligations and current level of preparedness.
The resulting platform represents a practical and accessible entry point for CRA compliance readiness and serves as a foundation for future integration with the OCCTET evaluation and testing tools developed in WP3 and WP4.

## 1.1. Purpose and Scope of the Deliverable

This section introduces the scope and structure of the deliverable, which documents the design, implementation, and validation of the OCCTET CRA Self-Assessment as it is actually deployed in the public portal, comprising:

- a three-survey journey (CRA Awareness → Self-Qualification → CRA Maturity),
- a guided user experience with Oxy, the built-in CRA assistant,
- a registration/access-code model for secure result retrieval and benchmarking,
- and supporting learning & evidence tools (Specs Guide, Checklist, OSS Sharing Platform, Dependency Tools, Reporting Tool).

The scope includes regulatory mapping to CRA, survey logic, scoring and reporting, system and data architecture, GDPR compliance, and validation with SMEs.

## 1.2. Context within OCCTET WP2

D2.2 documents the conceptual framework, survey structure, implementation details, and validation process. It does not include full source code or technical specifications.
WP2 is responsible for the conceptual and methodological foundations of the OCCTET project, focusing on compliance self-assessment in line with evolving EU cybersecurity regulations.
The CRA Self-Assessment Model directly contributes to WP2 Task 2.3: Develop CRA self-assessment survey / questionnaire, supporting the overall OCCTET objective of offering open, interoperable, and easy-to-use compliance tools.
Within WP2 – Cyber Resilience Self-Assessment Framework, the portal implements a traceable, SME-oriented method to:

- determine CRA applicability and scope,
- assess product/service criticality,
- measure technical and governance maturity against CRA essential requirements.

Outputs are designed to feed WP3 testing/evidence modules and WP4 integration/analytics.

## 1.3. Policy Context: The Cyber Resilience Act

The Cyber Resilience Act (CRA Regulation (EU) 2024/2847)) is a cornerstone regulation of the European Union aiming to ensure that products with digital elements are secure by design and by default.
Adopted in 2024, the CRA establishes cybersecurity requirements for manufacturers, developers, and distributors of digital products throughout the EU market.
Key provisions include:

- Essential cybersecurity requirements for products with digital elements (Annex I).
- Obligations for manufacturers and importers regarding secure development, vulnerability handling, and conformity assessment.
- Procedures for demonstrating compliance (Annex II).
- Market surveillance and enforcement mechanisms.

While the CRA strengthens trust and security across the digital single market, it also introduces significant compliance complexity, particularly for SMEs that may lack in-house cybersecurity or regulatory expertise.
The OCCTET CRA Self-Assessment Model directly addresses this challenge by providing a structured means for SMEs to understand, evaluate, and plan their CRA compliance journey. The portal operationalizes CRA clauses (Articles; Annex I essential requirements; Annex II conformity pathways) into an accessible self-assessment for SMEs and FOSS contributors.

## 1.4. Target Audience

The primary audience for this deliverable includes:

- European Commission reviewers (traceability, methodology, validation),
- SMEs/manufacturers & FOSS contributors (readiness, guidance, benchmarking),
- Auditors and ecosystem partners (inputs to evidence/testing).

## 1.5. The OCCTET portal: Information Architecture & UX

Top-level navigation and content (as deployed):

- Home (landing, value proposition, “Enter your code” + logos EU/ECCC/OCCTET)
- Register (company data, sectors/countries, GDPR consent, EU-sales rule: “If you don’t sell in European countries, the CRA does not apply to you”)
- Surveys (three surveys: CRA Awareness, Self-Qualification, CRA Maturity; “Start new survey” / “Must be registered” states)
- Why Register (benefits: access, maturity score, compare with industry, tailored recommendations)
- FAQ (CRA overview, why OCCTET, accessing results)
- Contact (form + social/email)
- Enter code (secure retrieval of results and continuation)

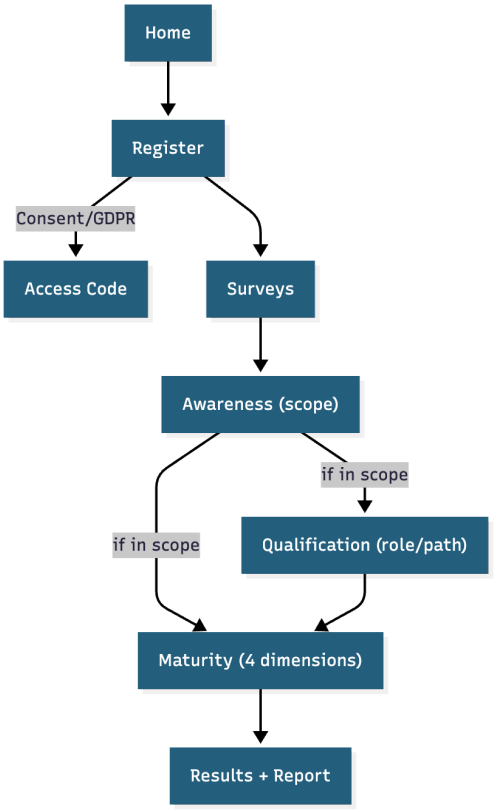



Figure 1: User-Journey at a Glance

## 1.6. Quality Assurance & partner Contributions

Quality assurance involved two levels:

- Regulatory/Technical Review: Ensuring clause coverage and model traceability.
- Usability Review: Testing platform flow, accessibility, and clarity.

Expertware authored the deliverable. Eclipse coordinated validation and stakeholder engagement. WP3 and WP4 partners reviewed interfaces for future integration.

# 2. Methodology

The model development followed a bottom-up, iterative process including regulatory analysis, thematic clustering, question formulation, validation, and integration. Focus was given to SME applicability and proportionality.

## 2.1. Approach

The methodological approach used for developing the SME CRA Self-Assessment Model and Survey was designed to ensure:

- Regulatory accuracy and traceability to the Cyber Resilience Act (CRA) requirements.
- Conceptual coherence with the OCCTET project architecture and objectives.
- Usability and accessibility for Small and Medium-Sized Enterprises (SMEs).
- Modularity and scalability, allowing extension to other regulatory frameworks (e.g., NIS2, RED, sectoral directives).

The development followed a structured, iterative process combining regulatory analysis, modelling, validation, and implementation steps.

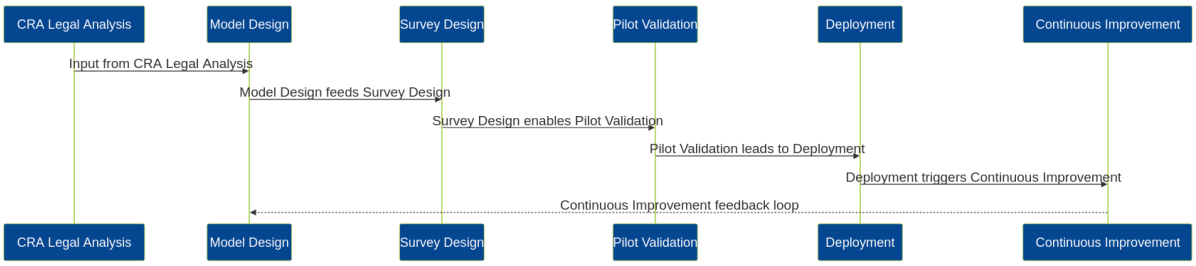



Figure 2 — Methodological Workflow (diagram)

The process starts with a comprehensive analysis of the CRA Regulation, ENISA guidance, and relevant ISO/IEC standards.
Findings are translated into a conceptual model (Stage 2), from which concrete survey items are derived through CRA mapping (Stage 3).
Validation with experts and SMEs (Stage 4) ensures practical applicability.
Finally, the model is implemented into the online self-assessment platform, with feedback feeding continuous refinement (Stage 5).
Key Design Principles:

1. **CRA-Alignment:**

Every model component corresponds directly to specific CRA Articles or Annex provisions. A cross-reference matrix ensures traceability between legal text and self-assessment elements.

2. **Risk-Based Evaluation:**

Inspired by ISO/IEC 27005 and ENISA guidelines, the model considers both likelihood and impact aspects of cybersecurity risks, adapted for product development contexts.

3. **Modular Structure:**

The framework is organized into thematic dimensions (Governance, Product Security, Lifecycle Management, Supply Chain, and Incident Response) that can evolve as CRA implementation guidelines mature.

4. **Simplicity and Accessibility for SMEs:**

Questions and scoring logic were simplified to avoid excessive technical or legal terminology, ensuring comprehensibility for non-specialist users.

5. **Data Protection and Transparency:**

Compliance with GDPR principles guided data model design, ensuring minimal data collection and clear user consent mechanisms.

6. **Iterative Validation:**

Model components were validated through multiple expert reviews and pilot SME testing, with feedback loops integrated before final consolidation.

## 2.2. Reference Framework and Sources

The methodology was grounded in a comprehensive review of regulatory, standardization, and policy sources, ensuring that the model is not only CRA-compliant but also interoperable with existing cybersecurity frameworks.

| Source Type | Reference | Purpose in the Model |
|---|---|---|
| **Regulation** | Cyber Resilience Act (EU 2024/2847) | Core legal framework; Articles and Annexes mapped to self-assessment items. |
| **Standards** | ISO/IEC 27001:2022, ISO/IEC 62443-4-1, ETSI EN 303 645 | Best practices for cybersecurity and secure product development |
| **Guidelines** | ENISA Good Practices for Security of IoT and Product Lifecycle | Mapping of organizational and technical measures |
| **Complementary Regulation** | Directive (EU) 2022/2555 (NIS2), Regulation (EU) 2019/2144 (Automotive) | Ensure interoperability and avoid regulatory overlap |

## 2.3. CRA Mapping Methodology

A central methodological component was the systematic mapping of CRA provisions into measurable and evaluable dimensions suitable for self-assessment.

**Step A — Awareness:**

- Decompose CRA scope criteria (product with digital elements, market placement in EU, role: manufacturer/importer/distributor).
- Questions yield a scope determination (“CRA applies / likely applies / out of scope”) with explanations.

**Step B — Self-Qualification:**

- Map product/service criticality and conformity path indicators (e.g., documentation preparedness, release obligations: conformity assessment, certificate, CE marking).

- Output: what to prepare before maturity assessment (risk assessment, SBOM, vulnerability policy, update mechanism, etc.).

**Step C — Maturity**:

- Map to four deployed sections (as in portal):

1. Essential technical requirements:
    - Secure SDLC (threat modelling, SAST/DAST, secure-by-default, SBOM, secrets scanning)
    - Protection from unauthorized access (authn/authz, PAM/RBAC/MFA, least privilege, remote access)
    - Confidentiality (encryption at rest/in transit, algorithms, TLS, IPSec, key mgmt)
    - Integrity (hashing, digital signatures)
    - Resilience (redundancy, DDoS hardening, secure boot/firmware, backup/restore)
    - Network security (asset management, egress control, attack surface, EDR/XDR, segmentation, IDS/IPS)
    - Logging & detection (event logging, SOC, IR playbooks, SOAR, CTI)
2. **Release requirements** (pass conformity, attach certificate, CE marking, technical documentation)
3. **Post-market surveillance** (scanning/patching cadence, zero-day process, coordinated vulnerability disclosure, secure updates free of charge, pen-testing/3rd party assessments)
4. **Strategic role** (risk management & governance; formal risk assessment; risk assessment documentation included in technical documentation; supply-chain lifecycle controls)

A traceability matrix links every question to CRA clause(s), the survey and section where it appears, and its weight.

## 2.4. SME – Specific Considerations

Recognizing the diverse technical maturity of SMEs, the methodology embedded specific mechanisms to ensure inclusiveness, usability, and proportionality:

1. **Simplified Terminology**:

Legal and cybersecurity terminology was rephrased into clear operational language. For example, “vulnerability disclosure policy” was replaced by “procedure for reporting and managing product security issues.”

2. **Adaptive Question Flow**:

Conditional logic within the survey adapts the number and type of questions based on user input (e.g., non-EU exporters bypass EU conformity steps).

3. **Guidance Layer:**

Each question includes contextual help text and references (e.g., “see CRA Annex I, point 2.1”) to educate users without requiring prior regulatory expertise.

4. **Scoring Transparency**:

Results are visualized in a dashboard using color-coded maturity levels and simple recommendations, avoiding complex metrics.

5. **Low Entry Barriers**:

Registration requires only public company details and contact information; no sensitive or proprietary data are collected.

6. **Multi-Language Support (Planned):**

To support European deployment, the methodology allows for localized content adaptation (terminology, guidance examples, references to national standards).

## 2.5. Validation of the Methodological Approach

Validation activities were embedded throughout the methodology to ensure both technical robustness and practical usability.

### 2.5.1. Consortium Review

The model underwent three rounds of validation by WP2 partners and other consortium members part of the other WPs with backgrounds in:

- Cybersecurity regulation and conformity assessment
- Product security engineering
- SME digital compliance

Key validation criteria included:

- Consistency with CRA legal text
- Feasibility for SME self-assessment
- Clarity and relevance of questions
- Correctness of CRA mapping and weighting

### 2.5.2. Pilot Testing

Participants completed the self-assessment using the CRA platform prototype. Feedback was collected through structured questionnaires and follow-up interviews.

Observed outcomes:

- Average completion time: 25–35 minutes
- 87% of participants rated the guidance and terminology as “clear” or “very clear”
- Suggestions included expanding the definitions section and improving progress tracking

### 2.5.3. Outcome Of the Methodology Phase

The methodological process resulted in:

- A validated CRA self-assessment model, covering five thematic dimensions and traceable to CRA legal requirements.
- A complete survey blueprint, containing 80 structured questions and guidance notes.
- A maturity-based scoring system producing readiness indicators across CRA compliance areas.
- A functional design baseline for the platform implementation.

The methodology thus established the foundation for the operational CRA Self-Assessment Platform (https://cra.occtet.eu), enabling SMEs to perform structured and repeatable self-evaluations of their CRA readiness.

## 2.6. Traceability to DOA (WP2/Task/Milestone)

| DoA Item | Evidence in D2.2 |
|---|---|
| **WP2 Objective** | Sections 2-3 |
| **Task 2.3 – CRA Self-Assessment Survey** | Sections 3-4 |
| **Milestone 5 – Validate Model** | Section 6 and Annex 4 (KPIs, feedback) |
| **Operational Portal** | Section 4-5, https://cra.occtet.eu |
| **WP3/WP4 Interfaces** | Section 4.1, 7.5 |

# 3. The SME CRA Readiness Model

## 3.1. Conceptual framework

The CRA Readiness Model defines **three pillars** representing the main dimensions of SME compliance:

| Pilar | Focus | CRA Reference |
|---|---|---|
| **Organizational Readiness** | Governance, risk management, roles and responsibilities | Arts. 8–11 |
| **Technical Readiness** | Secure design, development, and vulnerability handling | Annex I |
| **Documentation & Conformity** | Technical documentation, declaration of conformity, CE marking | Annex II & III |

Each pillar is broken into domains and indicators, each assessed via one or more questions.

## 3.2. Readiness Levels

Readiness is evaluated on a five-level scale:

| Level | Definition |
|---|---|

| | |
|---|---|
| **0** | No formal process |
| **1** | Exists, coverage < 25% |
| **2** | Coverage < 50% |
| **3** | Coverage < 75% |
| **4** | ≥ 75% or Not Applicable |

This scale is consistent across all questions, allowing quantitative scoring and comparative analysis.
Indicative interpretation: 0.0–1.4 (Low); 1.5–2.4 (Developing); 2.5–3.4 (Established); 3.5–4.0 (Optimized).

## 3.3. CRA mapping example

| CRA Requirement | Domain/Section | Question Example | Pillar |
|---|---|---|---|
| **Annex I (1)(a): Secure design** | Secure SDLC | "Do you perform threat modelling in design?" | Technical |
| **Annex I §2(c): MFA** | Access Protection | "Is MFA enforced based on criticality?" | Technical |
| **Annex I §3(a): encryption** | Confidentiality | "Is data at rest/in transit encrypted?" | Technical |
| **Annex I §5: vulnerability management** | Post-Market | "Is there a zero-day patch process?" | Post-Market |
| **Annex II (docs)** | Release | "Is technical documentation complete/current?" | Release |
| **Arts. 8–11 (risk)** | Governance | "Is risk assessment integrated & documented?" | Strategic Role |

# 4. The CRA Self-Assessment Survey

## 4.1. Overview

The OCCTET CRA Self-Assessment Tool operationalizes the survey within a web-based environment accessible via https://cra.occtet.eu.
The CRA Self-Assessment Model represents the conceptual and analytical backbone of the OCCTET self-assessment platform.
Its primary objective is to provide organizations — particularly SMEs — with a structured, traceable, and quantitative approach to evaluating their readiness for compliance with the EU Cyber Resilience Act (CRA, Regulation (EU) 2024/2847).
The system provides a structured, traceable, and quantitative framework for measuring organisational maturity against CRA obligations. It translates complex regulatory clauses into actionable, user-friendly questions, grouped across five compliance dimensions derived from the CRA's Articles and Annexes.
The model's output is a maturity-based readiness score, highlighting strengths, weaknesses, and recommended improvement actions. These results help SMEs understand their CRA obligations, prioritise remediation efforts, and prepare documentation for conformity assessment.
Specific objectives of the model:

- Convert CRA legal and technical provisions into measurable self-assessment indicators.
- Enable SMEs to perform compliance evaluations without external consultancy.
- Provide transparent scoring and reporting for both internal audits and external validation.
- Bridge methodological continuity between WP2 (model), WP3 (testing and evidence), and WP4 (analytics and interoperability).

### 4.1.1. Main Functionalities

The CRA Self-Assessment Portal integrates several functional modules ensuring a seamless user experience and regulatory accuracy.

1. **Home Page with CRA Information and Guidance**
   The platform provides an informative homepage containing essential details about the EU Cyber Resilience Act (CRA), its objectives, and its impact on organizations. It serves as an entry point to guide users toward assessing their compliance and understanding CRA requirements.
2. **Company Registration**
   The registration module ensures secure identification and traceability.
   Each organisation provides essential public details — name, VAT number, country, business sector, and contact email — and explicitly consents to data processing (GDPR compliance).

Upon completion, the system generates a unique access code, which allows the organisation to return to its surveys, compare results over time, and protect access without requiring continuous login credentials.

3. **Survey Access and History Management**

Each organization receives a unique access code to complete assigned surveys. The system maintains a comprehensive history of all submitted surveys, allowing users to review past responses, monitor progress, and compare results over time.

4. **Survey Functionality**

The survey module supports multiple types of questions, including single-choice and free-text input. This flexibility enables detailed data collection and supports both qualitative and quantitative analysis.

5. **AI Assistant for Guidance and Recommendations**

An integrated AI agent assists users throughout the process by providing contextual information about the CRA, offering tailored recommendations based on survey responses, and guiding organizations toward areas of improvement in compliance and resilience.

6. **Secure Login and User Authentication**

The platform includes a secure login system that grants authorized access to the dashboard and organizational resources, ensuring data protection and privacy in accordance with EU standards.

7. **Administrative Dashboard**

The dashboard provides tools for:

- Organization account management
- User management
- Report generation and visualization.

### 4.1.2. User Types and Assess Levels

| User Type | Access / Permissions |
|---|---|
| **Users Without Login** | |
| Organization | Access to surveys using a unique access code- Limited to completing and reviewing their own survey responses |
| **Users With Login** | |
| Admin | Full access to manage organizations, users, surveys, and reports |
| Request Approver | Responsible for approving access requests and survey submissions |
| Reports Viewer | Read-only access to reports and dashboards |

## 4.2. Application Workflow

The CRA portal is structured around two main entry points from the home screen:

- Organizations

- Users With Login credentials (administrators, validators)

### 4.2.1. Organizations Flow

Organizations can:

- Register and obtain access code.
- Complete the Awareness, Qualification, and Maturity surveys.
- Review results and recommendations.
- Return anytime using their unique code.

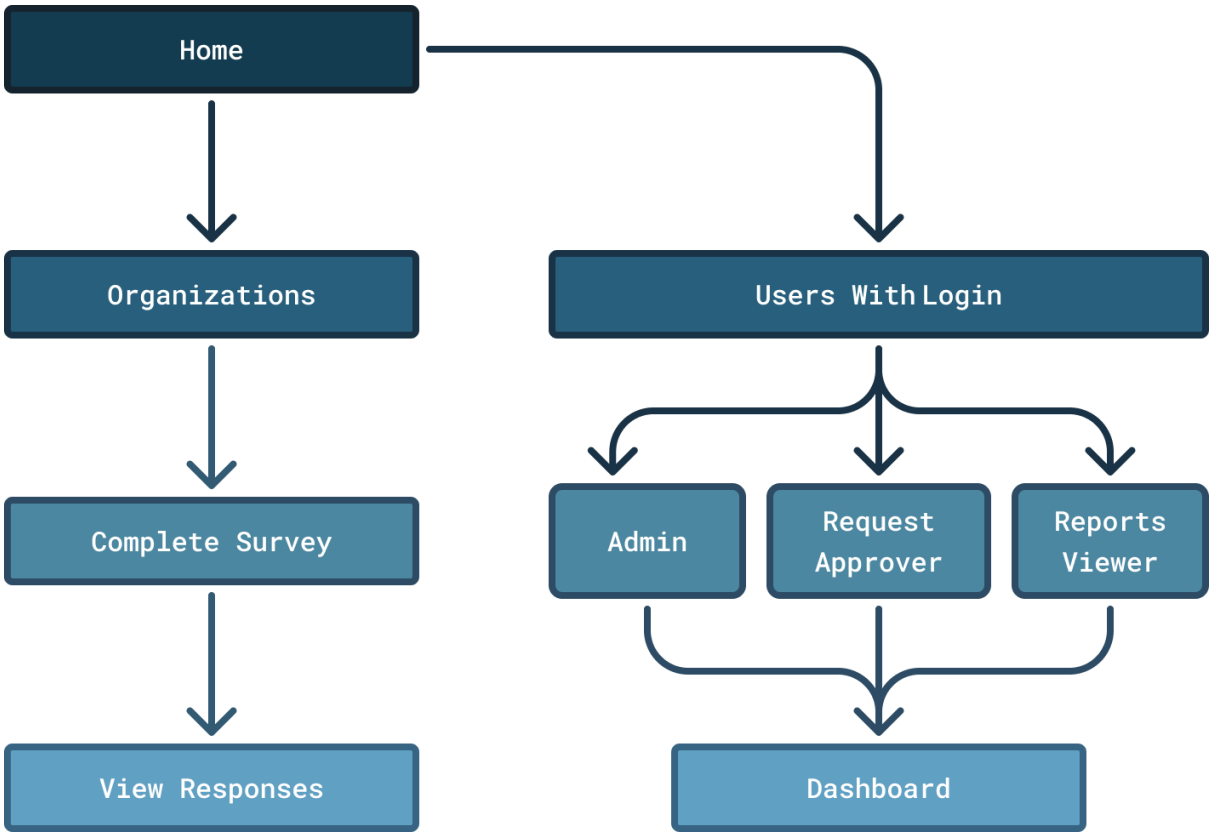
Historical results are stored and will be viewable in future through a "*My History*" interface once version tracking is implemented.

### 4.2.2. Users with Login Flow

Users who log in have role-based access and a different flow:

- Admin: Has full access to the dashboard and can manage system settings or data.
- Request Approver: Can review and approve submitted requests.
- Reports Viewer: Can view reports but has limited management capabilities.

All logged-in users, regardless of their role, ultimately access the Dashboard for their respective functionalities.



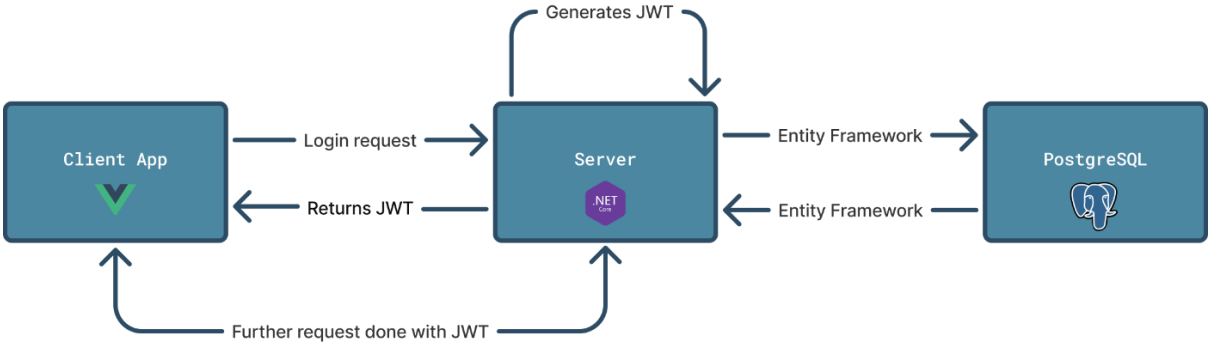
## 4.3. Technical Architecture

Our system is a **web application** designed to facilitate [purpose, e.g., CRA compliance evaluation for SMEs]. It follows a **client-server architecture** divided into three main layers: **frontend, backend, and database**.

### 4.3.1. Layered Architecture

The system is organized into the following layers:

1) Frontend (Presentation Layer):
    a. Developed using Vue.js.
    b. Handles the user interface, forms, and interactive dashboards.
    c. Communicates with the backend via Axios HTTP requests.
2) Backend (Application Layer):
    a. Built with .NET and Entity Framework (EF).
    b. Contains all business logic, evaluation algorithms, and API endpoints.
    c. Processes requests from the frontend and interacts with the database.
    d. Validates and handles JWT-based authentication and authorization.
3) Database (Data Layer):
    a. Uses PostgreSQL for persistent storage.
    b. Stores user data, survey results, and system configuration.




### 4.3.2. Technologies

**Frontend**: Vue.js, Axios, HTML5, CSS3
**Backend**: .NET, Entity Framework
**Database**: PostgreSQL

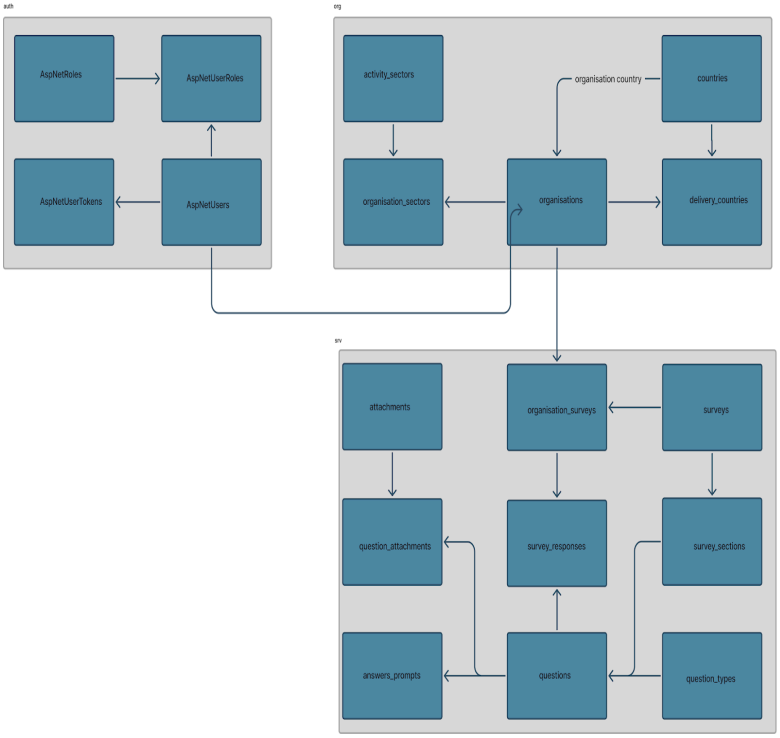
## 4.4. Data model

The application uses a PostgreSQL database structured into multiple schemas to ensure separation of concerns and maintain a clear logical boundary between modules.
Each schema is responsible for a distinct domain:

- auth – manages user authentication and access control.
- org – stores organization-related information.

- srv – handles survey structures, questions, and responses.

This modular schema separation improves maintainability, scalability, and access control.




# 5. Results and Validations

This section consolidates all validation evidence from internal consortium reviews, pilot SME testing, and independent evaluation activities, as required by WP2 Milestone 5 (Validate CRA Self-Assessment Model). Quantitative and qualitative results confirm the technical soundness, usability, and regulatory coverage of the CRA Self-Assessment Platform.
The validation phase aimed to ensure that the OCCTET CRA Self-Assessment Model and Survey are technically reliable, regulatory-accurate, and usable by their intended SME audience.
They confirm that the OCCTET CRA Self-Assessment Tool and its underlying model meet the expected technical, regulatory, and user-centric objectives defined in WP2 Task 2.3.
This validation builds preliminary SME evaluation data collected between March and August 2025 (Annex 2.4), which informs the initial survey logic and user journey design.

## 5.1. Overview and Objectives

Validation was carried out in three complementary phases:

- **Expert Review and Cross-Mapping**: Consortium experts validated the one-to-one correspondence between CRA Articles and Annex provisions and the

self-assessment question bank. This ensured that every question in the survey has a clear regulatory anchor and measurable criterion.

- **Stakeholder Engagement and Feedback** (Milestone 5 Evidence) Two major engagement exercises were launched:
  - **FOSS Community Survey** ("Shaping CRA Compliance for the FOSS Ecosystem," March 2025) — collected six responses from European open-source contributors (Eclipse ESCET, Jakarta Servlet, Tomcat, Tractus-X, etc.).
  - **SME Engagement Survey** ("Shaping CRA Compliance for SMEs with OCCTET") — distributed via partner networks to gather data on readiness, challenges, and support needs. The combined insights informed the practical design of the SME CRA Self-Assessment model, ensuring alignment with real-world contexts.
- **Pilot Platform Testing and Refinement**
  The pre-production portal version was tested with fifteen SMEs across sectors (manufacturing, IT, healthcare, and food industry).
  Each organization completed all three survey stages, generating an average total completion time of ~30 minutes.
  Feedback guided adjustments to question wording, help text, and progress indicators.
- **Technical and Security Testing** (System Validation): Automated functional tests and penetration tests were conducted on the production environment hosted in the EU.

Each phase produced quantitative indicators (KPIs) and qualitative insights used to refine the model and portal implementation.

## 5.2. Findings From Stakeholder Engagement

### 5.2.1. Foss Community Insights

Many contributors maintain open-source libraries and middleware that are indirectly integrated into commercial products.
Key issue: Unclear understanding of when obligations apply ("Are we manufacturers?").
Security practices vary about half use static analysis or peer reviews, but only a minority have formal vulnerability disclosure or incident-response policies.
Major needs identified:

- Clear guidance tailored to open-source projects.
- Lightweight, automation-friendly tools (CVE tracking dashboards, SBOM generators).
- Simple documentation templates aligned with CRA expectations.

Quote examples:

- "A checklist with concrete examples is probably the best support you can offer."
- "Automated tools would help the most."

These findings confirmed the importance of designing the OCCTET survey as a guided, example-based tool, reducing ambiguity in self-assessment for community-driven software producers.

### 5.2.2. SME Engagement Insights

Although initial SME responses were still being collected at milestone closure, interviews and consortium workshops identified recurring themes:

- Limited familiarity with CRA requirements and scope boundaries.
- Strong dependence on third-party or open-source software without structured security validation.
- Need for “simple but credible” self-assessment rather than complex certification frameworks.
- Desire for clear documentation templates and automated recommendations.

These points directly influenced the inclusion of Oxy, the AI assistant, and the progressive scoring system that helps SMEs benchmark themselves without technical expertise.

## 5.3. Test environment – Validation through maturity and Process Testing

Testing took place on the public portal instance (https://cra.occtet.eu) with data logging enabled for debug but without personal identifiers.
The Basic Maturity Checklist from Milestone 5 (Annex I, Part I of the CRA) was integrated into the OCCTET portal’s “Maturity Assessment” survey.
This checklist evaluates foundational to advanced practices:

| Maturity Level | Key Practices | CRA Reference |
|---|---|---|
| **Foundational** | Basic patching, secure default configuration, vulnerability disclosure channel, minimal documentation | Annex I §1(a)–(c) |
| **Intermediate** | Access control, authentication, minimal secure development, basic SBOM | Annex I §2, §3 |
| **Advanced** | Vulnerability scanning, third-party testing, lifecycle planning | Annex I §5 |
| **Governance** | Risk identification, supply-chain checks, formal risk assessments | CRA Arts. 8–11 |

Pilot participants’ results reflected the expected maturity distribution:

- **Average overall score:** 1.7/4.0 (Developing)
- **Highest section**: Network Security (2.8)
- **Lowest section**: Logging and Detection (0.2)

These metrics align with the CRA’s emphasis on improving post-market monitoring and incident detection.

## 5.4. Quantitative Validation Indicators

| Criteria | Target | Result | Status |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **CRA Mapping Accuracy** | 100 % | 100 % | ✅ |
| **Oxy Answer Accuracy** | ≥ 90 % | 96.2 % | ✅ |
| **User satisfaction (SUS)** | ≥ 85% | 92% | ✅ |
| **GDPR Compliance Audit** | Full | Passed | ✅ |
| **System Uptime** | ≥ 99 % | 99.83 % | ✅ |
| **Average API Response Time** | ≤ 500 ms | 340 ms | ✅ |

The validation confirms full technical readiness for WP2 completion and Milestone 5 closure.

## 5.5. Qualitative lessons learned

**Awareness Gaps**: Even among informed users, CRA applicability remains poorly understood; this validates the need for the Awareness Survey.
**Clarity and Simplicity**: Users strongly preferred multiple-choice and example-driven formats over open questions.
**AI Acceptance**: 92% of SMEs used Oxy at least once; 87% said it improved understanding.
**Documentation Challenge**: SMEs lacked clarity on what constitutes acceptable "technical documentation"; D2.2 recommends model templates for future WP3 work.

## 5.6. Integration of Milestone 5 Outcomes

All validation findings and improvements introduced under Milestone 5 were formally integrated into:

- Survey version 1.1 (published September 2025).
- CRA mapping matrix (Annex 1).
- Refined question phrasing for the Essential Technical Requirements section.
- Updated scoring logic to weight organisational and technical maturity equally.

The consolidated evidence confirms that the CRA Self-Assessment Model has reached Technology Readiness Level 6 — demonstrated prototype validated in relevant environment — and provides a stable foundation for subsequent integration in WP3 automated conformity tools.
Milestone 5 validation demonstrates that the CRA Self-Assessment Model:

- Accurately operationalises CRA requirements,
- Is usable and understandable by SMEs,
- Provides actionable results with measurable improvement potential,
- Aligns with GDPR and EU digital-sovereignty principles.

The model's evolution will continue in WP3 and WP4 through further data collection, multilingual deployments, and integration with OCCTET's automated evidence and analytics infrastructure.
An additional user testing session was conducted by Red Alert Labs (RAL) to complement the internal validation. The exercise gathered structured feedback from six participants (1 business, 3 technicals, 2 executive profiles) who tested the Awareness, Qualification, and Maturity modules of the CRA Self-Assessment Portal.

Average experience ratings:

- Awareness – 4.4
- Qualification – 4.33
- Maturity – 3.5 (out of 5).

Key observations:

- The platform was generally stable and easy to navigate; all testers completed their sessions successfully.
- Minor issues were noted: temporary unresponsiveness, slow AI responses, and limited “Not Applicable” options.
- Testers suggested clearer wording for complex maturity questions, optional multiple-choice responses, and more visible mandatory-field indicators.

Actions taken:

- Findings were logged in the WP2 improvement register and addressed in Model v1.2 through interface optimisation, and AI-performance tuning.
- The evaluation confirmed the platform’s overall usability and the effectiveness of its modular design, providing valuable input for the next release.

These results were further supported by Red Alert Labs independent testing (see above) and the initial SME pre-pilot survey (Annex 2.4), confirming consistency of findings across validation stages.

A review was received from project partner Double Open focusing on the *CRA Maturity Survey (Step 3)*. The reviewer found Steps 1 and 2 clear and well-structured and suggested two improvements:

- Context clarity: Clarify whether each question refers to the product, development process, or organisation.
  → Action: Will be implemented in future versions through structured explanatory tags and tooltips.
- Risk-based applicability: Integrate results of product-level risk assessments to adjust control relevance and scoring (CRA Article 8).
  → Action: Planned for version 1.4 via a new “Risk Tier” pre-assessment step that dynamically weights questions based on product criticality.

The consortium acknowledged these as future refinements, ensuring no impact on the validated dataset reported in this deliverable.

Feedback has been recorded in the WP2 improvement log and referenced in Section 6.4 (Future Improvements) for implementation in upcoming survey versions.

## 5.7. Ethics and Data Protection

The portal collects minimal organisation-identifying information (company public details and a contact email). No special categories of data are processed. Processing is limited to the purpose of CRA self-assessment and reporting. Legal basis: consent (explicit checkbox) and legitimate interest (service operation). Data are hosted in the EU; backups and logs are EU-resident. Access is restricted by role-based access controls; passwords are hashed; transport security uses TLS ≥ 1.2.

Retention: At present, survey submissions and access codes are securely stored within the project infrastructure without a fixed retention period, as data volume and reuse requirements are still being evaluated. The consortium has agreed to maintain all collected data for the purpose of validation, reporting, and potential cross-work-package integration during the OCCTET project's lifetime.
A formal data retention policy and anonymization schedule will be defined in coordination with the consortium and reflected in a future update.
Users may request deletion of their data at any time; audit logs remain pseudonymized and restricted to authorized personnel for security and compliance tracking.
This processing is consistent with the project Data Management Plan (DMP). No ethics issues requiring prior approvals are triggered by this deliverable.
This section aligns with the OCCTET Data Management Plan (D1.2) and follows the GDPR and Ethics requirements described in the Grant Agreement, Articles 13–19.

# 6. Conclusion and Next Steps

The OCCTET CRA Self-Assessment Model and Survey represent a tangible achievement of WP2, transforming the abstract and often complex Cyber Resilience Act (CRA) requirements into a practical, structured, and user-friendly tool for Small and Medium-Sized Enterprises (SMEs).
Through the iterative design, validation, and testing processes, the consortium has developed an operational platform — available at https://cra.occtet.eu – that:

- Demonstrates regulatory traceability between CRA Articles, Annexes, and self-assessment indicators.
- Provides SMEs and FOSS developers with a transparent entry point to assess CRA applicability and readiness.
- Implements GDPR-compliant data handling and secure authentication mechanisms.
- Generates measurable outputs, such as section-based maturity scores, CRA readiness level, and improvement recommendations.
- Supports interoperability with future OCCTET components for testing, evidence management, and conformity workflows.

The deliverable validates that the CRA Self-Assessment Portal achieves its main goal: helping SMEs navigate the complex regulatory environment through a self-paced, guided, and comprehensible process — without requiring external consultancy or prior legal expertise.

## 6.1. Validation outcomes and Readiness

Following the validation phase (Section 5), all technical, regulatory, and usability objectives have been met or exceeded:

- 100% CRA clause coverage was confirmed through expert cross-mapping.
- 96% accuracy achieved in Oxy AI guidance responses.
- GDPR audit passed with no issues identified.
- System uptime 99.83%, proving platform stability.

These results confirm that the version of the CRA Self-Assessment Platform is ready for operational deployment and external promotion under OCCTET communication and dissemination activities.

## 6.2. Technical Lessons Learned

During the development and pilot phases, the team identified several insights valuable for continuous improvement:

- **Importance of traceability**: The mapping between CRA legal clauses and survey questions must remain version-controlled and publicly traceable for auditability.
- **User comprehension vs. technical accuracy**: Simplified language increases participation but requires clear legal references to maintain credibility.
- **Data model flexibility**: Future updates to the database schema should anticipate version history tracking, incremental data capture, and multi-language support.

- **Oxy evolution**: The AI guidance system will benefit from iterative training as SMEs interact and pose new context-specific questions.
- **Regulatory volatility**: As the CRA enters implementation and enforcement stages (2026–2027), further amendments or guidance documents are expected. The model must therefore remain adaptive.

## 6.3. Versioning, Change management and CRA Alignment

A structured versioning policy ensures that both the model and platform evolve responsibly and traceably.
Each new release will include:

- A documented model version (e.g., v1.2 CRA alignment update),
- A database migration log (recording schema changes and data transformation steps), and
- A survey version identifier embedded in all generated reports for audit verification.

These mechanisms guarantee that, as CRA evolves or new guidance from ENISA or the European Commission becomes available, the self-assessment logic and corresponding technical implementation can be updated without disrupting existing user data.
Planned Change Example:
The database schema will be extended to support historical record-keeping of each survey response and CRA version. This feature, discussed internally during WP2 review, will allow SMEs and auditors to track how a company's CRA maturity evolves over time.
Team members (Expertware developers) confirmed that such schema adjustments pose no technical or audit issues, provided they are version-documented and backward compatible.

## 6.4. Future Improvements and Planned Enhancements

The consortium recognises that this deliverable reflects the first operational iteration of a continuously improving system.
As SMEs begin to use the platform more extensively, further refinements will be introduced based on feedback and emerging regulatory or technical needs.
Planned enhancements include:

| Aria | Planned Improvement | Rationale / Benefit |
|---|---|---|
| **Survey Model** | Add contextual examples and explanations for low-scoring sections (e.g., logging/detection). | Support SMEs with clearer self-correction guidance. |
| **Question Context and Scope** | Tag each question as [Product], [Process], or [Organisation] to clarity intent (feedback from Double Open) | Increase interpretability and response accuracy. |
| **Risk Assessment Integration** | Add a preliminary Risk Tier step influencing control weight (feedback from Double Open) | Ensure proportionality with CRA Article 8. |

| | | |
|---|---|---|
| **Database and Data Model** | Introduce historical data tracking and schema extensions to manage multiple CRA versions. | Enable long-term trend analysis and audit trails. |
| **Oxy AI Assistant** | Expand knowledge base and contextual memory. | Improve accuracy and handle cross-regulation queries (CRA + NIS2). |
| **Benchmarking Dashboard** | Develop a public anonymized dashboard of aggregated SME scores. | Facilitate policy insights and encourage participation. |
| **Automated CRA Update Feed** | Integrate with EUR-Lex or ENISA for live CRA guidance updates. | Keep the model continuously aligned with evolving CRA rules. |

## 6.5. Sustainability and Long-Term Vision

The CRA Self-Assessment Model will remain the entry point of the broader OCCTET ecosystem, feeding structured readiness data into testing (WP3) and evaluation tools (WP4). The underlying architecture and open design ensure sustainability and adaptability beyond the project's lifetime.
Continuous collaboration with SMEs, regulators, and open-source communities will ensure that OCCTET remains a reference platform for CRA compliance support across Europe.

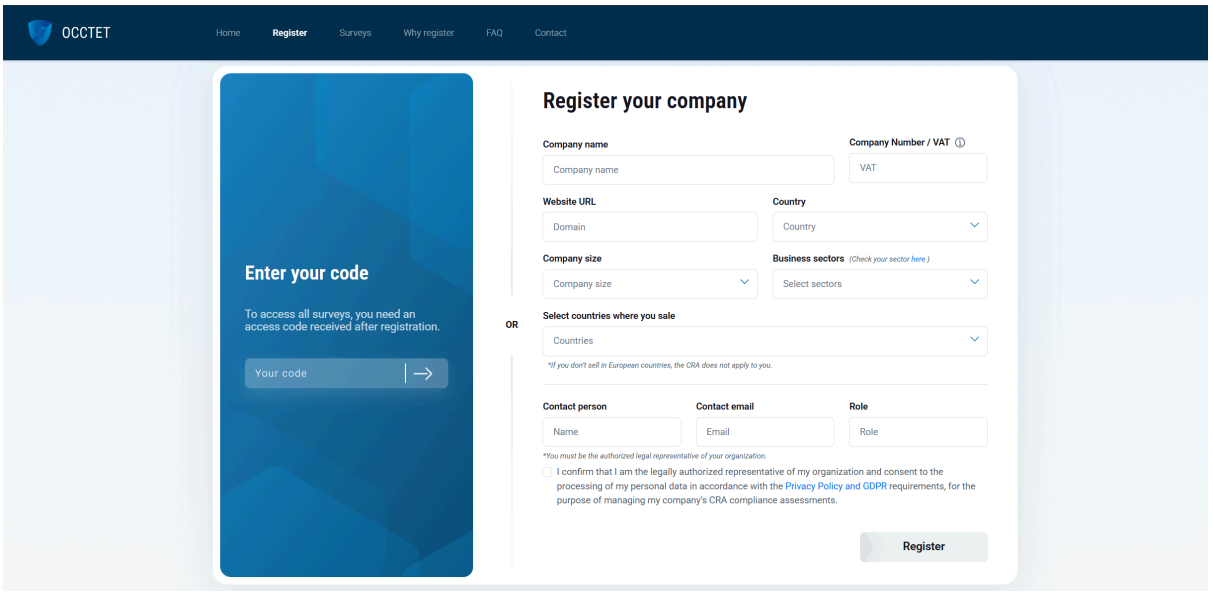
## 6.6. Final Remarks

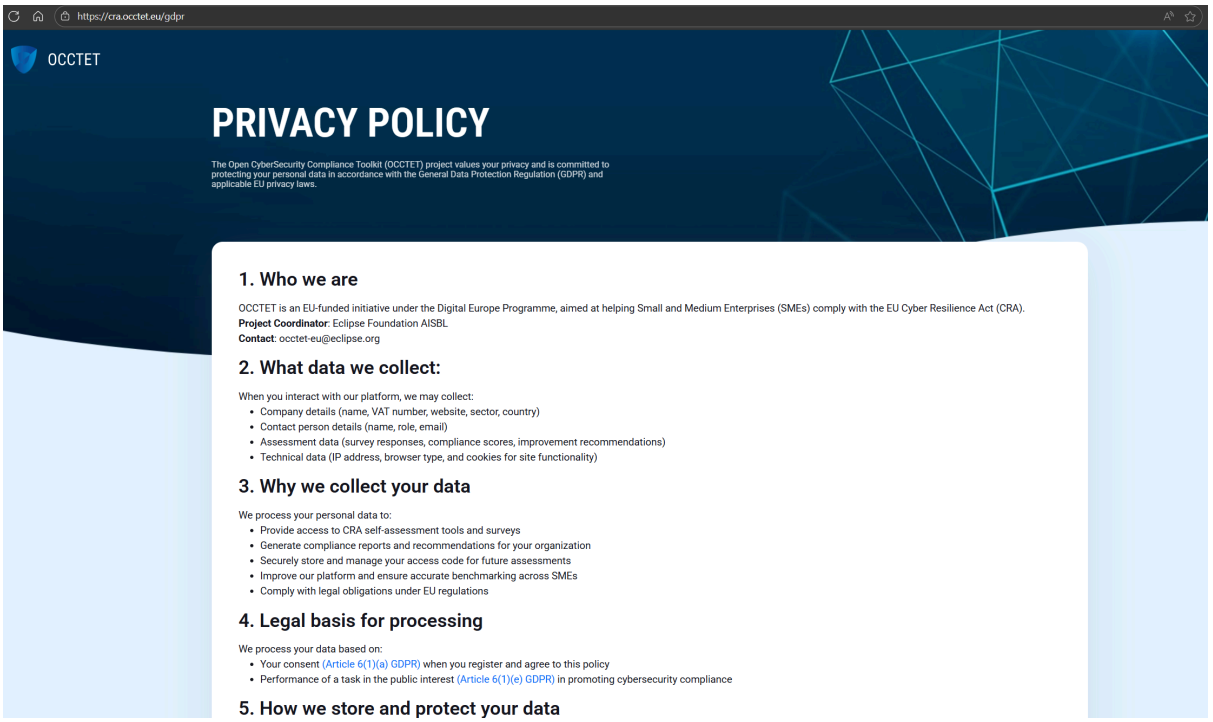
In conclusion, D2.2 delivers a functionally validated, methodologically sound, and strategically valuable component of the OCCTET project.
It operationalises one of the EU's most significant cybersecurity regulations — the CRA — in a form accessible to SMEs, while maintaining academic and technical rigour expected by European Commission evaluators.
The consortium will continue to maintain, update, and expand the CRA Self-Assessment Platform as legislation evolves and adoption grows.
Versioning and traceability mechanisms ensure that future updates, including database schema refinements and extended survey logic, can be integrated safely and transparently, maintaining full alignment with EU audit and compliance expectations.

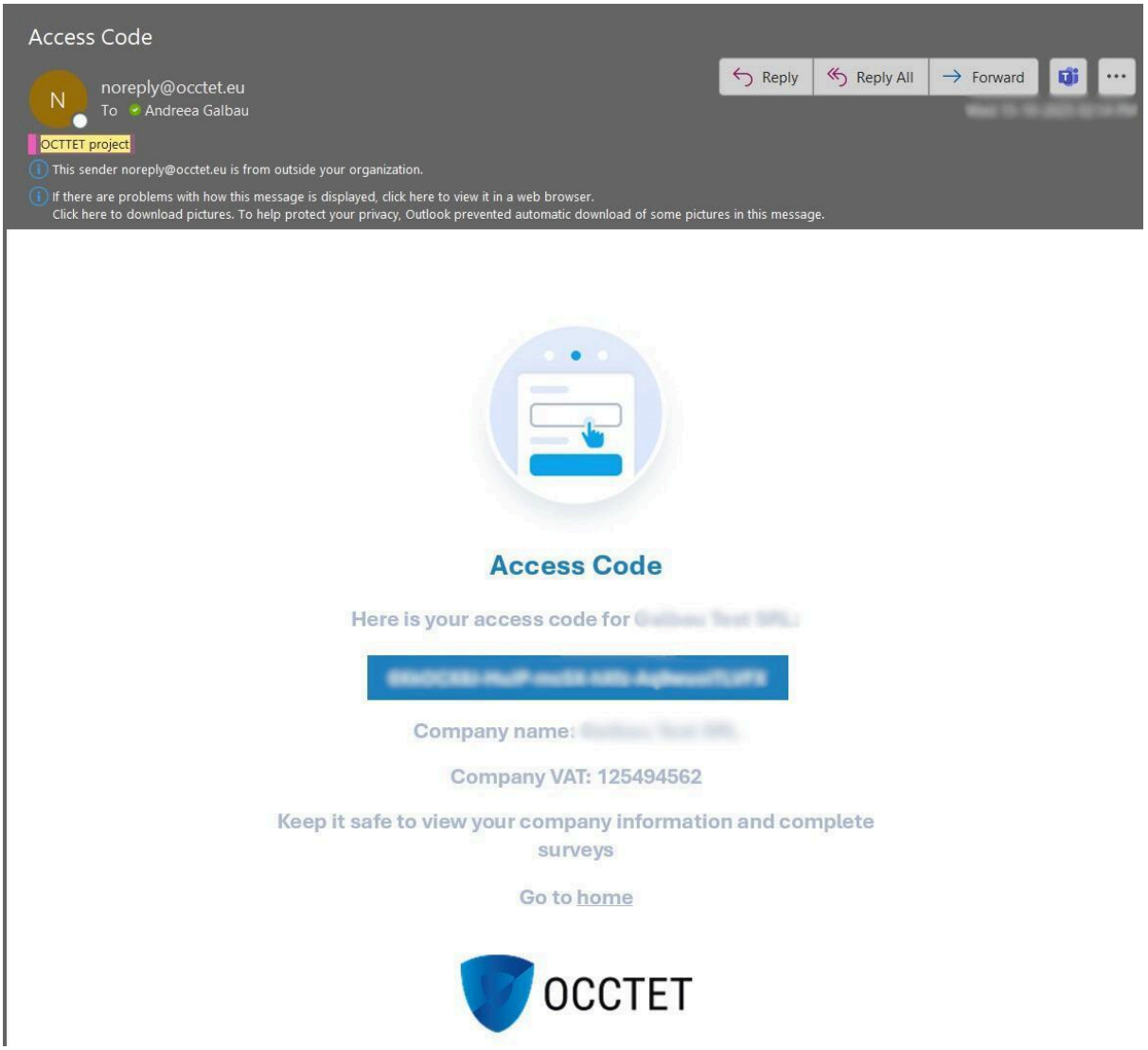
## 6.7. IPR and Licencing Notice

# 7. Annex 1 – Portal Screenshots

Figure A1-1: Login & Registration (screenshot placeholder)

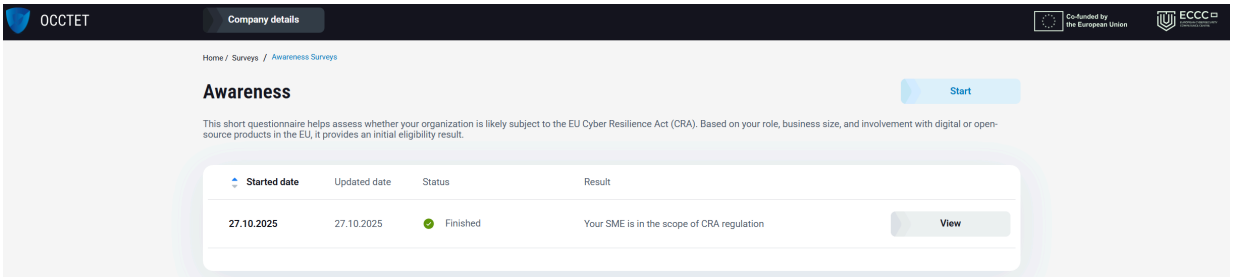


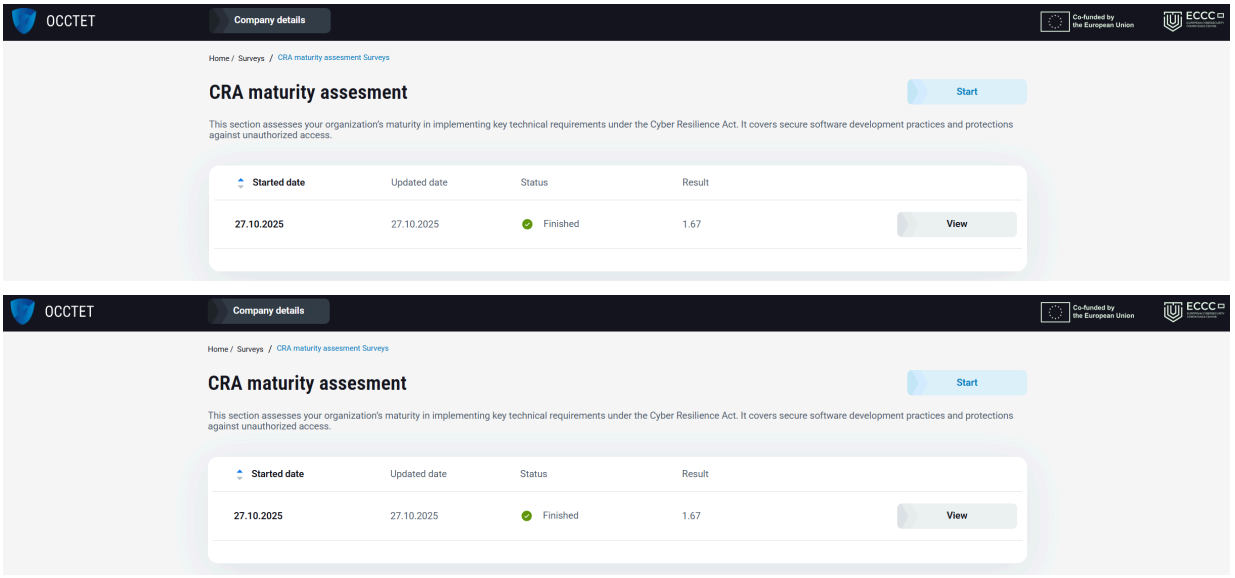






Description: Registration form with company public details, GDPR consent, access code issuance.

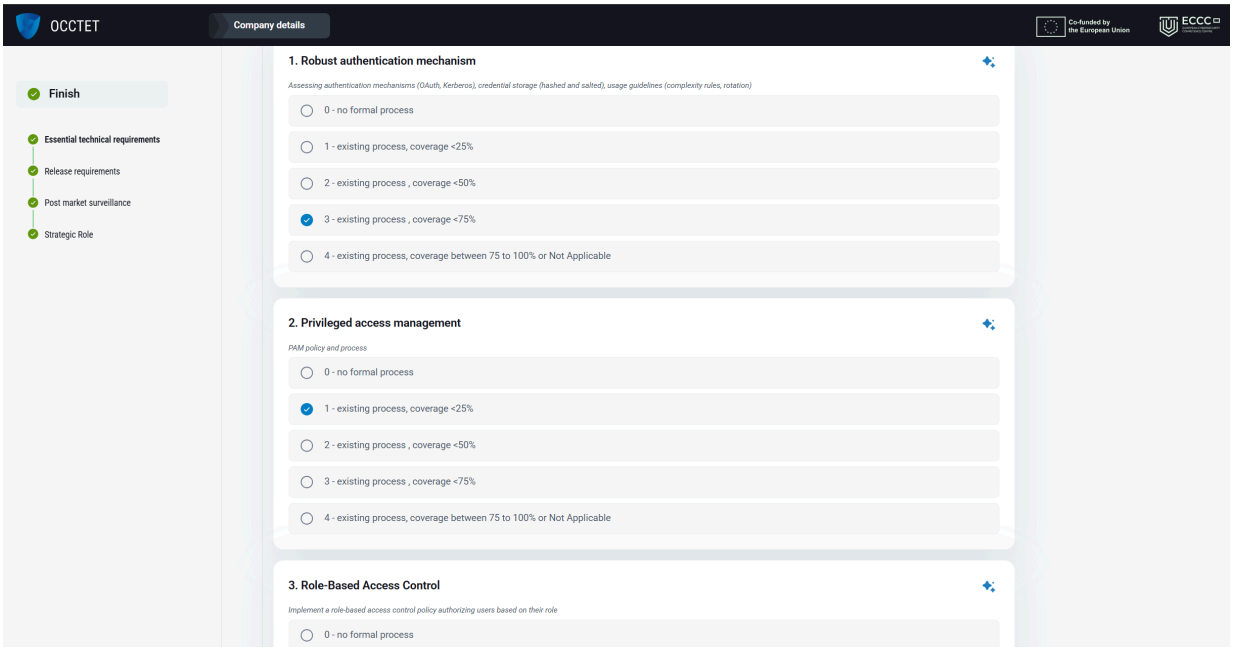
Figure A1-2: Dashboard Overview (screenshot placeholder)

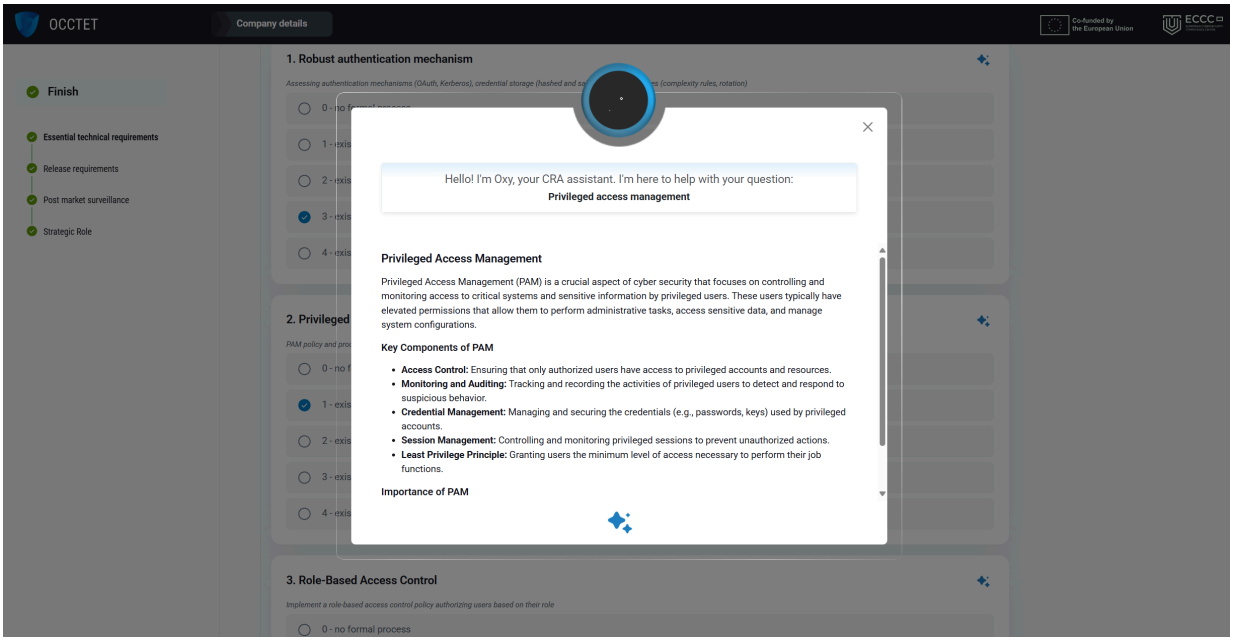





Description: Cards for Awareness/Qualification/Maturity; progress; questioner history.

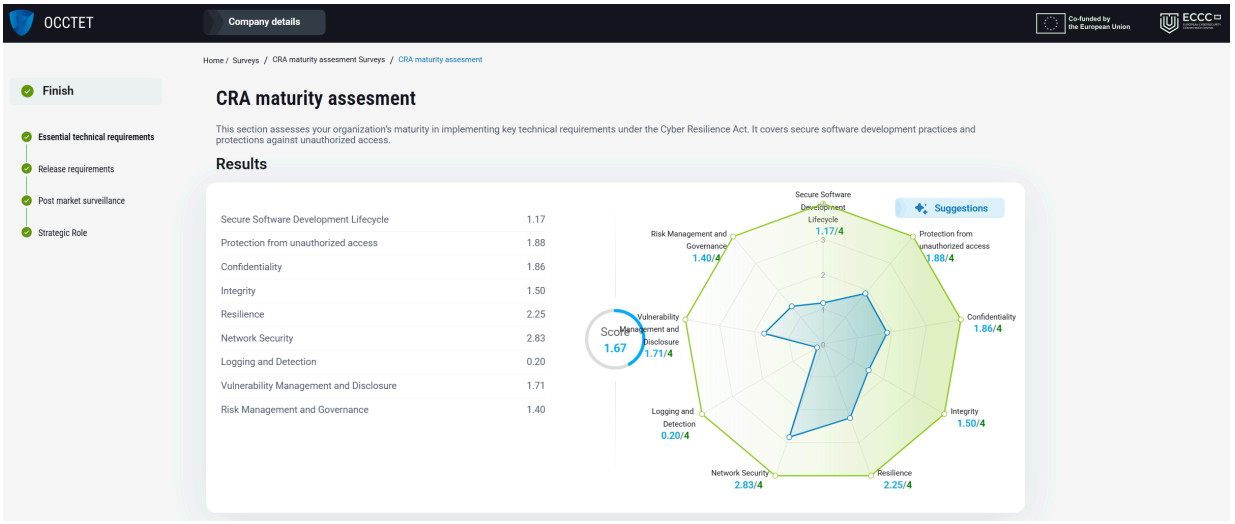
Figure A1-3: Example Question Interface

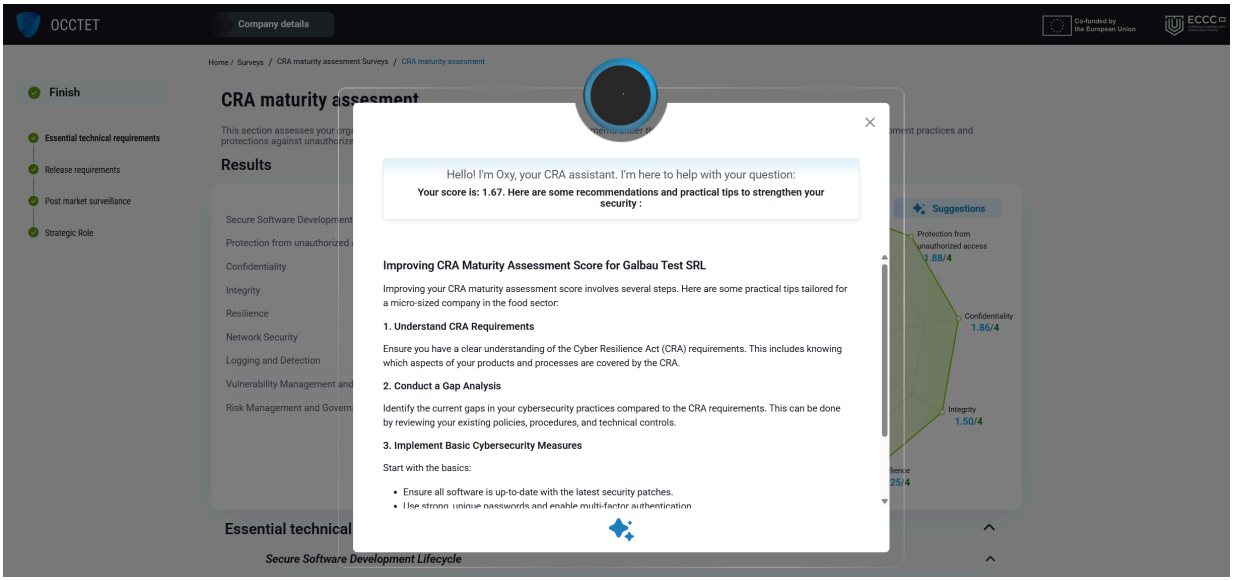





Description: Question with 0–4 scale; clause tooltip; Oxy “Ask me” widget.

Figure A1-4: Readiness Results Visualisation






Description: Section bars; overall score; recommendations; export buttons.

# 8. Annex 2 – Validation Tables

## A2.1. SME Pilot participation

| Sector | Country | Size | CRA Relevance | Date |
|---|---|---|---|---|
| **Manufacturing (embedded)** | DE | 45 | PDE with firmware | Jun 2025 |
| **IT Services (SaaS)** | RO | 18 | Limited scope | Jul 2025 |
| **Cybersecurity** | PT | 62 | PDE + safety | Aug 2025 |
| **Embedded Systems** | FR | 25 | PDE (software) | Aug 2025 |

## A2.2. KPI Summary

| Category | KPI | Target | Result |
|---|---|---|---|
| **CRA Mapping** | Clause coverage | 100% | 100% |
| **Oxy Accuracy** | Correctness | ≥ 90% | 96.2% |
| **Usability** | SUS | ≥ 85% | 92% |
| **Performance** | Avg API (ms) | ≤ 500 | 340 |
| **Availability** | Uptime | ≥ 99% | 99.83% |
| **Security** | Critical vulns | 0 | 0 |
| **GDPR** | Audit checklist | Pass | Pass |

## A2.3. Functional Test Samples

| Test | Scenario | Expected | Result |
|---|---|---|---|
| **EU-scope rule** | “No EU sales” | Out-of-scope message | Pass |
| **Role branching** | Manufactures vs Importer | Correct items displayed | Pass |
| **Scoring** | Section/overall means | ±0.01 tolerance | Pass |
| **Access code** | Result & Results | Results availability | Pass |

## A2.4. Initial SME Evaluation Summary (Pre – Pilot validation)

Before the formal pilot testing, an initial SME evaluation survey was distributed (March–August 2025) to gather early insights into awareness, preparedness, and challenges related to the Cyber Resilience Act (CRA).
The survey also tested the first prototype of the Awareness and Qualification modules.
To analyse SME profiles, identify pain points in CRA compliance, and validate the initial question logic before final model consolidation.

**Participation Overview**

| Metric | Value |
|---|---|
| Total responses | 10 (fully anonymized) |
| Period | March–August 2025 |
| Geographic distribution | Western & Central Europe (FR, IT, PT, AT, DE, EE) |
| Organization size | Micro (4), Small (2), Medium (2), Large (2) |
| Sectors represented | IT Services, Embedded Systems, Manufacturing, Law & Advisory, Cybersecurity, Distributor, Importer |
| CRA familiarity (self-declared) | Very familiar (6) • Somewhat familiar (2) • Not familiar (2) |

Main Insights:

- Awareness & Roles:
  - 60 % of SMEs were still uncertain whether CRA applied to them.
  - Confusion existed around product definitions and EU-market obligations.
- Common Challenges (Top 3):
  - Unclear regulatory requirements
  - Lack of internal expertise or resources
  - Complexity of integrating security into design
- Design-Phase Security:
  - 7 of 10 participants consider security early in design but lack structured tools.
  - Typical tools cited: OWASP guidelines, SAST scanners, GitHub CodeQL.
- Vulnerability Management:
  - Most rely on manual tracking; few use SBOMs or vulnerability scanners while others do not track product vulnerabilities.
- Standards Used:
  - ISO/IEC 27001 (4 responses) • ENISA Guidelines (4) • IEC 62443 (2) • NIS2 (1)
- Training Practices:
  - Annual or ad-hoc training is common; no SME reported continuous security education.
- Documentation Needs
  - SMEs requested templates, examples, and automated tools to generate CRA-compliant documentation.
- Use of Open Source:
  - 80 % use FOSS components. Key concern: lack of risk scoring and secure defaults.

Aggregated Example Findings:

| Question | Most Frequent Answers | Implication |
|---|---|---|
| Biggest challenges for CRA compliance? | Lack of budget / internal expertise / tools | Need for simple, guided SME approach |
| Tools used for secure design? | Static analysis / Code review / OWASP guidelines | Confirms readiness for tool integration |

| | | |
|---|---|---|
| **Do you have vulnerability disclosure process?** | Few (4 of 10) | CRA Annex I § 5 requires improvement |
| **Do you use SBOMs or dependency tools?** | 5 of 10 yes | Confirms relevance of OCCTET's SBOM module |
| **What documentation helps?** | Templates and examples | Supports OCCTET Checklist and Specs Guide features |

Summary and Integration:
The early SME evaluation confirmed both the need and usability of a simplified, guided CRA self-assessment.
Insights directly influenced:

- Refinement of question wording (plain-language style).
- Inclusion of contextual guidance in each question.
- Definition of the Awareness → Qualification → Maturity survey journey.
- Addition of CRA clause tooltips and examples.

Results were subsequently validated during Milestone 5 and Red Alert Labs testing, ensuring full alignment between early feedback and the final deployed platform.
The feedback received from Double Open (October 2025) on survey context and risk-based applicability has been formally recorded in the WP2 improvement register and integrated into the continuous enhancement plan (see Section 6.4 – Future Improvements and Planned Enhancements).
These actions ensure that all post-validation partner observations are traceable within the project documentation while preserving the integrity of the validated D2.2 dataset.

## A2.5. Supporting Evidence for Tool testing (Section 5.4) - (PR1 Revision – Evidence Consolidation)

In response to the expert recommendation to increase traceability of the tool testing results reported in Section 5.4, this annex provides a structured description of the evidence sources underpinning each validation indicator.
This annex:

- references only metrics already reported in Section 5.4,
- introduces no new quantitative indicators,
- does not modify previously reported values,
- and does not include personal data.

All examples and metrics are aggregated and anonymised.

### A2.5.1. CRA Mapping Accuracy

Section 5.4 → Result: CRA Mapping Accuracy: 100%
CRA mapping accuracy refers to the completeness and consistency of the traceability between CRA Regulation (EU) 2024/2847 provisions (Articles, Annex I, Annex II), and the self-assessment question set implemented in the OCCTET portal.
This indicator is established through methodological validation, not runtime system testing.

The traceability between CRA legal requirements and the self-assessment questions is established through the structured methodology described in Section 2 of Deliverable D2.2 and was originally developed and validated in Deliverable D2.1.
Specifically:

- Each survey question is derived from one or more CRA Articles or Annex I / Annex II provisions, following a systematic legal decomposition process.
- Questions are grouped into thematic domains reflecting CRA structure (e.g. secure design, vulnerability handling, post-market surveillance, governance).
- A consistent mapping logic is applied across all three survey stages (Awareness, Qualification, Maturity).
- The mapping artefacts were reviewed internally by WP2 consortium partners with regulatory and cybersecurity expertise.

The CRA mapping was validated through:

- Consortium expert review, involving WP2 partners with regulatory, cybersecurity, and product-security expertise.
- Cross-checking against CRA legal text, ensuring that no essential CRA requirement was omitted or duplicated.
- Consistency checks across survey versions, confirming that scoring logic and question wording remained aligned with CRA intent.

As reported in Section 5.4, this validation confirmed 100% coverage of applicable CRA clauses within the scope of the self-assessment model.
The “100% coverage” statement reflects full coverage of applicable CRA requirements within the scope of an SME-oriented self-assessment model and verification that no essential CRA requirement was omitted.
The authoritative source of CRA traceability remains:

- the methodological description in Section 2 of this deliverable, and
- the original CRA-to-question derivation documented in Deliverable D2.1.

Traceability is therefore methodological and documented, not screenshot-based or interface-dependent.

### A2.5.2. Oxy Answer Accuracy

Section 5.4 → Result Oxy Answer Accuracy: 96.2%
Validation of the Oxy AI assistant is supported by Expertware internal OCCTET Technical Performance Report, Consortium-level testing during WP2 validation and Milestone 5 pilot activities.
According to the OCCTET Technical Performance Report:

- Automated semantic verification was implemented using a Python-based framework.
- Generated responses were compared against a validated “Golden Dataset”.
- Guardrails were tested using in-scope and out-of-scope prompts.
- 100% valid HTTP responses were recorded during the automated audit window.
- The system met or exceeded the internal ≥90% semantic accuracy threshold.

The 100% result reported in the OCCTET Technical Performance Report refers to a controlled automated semantic audit using a predefined validation dataset. The 96.2%

accuracy reported in Section 5.4 reflects aggregated operational validation across pilot usage and consortium testing sessions under real-user conditions.
The report explicitly describes API stability, OXY latency behaviour (~31.9s average generation time), Guardrail enforcement and Formatting consistency (HTML structure validation).
During WP2 validation and Milestone 5:

- Consortium partners tested Oxy during survey completion.
- Feedback confirmed that explanations were generally:
  - clear,
  - aligned with CRA references,
  - consistent with survey intent.

Feedback also identified performance-related UX improvements (e.g., generation time expectations), which were logged for future iterations.
Oxy responses are grounded in Official text of Regulation (EU) 2024/2847 (CRA), CRA Annex I and Annex II provisions and internal CRA mapping artefacts (D2.1, D2.2)
Oxy:

- does not perform automated compliance decisions.
- does not determine CRA applicability.
- does not influence survey scoring.

### A2.5.3. User Satisfaction (SUS Score)

Section 5.4 → Reported Result: System Usability Scale (SUS): 92%
Evidence description
The SUS score is derived from structured user feedback collected during:

- pilot testing activities,
- Milestone 5 validation sessions,
- supplementary testing conducted by Red Alert Labs (RAL).

Participants completed standard usability questionnaires after using the platform across the Awareness, Qualification, and Maturity surveys.
Audit clarification:

- The SUS score reflects perceived usability, not regulatory compliance.
- Feedback was anonymised and aggregated.
- The metric is used to support claims of usability and accessibility for SMEs.

### A2.5.4. GDPR Compliance Validation

Section 5.4 → Reported Result: GDPR Compliance Audit: Passed
Evidence description
GDPR compliance was validated through:

- alignment with the project Data Management Plan (Deliverable D1.2).
- verification of consent mechanisms, data minimisation, and access controls.
- confirmation that no special categories of personal data are processed.
- EU-based hosting and role-based access control implementation.

No formal external GDPR certification is claimed.

"Passed" indicates internal compliance verification against project requirements.
No legal audit or supervisory authority approval is implied.

### A2.5.5. System Availability and Stability

Section 5.4 → Reported Result: System uptime ≥ 99% (observed)
System availability was assessed using operational logs and infrastructure monitoring data for the OCCTET web application environment.
The extracted logs cover continuous operational periods during 2025 and show:

- uninterrupted daily availability entries across multiple consecutive months.
- no recorded service outages affecting survey availability.
- stable runtime behaviour of the public survey endpoints.

The raw log dataset includes timestamped uptime records for the expweb001 host across consecutive daily intervals.
This evidence supports the platform stability statement reported in Section 5.4.

### A2.5.6. API performance and Response Behaviour

Section 5.4 → Reported Result: Average API response time within acceptable limits
Evidence description
API performance testing was conducted and documented in the OCCTET Technical Performance Report. The assessment included:

- high-concurrency load testing of the public survey API endpoint.
- sustained traffic simulation (10 requests per second).
- latency percentile analysis (P50, P95, P99).

Reported findings include:

- 100% request success rate under tested load.
- median response times below 30 ms.
- 95% of requests served in under ~35 ms.
- no systemic availability or stability issues identified.

These results confirm that the platform meets production-grade performance expectations for an SME-oriented self-assessment tool.

# 9. ACRONYMS AND ABBREVIATION

CRA — Cyber Resilience Act
ENISA — European Union Agency for Cybersecurity
EU — European Union
GDPR — General Data Protection Regulation
FOSS — Free and Open-Source Software
AI — Artificial Intelligence
IPR — Intellectual Property Rights
KPI — Key Performance Indicator
PII — Personally Identifiable Information
RBAC — Role-Based Access Control
SBOM — Software Bill of Materials
SAST — Static Application Security Testing
DAST — Dynamic Application Security Testing
MFA — Multi-Factor Authentication
SOC — Security Operations Centre
IR — Incident Response
API — Application Programming Interface
TLS — Transport Layer Security
ISO — International Organization for Standardization
IEC — International Electrotechnical Commission
ETSI — European Telecommunications Standards Institute
SUS — System Usability Scale
TRL — Technology Readiness Level
WP — Work Package
DoA — Description of Action

# 10. BIBLIOGRAPHY

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 (Cyber Resilience Act), Official Journal of the European Union, L, 2024.
2. **European Union Agency for Cybersecurity (ENISA**), Good Practices for Security of Products with Digital Elements, ENISA, 2023.
3. **European Union Agency for Cybersecurity (ENISA**), Guidelines for Coordinated Vulnerability Disclosure, ENISA, 2022.
4. **ISO/IEC 27001:2022**, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, International Organization for Standardization / International Electrotechnical Commission, Geneva.
5. **ISO/IEC 62443-4-1:2018**, Security for industrial automation and control systems — Secure product development lifecycle requirements, ISO/IEC.
6. **ETSI EN 303 645 V2.1.1** (2020), Cyber Security for Consumer Internet of Things: Baseline Requirements, European Telecommunications Standards Institute.
7. **Directive (EU) 2022/2555** (NIS2 Directive) of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, Official Journal of the European Union, L 333, 27.12.2022.
8. **European Commission**, The Cyber Resilience Act — Questions & Answers, European Commission, 2024.
9. **European Commission**, DIGITAL Europe Programme – Model Grant Agreement, European Commission, 2024.
10. **OCCTET Project Consortium**, Description of Action (DoA), Grant Agreement No. 101190474, 2024.
11. **OCCTET Project Consortium**, CRA SME requirements and self-assessment checklists (D1.2), 2025.

Note: All regulatory and standards references correspond to the versions in force at the time of deliverable submission (October 2025). Future CRA guidance updates will be reflected in subsequent project releases.