

**MÉLANIE BATS**  
**MISSION:**  
**CRA-POSSIBLE**  
**CTO@OBEO**

# 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.

**SAME IDEA.**  
**DIGITAL WORLD.**



### 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.**

# 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”*



# MISSION 1: BUILD THE SYSTEM

CONFIDENTIAL



## 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





# 13

## DELIVERABLES

STRUCTURED IN 5 BLOCKS

# 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.

 <p><b>MANUFACTURER</b> Designs and develops the product</p> <p><b>KEY RESPONSIBILITIES</b></p> <ul style="list-style-type: none"><li>• Full compliance with CRA requirements</li><li>• Risk management &amp; security lifecycle</li><li>• Technical documentation &amp; evidence</li><li>• Declaration of Conformity</li></ul> <p><b>DELIVERABLES SCOPE</b> Full set of deliverables</p>	 <p><b>IMPORTER</b> Places a product from a third country on the EU market</p> <p><b>KEY RESPONSIBILITIES</b></p> <ul style="list-style-type: none"><li>• Verify that the product complies with CRA</li><li>• Ensure required documentation is available</li><li>• Maintain traceability</li><li>• Keep DoC and key evidence accessible</li></ul> <p><b>DELIVERABLES SCOPE</b> Sub-set of deliverables (verification &amp; access)</p>	 <p><b>DISTRIBUTOR</b> Makes the product available on the EU market</p> <p><b>KEY RESPONSIBILITIES</b></p> <ul style="list-style-type: none"><li>• Ensure product has DoC</li><li>• Ensure manufacturer information is available</li><li>• Cooperate with authorities if needed</li></ul> <p><b>DELIVERABLES SCOPE</b> Minimal set (DoC &amp; basic information)</p>	 <p><b>OUR GOAL</b></p> <p>Provide a practical framework that adapts to your role.</p> <ul style="list-style-type: none"><li>✓ Focus on what is required for your role</li><li>✓ Leverage the right evidence from others</li><li>✓ Stay compliant, without unnecessary complexity</li></ul>
--	---	--	--



## TAKEAWAY

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

# 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”*



# 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

**EXAMPLE**

## RISK ASSESSMENT IN ACTION

MISSION FILE  
CRA // RISK REGISTER

**THREAT:** Brute force on login API

 <b>LIKELIHOOD</b> How likely is it to happen? <b>4</b> / 5 HIGH	 <b>IMPACT</b> What would be the damage? <b>3</b> / 5 MODERATE	 <b>RISK LEVEL</b> Likelihood × Impact <b>12</b> / 25 HIGH
---	--	--

 **DECISION:**  
Can we accept this risk?

**NOT ACCEPTABLE**  
A treatment plan is required.

CONFIDENTIAL - CLEARANCE LEVEL: TOP SECRET

*“Every decision must be justified”*

# 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!**”*

**EXAMPLE**

**MISSION FILE**  
CRA // TREATMENT PLAN

**FROM RISK TO ACTION**

**RISK:** Brute force on login API **HIGH**

**✗ BEFORE: VAGUE**

*“Improve security on the login API”*

**!** Too vague.  
Impossible to verify.

**>**

**✓ AFTER: CONCRETE & TESTABLE**

**TREATMENT: MITIGATE**

- **Rate limiting:** 5 attempts per minute per IP
- **Account lockout:** after 10 failed attempts, lock account for 15 minutes
- **MFA** required for admin accounts

**VERIFICATION:**  
**Penetration test**  
Login brute force attempt script

IMF - CONFIDENTIAL CLEARANCE LEVEL: TOP SECRET

OPEN COMMUNITY EXPERIENCE

# MISSION 6: BRING YOUR GADGETS

Automated pipeline: Every build produces compliance evidence

*“Evidence is  
generated continuously,  
not manually”*

EXAMPLE

## AUTOMATED COMPLIANCE PIPELINE

TOOLS TURN ACTIONS INTO EVIDENCE.

MISSION FILE  
CRA // TOOLCHAIN & EVIDENCE



### TOOLCHAIN

AUTOMATE. INTEGRATE. GENERATE EVIDENCE.



#### JENKINS

Build & SBOM



#### SONARQUBE

Code Analysis (SAST)



#### DEPENDENCY-TRACK

Software Composition  
& Dependencies



#### DEFECTDOJO

Vulnerability Management



### OUTPUT (linked to deliverables)



SBOM

#### SBOM

Software Bill of Materials



V&V REPORT

#### V&V Report

Verification & Validation  
(partially automated)



CVE Log

Tracked Vulnerabilities  
& Status



COMPLIANCE STATUS

#### Compliance Status

Always up to date

IMF - CONFIDENTIAL - CLEARANCE LEVEL: TOP SECRET



IMF-2047-CRA-TOOLCHAIN-005  
MISSION 6: BRING YOUR GADGETS

# 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

The screenshot displays the Obeo Docs Hub (Private) interface. At the top, there is a search bar and navigation links for Home and Download. The main content area is titled "CRA Compliance" and "Getting Started Guide". A sidebar on the left lists various documents, including "Compliance Status Dashboard", "Toolchain Setup Guide", "Shared Policies", "Cybersecurity Policy (ORG-POL-001)", "Risk Acceptance Criteria (COM-L-6.3)", "Vulnerability Disclosure Policy (ORG-CVD-001)", "Risk Communication Policy (COM-L-6.6)", "Shared Reference Documents", "Threat Catalogue (COM-THREATS)", "Security Requirements (COM-L-7.3)", "Coding Guidelines", "Third-Party Assessment Template", "Product Templates", "Product Context (L-6.2)", "Asset Inventory (L-6.4a)", "Threat Model (L-6.4b)", "Risk Register & Treatment Plan (L-6.4c/d/6.5)", "Risk Communication (L-6.6)", "Security Review Plan (L-6.7)", "Security Plan (L-7.2)", "Security Requirements (L-7.3)", "Security Architecture (L-7.4)", "SBOM Reference (L-7.5a)", "Implementation Evidence (L-7.5b)", "Verification & Validation Report (L-7.6)", "CVE Log (L-7.8)", "Decommission Plan (L-7.10)", and "Third-Party Assessment (L-7.9)".

The main content area is titled "CRA Compliance Repository – Getting Started Guide". It contains three sections:

- 1. What is the CRA?**

The Cyber Resilience Act (CRA) is an EU regulation (2024/2847) that requires manufacturers of software and hardware products to ensure their products meet basic cybersecurity standards before placing them on the European market. It covers everything from connected devices to standalone software. The regulation entered into force in 2024, and manufacturers must be fully compliant by 2027.

In practice, this means you need to document that you have thought about security risks, addressed them, and can prove it.
- 2. What is this repository?**

This repository is our compliance dossier – the central place where we collect all the documents that prove our software products meet CRA requirements.

Think of it like a structured folder of evidence. For each product, there is a set of documents (called *deliverables*) that describe what the product does, what risks it faces, what security measures are in place, and how we handle vulnerabilities. When all the required documents are complete and approved, we can sign a Declaration of Conformity (DoC) – the formal statement that the product meets the regulation.

**NOTE**

You do not need to be a compliance expert to contribute. This guide explains what each document is for and in what order to fill things in.
- 3. The three main things you need to do**
  1. Read the shared policies and reference documents (the policy/ and common/ folders). These apply to all products and you do not need to rewrite them for each product. They establish our baseline security posture and the vocabulary used across all deliverables.

A "Contents" sidebar on the right lists the following items:

1. What is the CRA?
2. What is this repository?
3. The three main things you need to do
4. What documents are required?
5. How to add a new product
6. Repository structure
7. Document status lifecycle
8. A note on shared documents





“Compliance lives *with the code*”

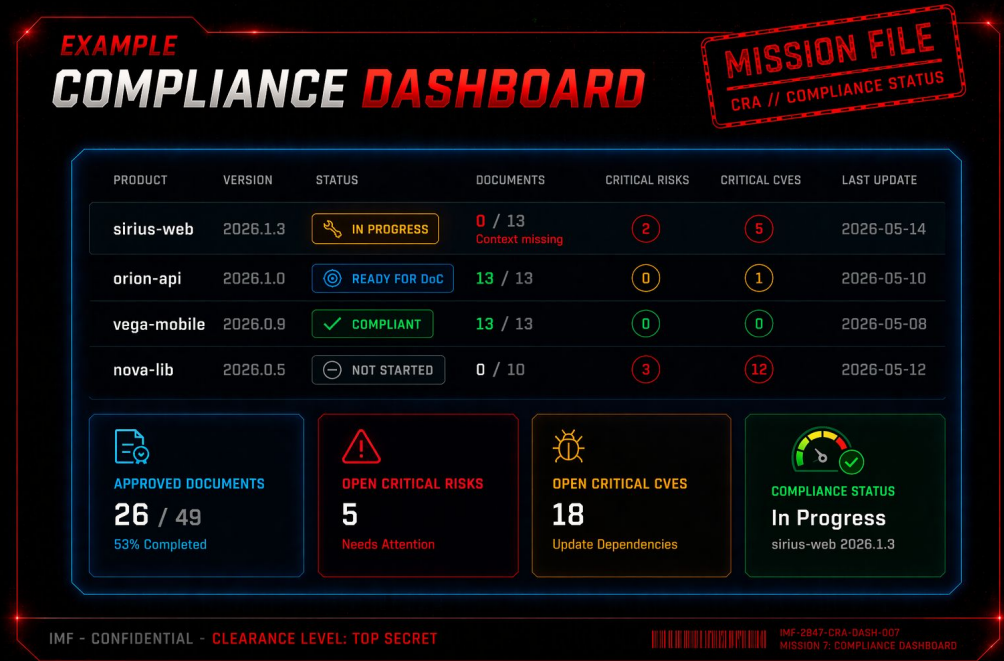
# MISSION 8: TRACK YOUR PROGRESS

## 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”

# 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 x 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, supplier
- 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
- Alignment 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
- Compliance is an engineering system, not paperwork



Turn CRA into a system. Mission Possible.

# 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



## 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



13  
REQUIRED  
DELIVERABLES

## COMPLIANCE BACKBONE

Gives you structure,  
traceability and a solid  
starting point.

## 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



## SECURE DEVELOPMENT

What to add

- Secure coding guidelines
- Code review checklist

Enriches

- Security Plan
- Verification & Validation

Brings

- Consistent practices
- Fewer vulnerabilities
- Stronger implementation



## 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



## 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.

# 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**”*



**YOUR MISSION : TURN CRA INTO A SYSTEM**

# MISSION ACCOMPLISHED



START WITH **ONE PRODUCT.**



FOLLOW THE **SEQUENCE.**



USE **TEMPLATES.**



**AUTOMATE EVIDENCE.**

**MISSION POSSIBLE.**



13 DOCUMENTS.  
4 BLOCKS.  
1 SYSTEM.

**Now playing in your organisation! Official release: 2027**

# THANK YOU

THIS PRESENTATION WILL SELF-DESTRUCT IN:

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



[melanie.bats@obeo.fr](mailto:melanie.bats@obeo.fr)

