
MÉLANIE BATS
MISSION:
CRA-POSSIBLE
CTO@OBEO
OBEO
OCX 26
OPEN COMMUNITY EXPERIENCE

MISSION BRIEFING

WHY CRA EXISTS & WHO IS RESPONSIBLE

WHY CRA EXISTS

- **Reduce** real risks
- **Prevent** incidents
- Build **secure products** by design

TOYS
must be safe.

DIGITAL PRODUCTS
must be secure by design.

KEY ACTORS

Manufacturer
builds and markets the product

Importer
brings it to the EU market

Distributor
makes it available

Authorized Representative
acts on behalf of the manufacturer

In most cases: **YOU ARE THE MANUFACTURER**

CRA IS NOT JUST COMPLIANCE.
IT'S ABOUT BUILDING SECURE PRODUCTS.

OBEO

OCX 26 OPEN COMMUNITY EXPERIENCE

MISSION BRIEFING: THE THREAT

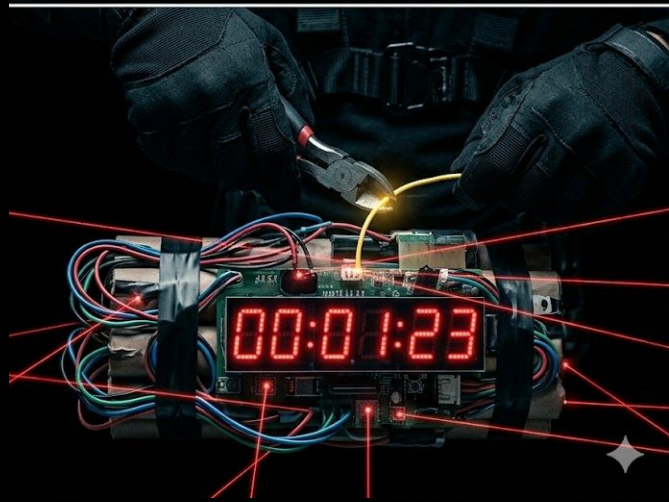
CRA (EU Regulation 2024/2847)

→ **Mandatory** by **2027**

Why it **feels hard**?

- Long → Complex requirements
- Ambiguous → Legal language
- Not directly actionable → No clear steps
- Cross-team impact → dev, security, product

"Reading CRA doesn't tell you what to do on Monday morning"



YOUR MISSION, SHOULD YOU ACCEPT IT

Become **CRA compliant**:

Without slowing down development,

Without adding **heavy processes**,

Without duplicating work.

"Integrate compliance into your existing workflow"

INTEL REPORT: WHAT CRA REALLY MEANS

CRA = 3 things

1. **Understand your risks**
2. **Address your risks**
3. **Prove it with evidence**

Implications:

- Not just security → **traceability**
- Not just action → **documentation**
- Not just docs → **consistency**

MISSION STRATEGY: TURN CHAOS INTO SYSTEM

We turned CRA into a system:

📄 Templates → structured deliverables

✅ Checklists → clear expectations

🔁 Workflow → ordered process

🤖 Toolchain → automated evidence

A reusable system you can apply to every product

“ Treat compliance like engineering, not paperwork ”

OBEO

OCX 26 OPEN COMMUNITY EXPERIENCE

MISSION 1: BUILD THE SYSTEM

CONFIDENTIAL

13
DELIVERABLES
STRUCTURED IN 5 BLOCKS

CONTEXT & SCOPE

01 Product Context
02 Asset Inventory

RISK MANAGEMENT

03 Threat Model
04 Risk Register
05 Risk Treatment Plan
06 Risk Communication Record

SECURITY LIFECYCLE

07 Security Plan
08 Verification & Validation Report

AUTOMATED EVIDENCE

09 SBOM
10 CVE Log

GOVERNANCE

11 Cybersecurity Policy
12 Risk Acceptance Criteria
13 Vulnerability Disclosure Policy

OBEO

OCX26 OPEN COMMUNITY EXPERIENCE

MISSION LEVELS: WHAT DOES THIS MEANS FOR YOU?

CRA responsibilities vary by role → You don't need to do everything, but you need to do the right things.

MANUFACTURER

Designs and develops the product

KEY RESPONSIBILITIES

- Full compliance with CRA requirements
- Risk management & security lifecycle
- Technical documentation & evidence
- Declaration of Conformity

DELIVERABLES SCOPE

Full set of deliverables

IMPORTER

Places a product from a third country on the EU market

KEY RESPONSIBILITIES

- Verify that the product complies with CRA
- Ensure required documentation is available
- Maintain traceability
- Keep DoC and key evidence accessible

DELIVERABLES SCOPE

Sub-set of deliverables (verification & access)

DISTRIBUTOR

Makes the product available on the EU market

KEY RESPONSIBILITIES

- Ensure product has DoC
- Ensure manufacturer information is available
- Cooperate with authorities if needed

DELIVERABLES SCOPE

Minimal set (DoC & basic information)

OUR GOAL

Provide a practical framework that **adapts** to your role.

- Focus on what is required for your role
- Leverage the right evidence from others
- Stay compliant, without unnecessary complexity

TAKEAWAY Understand your role. Produce **what's** required. Rely on what others provide. Compliance is a shared mission.

OBEO

OCX 26 OPEN COMMUNITY EXPERIENCE

MISSION SPLIT: HUMANS VS MACHINES

To make CRA work, you need both:

🤖 Machines = Evidence & Monitoring

- SBOM generation
- Vulnerability detection
- Security scans
- Status tracking

🧠 Human = Context & Risk Management

- Risk decisions
- Threat modeling
- Architecture
- Accepting or rejecting risks

"Automation produces evidence"

"Humans make the decisions"

MISSION 2: FOLLOW THE SEQUENCE

Each step produces one or more deliverables

Each step depends on the previous one

You cannot skip steps

MISSION 3: WHAT COULD GO WRONG?

Threat model = identify attacks on your product

Ask 3 questions:

- Who can attack?
- What do they target?
- How can they attack?

Build from:

- **Assets** (what you protect)
- **Shared threats catalogue** (common threats)
- **Product-specific threats**

Every threat must be linked to at least one asset

"Think like an attacker"

OBEO

OCX 26 OPEN COMMUNITY EXPERIENCE

MISSION 4: MAKE RISK DECISION EXPLICIT

For each threat:

- Assess **likelihood** (1–5)
- Assess **impact** (1–5)
- Compute risk level
- Decide: acceptable or not
- Decision is mandatory

Every risk must have a clear status:

- Acceptable
- Not acceptable

"Every decision must be justified"

OBEO

OCX 26 OPEN COMMUNITY EXPERIENCE

MISSION 5: TURN RISK INTO ACTION

For each unacceptable risk:

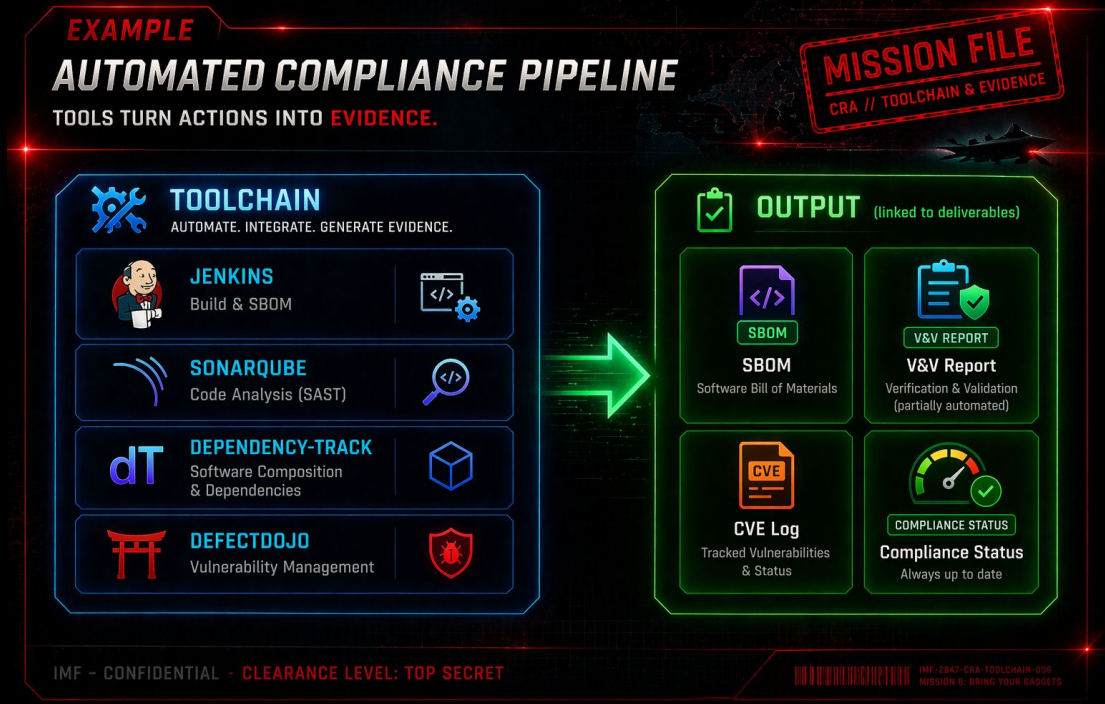
1. Choose a **treatment option**: Mitigate / Avoid / Transfer / Accept
2. Define **concrete measures**
3. Assign an **owner + deadline**
4. Define how you **verify** it

"No vague actions : only concrete measures!"

MISSION 6: BRING YOUR GADGETS

Automated pipeline: Every build produces compliance evidence

"Evidence is generated continuously, not manually"



OBEO

OCX 26 OPEN COMMUNITY EXPERIENCE

MISSION 7: MAKE IT REAL

How we implemented it:

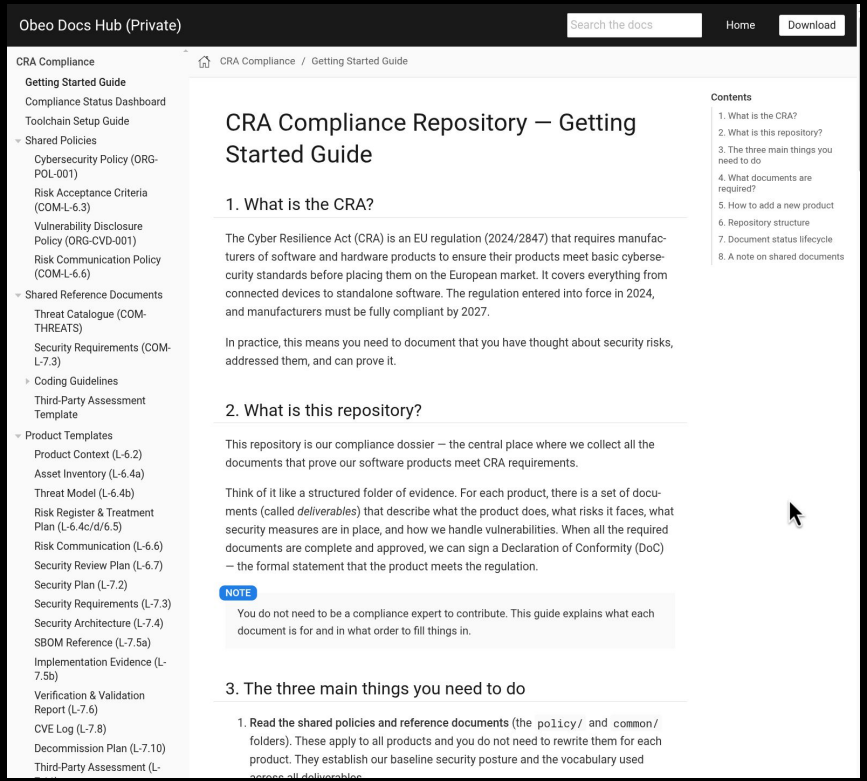
- Templates written in AsciiDoc
- Centralised with Antora
- One template per deliverable

For **each product**:

- Templates are instantiated
- Stored in the product repository
- Versioned with the code

Result:

- Same structure for all products
- Easy to maintain and evolve
- Compliance becomes part of development



"Compliance lives with the code"

OBEO

OCX26 OPEN COMMUNITY EXPERIENCE

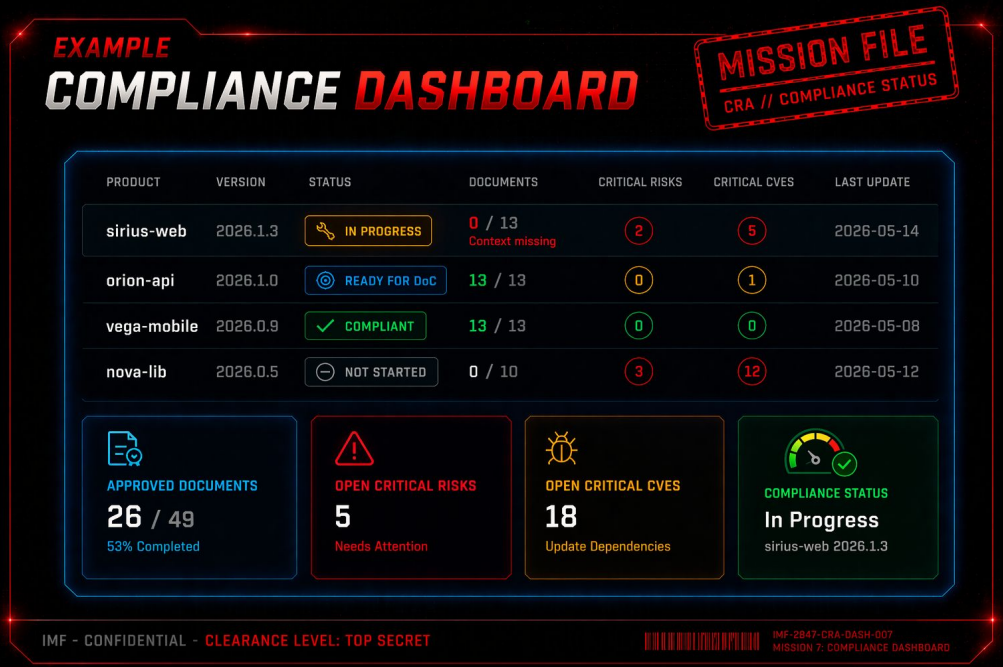
MISSION 8: TRACK YOUR PROGRESS

What you track

- Approved documents
- Open critical risks
- Open critical CVEs

Status levels

- 🚫 Not Started
- 🚧 In Progress
- 🎯 Ready for DoC
- ✅ Compliant



"You always know what is missing"

OBEO

OCX 26 OPEN COMMUNITY EXPERIENCE

CRA COMPLIANCE CHEATSHEET

13 DELIVERABLES • 5 THEMES • 1 SYSTEM

COMPLIANCE IS A SYSTEM

CONTEXT & SCOPE

Understand the product and what needs to be protected

1 PRODUCT CONTEXT

OBJECTIVE

Describe the product, its intended use and its operational environment.

CONTENT

- Product description, main functionalities
- Target users, deployment context (cloud, on-prem, embedded...)
- System boundaries and interfaces

2 ASSET INVENTORY

OBJECTIVE

Identify what needs to be protected.

CONTENT

- List of assets (data, services, components)
- Classification (critical, sensitive...)
- Mapping between assets and product components

RISK MANAGEMENT

Identify, assess, decide and communicate

3 THREAT MODEL

OBJECTIVE

Identify potential threats affecting the product.

CONTENT

- Threats linked to assets
- Threat actors (internal, external)
- Attack vectors, entry points
- Reuse of shared threat catalogues
- Product-specific threats

4 RISK REGISTER

OBJECTIVE

Assess and prioritize risks.

CONTENT

- List of identified risks
- Likelihood scoring, impact scoring
- Risk level (e.g., likelihood × impact)
- Risk prioritization

5 RISK TREATMENT PLAN

OBJECTIVE

Define how risks are handled.

CONTENT

- Treatment decision: mitigate, avoid, transfer or accept
- Concrete security measures
- Mapping to risks, owner, deadlines
- Traceability to implementation

6 RISK COMMUNICATION RECORD

OBJECTIVE

Ensure that risk decisions are explicit and documented.

CONTENT

- Risk acceptance decisions
- Justifications
- Stakeholder validation
- Decision history

SECURITY LIFECYCLE

Build security into development

7 SECURITY PLAN

OBJECTIVE

Define how security is integrated into the development lifecycle.

CONTENT

- Security activities per phase (design, develop, test, release)
- Roles and responsibilities
- Security controls and practices
- Integration with CI/CD

8 VERIFICATION & VALIDATION REPORT

OBJECTIVE

Demonstrate that security measures are implemented and effective.

CONTENT

- Security testing results
- Verification of implemented controls
- Penetration tests / audits
- Coverage of requirements

AUTOMATED EVIDENCE

Prove continuously

9 SOFTWARE BILL OF MATERIALS (SBOM)

OBJECTIVE

Provide transparency on software components.

CONTENT

- List of dependencies and components
- Versions, suppliers
- Licensing information
- Generated automatically where possible

10 VULNERABILITY & CVE LOG

OBJECTIVE

Track known vulnerabilities and their status.

CONTENT

- List of detected vulnerabilities (CVEs)
- Severity
- Status (open, mitigated, accepted)
- Links to fixes or mitigations
- Continuous update via tooling

GOVERNANCE

Define rules, set the bar, manage disclosure

11 CYBERSECURITY POLICY

OBJECTIVE

Define the organization's security principles and rules.

CONTENT

- Security objectives
- Secure development principles
- Roles and responsibilities
- Compliance commitments

12 RISK ACCEPTANCE CRITERIA

OBJECTIVE

Define what level of risk is acceptable.

CONTENT

- Risk thresholds
- Decision guidelines
- Aligment with business impact

13 VULNERABILITY DISCLOSURE POLICY

OBJECTIVE

Define how vulnerabilities are reported and handled externally.

CONTENT

- Reporting process for external parties
- Contact channels
- Response timelines
- Disclosure policy

WORKFLOW SEQUENCE

Compliance is a sequence, not a checklist.

1. **Product Context** — Describe product, usage, environment
2. **Assets** — Identify what needs to be protected
3. **Threats** — Identify what could go wrong
4. **Risks** — Assess likelihood and impact
5. **Treatment** — Decide and implement mitigation actions
6. **Evidence** — Prove measures are implemented and effective
7. **Declaration of Conformity** — Declare compliance

KEY PRINCIPLES

- Compliance follows a defined sequence, not a checklist
- Each document has a clear purpose and ownership
- Documents are interconnected and traceable (assets → threats → risks → treatment → evidence)
- Automate evidence whenever possible
- Version documentation with the product
- Vompliance is an engineering system, not paperwork

Turn CRA into a system. Mission Possible.

OBEO

OCX26 OPEN COMMUNITY EXPERIENCE

MISSION+: EXTEND THE SYSTEM

BEYOND THE MINIMUM - BUILD A STRONGER COMPLIANCE SYSTEM

BACKBONE + ENRICHMENT

TWO LEVELS. ONE SYSTEM.

CORE: REQUIRED

The backbone.
13 deliverables to comply.

= MINIMUM & STRUCTURE

RECOMMENDED

Go further.
Add depth, maturity and operational strength.

= ENRICH & STRENGTHEN

ARCHITECTURE & DESIGN

What to add
- System architecture description
- Data flow diagrams (DFD)

Enriches
- Product Context
- Threat Model

Brings
- Better understanding
- More accurate threats
- Clearer boundaries

SECURE DEVELOPMENT

What to add
- Secure coding guidelines
- Code review checklist

Enriches
- Security Plan
- Verification & Validation

Brings
- Consistent practices
- Fewer vulnerabilities
- Stronger implementation

13 REQUIRED DELIVERABLES

COMPLIANCE BACKBONE

Gives you structure, traceability and a solid starting point.

OPERATIONS & MONITORING

What to add
- Incident response plan
- Monitoring & logging strategy

Enriches
- Security Plan
- Vulnerability & CVE Log

Brings
- Faster detection & response
- Continuous visibility
- Stronger evidence over time

THIRD-PARTY & SUPPLY CHAIN

What to add
- Supplier assessment
- Third-party risk analysis

Enriches
- Asset Inventory
- Risk Register
- SBOM

Brings
- Better supplier visibility
- Managed supply chain risks
- Stronger trust

TESTING & ASSURANCE

What to add
- Security test strategy
- Detailed penetration test reports

Enriches
- Verification & Validation Report

Brings
- Deeper testing coverage
- Proof of effectiveness
- Confidence in compliance

KEY IDEA

THE 13 GIVE YOU THE SPINE.

THE RECOMMENDED ADD THE MUSCLES.

TAKEAWAY 13 DOCUMENTS ARE THE BACKBONE. THESE MAKE IT STRONGER.

Start with the required.
Grow with the recommended.

OBEO

OCX 26 OPEN COMMUNITY EXPERIENCE

MISSION INSIGHT

- **CRA is** not just regulation → it's a **system**
- **Compliance is** not a phase → it's a **workflow**
- **Security is** not enough → you must **prove it**

"Turn compliance into a repeatable engineering practice"

Now playing in your organisation! Official release: 2027

OBEO

OCX26 OPEN COMMUNITY EXPERIENCE

THANK YOU

THIS PRESENTATION WILL SELF-DESTRUCT IN:

3... 2... 1...

melanie.bats@obeo.fr

OBEO

OCX 26
OPEN COMMUNITY EXPERIENCE