First steps towards CRA conformity. A practical introduction to cybersecurity risk management

Harald Fischer
Security Aspect Lead @ balena

ONE DOES NOT SIMPLY
PUT A PRODUCT ON THE EU MARKET
imgflip.com

From Dec 11. 2027
Every manufacturer of products with digital elements, including software only products, placed on the EU market needs to declare conformity with the EU Cyber Resilience Act.

CRA Article 13 (2)

“Manufacturers **shall** undertake an **assessment** of the **cybersecurity risks** associated with a product with digital elements and take the outcome of that assessment into account during the **planning**, **design**, **development**, **production**, **delivery** and **maintenance phases** of the product with digital elements with a view to minimising cybersecurity risks, preventing incidents and minimising their impact, including in relation to the **health** and **safety** of users”

CRA Article 13 (3)

“That cybersecurity risk assessment **shall** comprise at least an analysis of cybersecurity risks based on the **intended purpose** and **reasonably foreseeable use**, as well as the **conditions of use**, of the product with digital elements, such as the **operational environment** or the **assets to be protected**, taking into account the **length of time the product is expected to be in use**.”

Requirements

Product Context

Criteria + Method

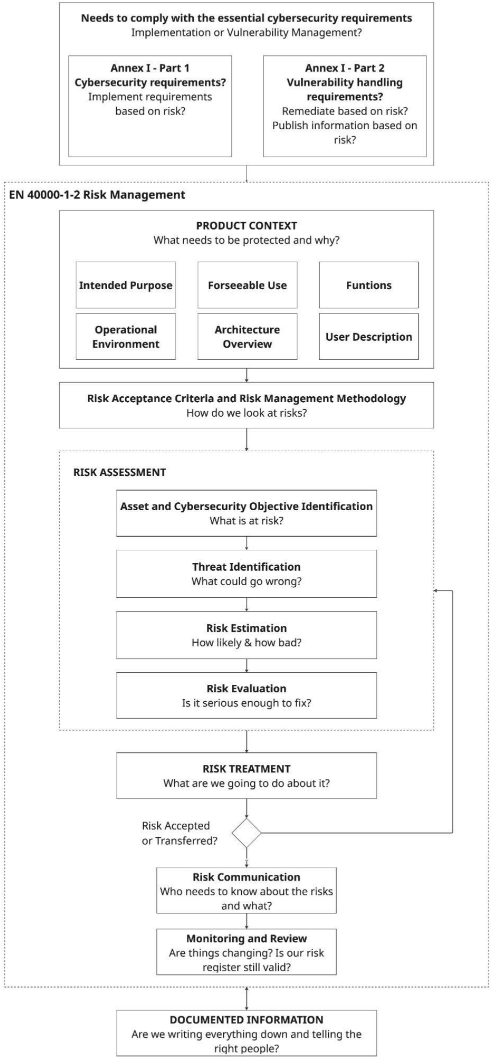
Risk Assessment

Risk Treatment

Communication

Review + Monitor

Documentation



Needs to comply with the essential cybersecurity requirements
Implementation or Vulnerability Management?

Annex I - Part 1
Cybersecurity requirements?
Implement requirements based on risk?

Annex I - Part 2
Vulnerability handling requirements?
Remediate based on risk?
Publish information based on risk?

EN 40000-1-2 Risk Management

PRODUCT CONTEXT
What needs to be protected and why?

Intended Purpose

Forseeable Use

Funtions

Operational Environment

Architecture Overview

User Description

Risk Acceptance Criteria and Risk Management Methodology
How do we look at risks?

RISK ASSESSMENT

Asset and Cybersecurity Objective Identification
What is at risk?

Threat Identification
What could go wrong?

Risk Estimation
How likely & how bad?

Risk Evaluation
Is it serious enough to fix?

RISK TREATMENT
What are we going to do about it?

Risk Accepted or Transferred?

Risk Communication
Who needs to know about the risks and what?

Monitoring and Review
Are things changing? Is our risk register still valid?

DOCUMENTED INFORMATION
Are we writing everything down and telling the right people?

EN40000-1-2 draft

CRA Requirements

Why you need the risk assessment

Example - Annex I Part 1 (j)

“be designed, developed and produced to limit attack surfaces, including external interfaces”

Does now every product need to protect against any physical local attacks?

Requirements

Why you need the risk assessment

1. **Read Essential Cybersecurity Requirements: CRA Annex I - Part 1 - 2(a-m) and Part 2 1+4**
2. **Do you need to implement the requirement?**
    a. What risks have you identified?
    b. How do you treat those risks?
    c. Do risks obligate an implementation?

Product context

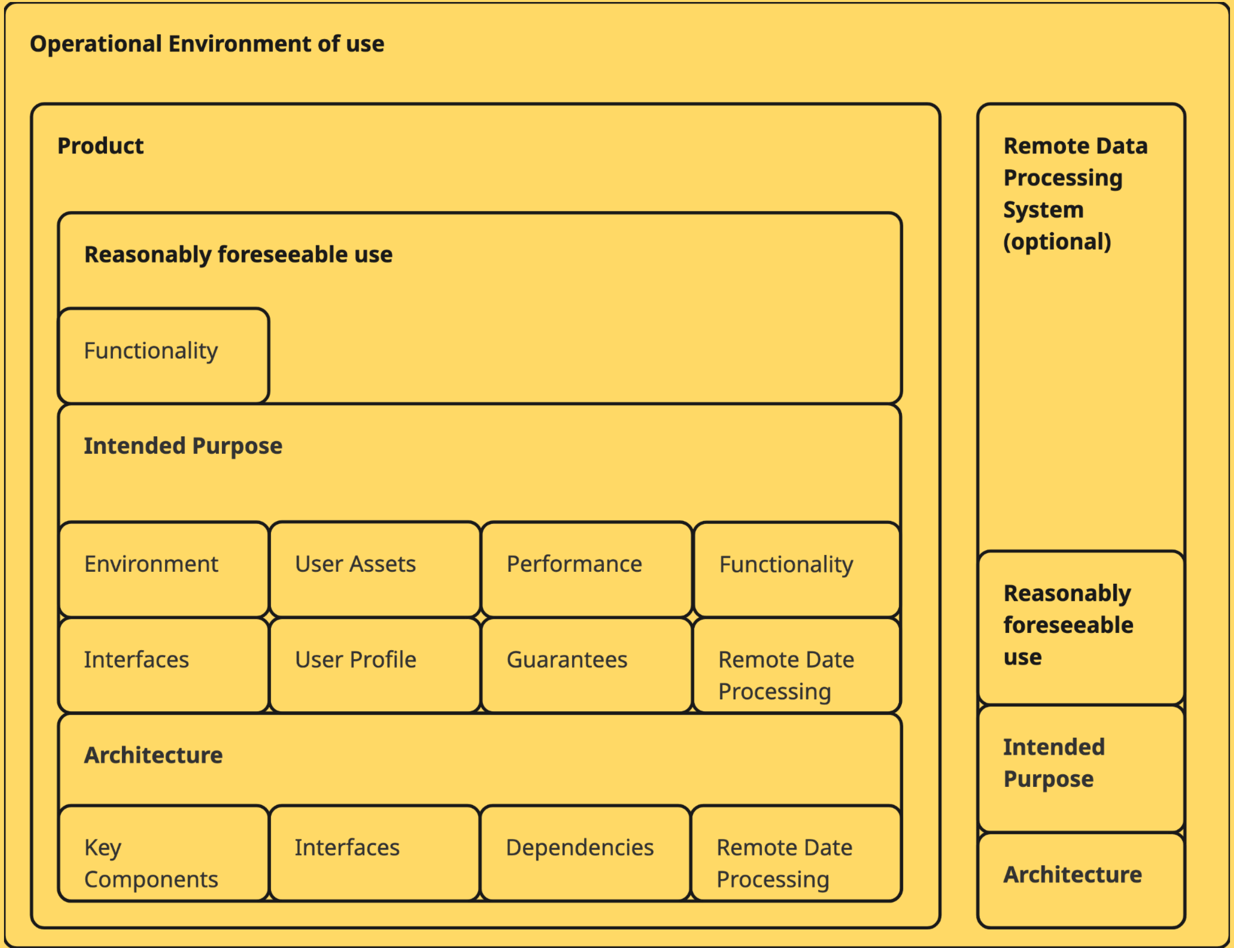
Product Context

Define your product as detailed and narrow as possible

- Intended purpose and reasonably foreseeable use
- Product’s functions
- Operational environment of use
- Product’s architecture overview
- Product’s user descriptions
- Needs a remote data processing system (RDPS)
    - Operational Environment of RDPS

Create a block diagram for better understanding

Product Context



Operational Environment of use

Product

Reasonably foreseeable use

Functionality

Intended Purpose

Environment

User Assets

Performance

Functionality

Interfaces

User Profile

Guarantees

Remote Date Processing

Architecture

Key Components

Interfaces

Dependencies

Remote Date Processing

Remote Data Processing System (optional)

Reasonably foreseeable use

Intended Purpose

Architecture

Product Context

Document your products context

1. **Create a list or table for your product and its remote data processing system with**
   a. all user profiles
   b. functions
   c. stored data
   d. interfaces
   e. dependencies and other assets
   f. Operational environment
2. **You’ll need this for the risk identification**

Risk acceptance criteria and risk management methodology

Criteria + Method

Define what is at risk: Cybersecurity Objectives

CIAPS

Confidentiality: Data is only accessible to authorized persons/systems

Integrity: Data and functions are protected against unauthorized changes

Availability: Critical functions are reachable and resilient during attacks

Privacy: Personal identifiable information (PII) is minimized and protected

Safety: The product does not cause physical harm or environmental damage

Criteria + Method

Define how you manage risks

1. **Define your risk management methodology**

   Like coding and review guidelines:

   a. How to identify risks

   b. How to estimate risk

      i. Likelihood and Impact

   c. How to evaluate treatment

   d. How to treat risks

2. **Define what risks can be accepted**

Criteria + Method

How do you identify Risks

- Execute Threat modelling practices
    - Four Question Framework
        - Shostack Threat Modeling
    - STRIDE
        - OWASP Threat Modeling Process
    - OWASP Threat Modeling Project

Criteria + Method

OWASP Risk Rating Methodology

1. **Risk = Likelihood * Impact**
   a. Likelihood = max(all likelihood factors)
   b. Impact = max(all impact factors)
2. You always needs to assess the **Inherent risk**
   a. The risk without any security measure
      i. No secure coding, no SAST/DAST, …
3. Then you treat the risks (Avoid, Mitigate, Accept, Transfer)
   a. Implement Secure Coding, SAST, …
4. Then you assess the **residual risks**

Criteria + Method

How you estimate **likelihood** - The "Attacker" Profile

Factor	Description & CRA Alignment	Scoring Criteria (1, 5, 9, 15)
Skill Level	Technical capability of the group	**1:** No skills **5:** Advanced user **9:** Security penetration skills
Motive	Incentive to find/exploit this specific target	**1:** Low | no reward **4:** Possible reward **9:** High reward
Opportunity	Resources required to find the exploit	**0:** Full | expensive access **4:** Special access **9:** No access required
Size	The population of the threat group	**2:** Developers **5:** Partners **9:** Anonymous Internet users
User Profile	**CRA EXTENSION:** Capability of the victim to mitigate	**1:** Professional | Supervised | Trained **5:** Adult Consumer **9:** Vulnerable | Child

Criteria + Method

How you estimate **likelihood** - The "Product" Profile

Factor	Description & CRA Alignment	Scoring Criteria (1, 3,4, 5, 6, 7, 9)
Ease of Discovery	Addresses Discoverability	**1:** Impossible **3:** Difficult **7:** Easy **9:** Automated tools.
Ease of Exploit	Addresses Attack Scalability	**1:** Theoretical **3:** Difficult **5:** Easy **9:** Automated tools
Awareness	Known status of the vulnerability	**1:** Unknown **4:** Hidden **6:** Obvious **9:** Public knowledge
Intrusion Detection	Speed of materialization/detection	**1:** Active detection **3:** Logged/Reviewed **9:** Not logged

How you estimate **impact** - Technical "Blast Radius"

Criteria + Method

Factor	Description & CRA Alignment	Scoring Criteria (1, 5, 9)
Confidentiality	How much data is disclosed?	**1:** Minimal non-sensitive **5:** Extensive sensitive **9:** Total data disclosure.
Integrity	How much data or firmware is corrupted?	**1:** Minimal non-sensitive **5:** Extensive sensitive **9:** Total data corruption
Availability	How much service/function is lost?	**1:** Secondary services **5:** Primary services **9:** Total loss of service
Accountability	Are the attacker's actions traceable?	**1:** Fully traceable **5:** Possibly traceable **9:** Completely anonymous
CRA / Scalability	**CRA EXTENSION:** Multi-product disruption via RDPS.	**1:** Single isolated instance **5:** Localized subset **9:** Simultaneous mass-exploitation

Criteria + Method

How you estimate **impact** - Your Liability Profile

Factor	Description & CRA Alignment	Scoring Criteria (1, 3, 4, 5, 7, 9, 15)
Financial Damage	Economic loss resulting from an exploit	**1:** < cost to fix **3:** Minor profit effect **7:** Significant profit effect **9:** Bankruptcy
Reputation Damage	Harm to the brand and market trust	**1:** Minimal **4:** Loss of major accounts **5:** Loss of goodwill **9:** Brand damage
Non-Compliance	Exposure introduced by regulatory violations	**2:** Minor violation **5:** Clear violation **7:** High profile violation.
Privacy Violation	Volume of PII disclosed to unauthorized parties	**3:** One individual **5:** Hundreds **7:** Thousands **9:** Millions of people
Safety | Health | CRITIS	**CRA EXTENSION:** Physical harm, RDPS scalability or Critical Infrastructure affected	**1:** No physical effec **5:** Minor injury/subset affected **9:** Direct safety concern, Mass disruption, **CRITIS**

Criteria + Method

How you calculate **risk score**

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Risk = Likelihood * Impact

Risk score can be 0 - 81

Overall Risk Severity

Impact	HIGH	Medium (>=18)	High (>=36)	Critical (>=54)
	MEDIUM	Low (>=9)	Medium (>=18)	High (>=36)
	LOW	Note (< 9)	Low (>=9)	Medium (>=18)
		LOW	MEDIUM	HIGH
	Likelihood			

Criteria + Method

Risk Acceptance Criteria

Acceptance Level	OWASP Score	CRA Treatment Requirement
Negligible / Note	**0 – 9**	Risks are documented but typically accepted as they represent a negligible threat to the product context
Low **Acceptable with Review**	**10 – 17**	Residual risk is communicated to the user. Standard for non-critical consumer products.
Medium | Unacceptable	**18 – 35**	Requires "appropriate risk treatment" according to your provided guidelines to reduce the score before launch.
High | Unacceptable	**36 – 53**	Unacceptable under CRA standards; mandatory mitigation using "state of the art" controls is required.
Critical | Unacceptable	**54 – 81**	Represents high-profile violations or direct life-safety concerns; the product generally cannot be released in this state.

Criteria + Method

Risk Acceptance Criteria - Special Cases

1. **Health & Safety** Impact = 9 → Unacceptable
2. **Attack Scalability** Impact = 9 → Unacceptable
3. **User Profile (Vulnerable Users/Child)** Impact = 9

   → You **cannot** treat the impact, you need to significantly lower the likelihood
4. **Critical Infrastructure** Impact = 9

   → You **cannot** treat the impact, you need to significantly lower the likelihood
5. **Awareness** Likelihood = 9 → **Public known exploitable vulnerability** → **Violates CRA requirements Annex I** ⇒ Mitigate

Risk Assessment

Risk Assessment

Asset and Cybersecurity Objective Identification

1. **Input:** Product context
2. **Steps:**
   a. **Identify all Assets:** (PII, keys, hardware components, interfaces, configuration, communication)
   b. **Identify Cybersecurity Objectives** for each asset: **CIAPS**
3. **Result:** List of Assets with related cyber security objectives:

Asset Category	Specific Asset Example	Primary Cybersecurity Objective
Data Assets	Authentication Tokens / Keys	**Confidentiality:** Prevent unauthorized access to sensitive credentials.
Functions	Product configuration	**Integrity:** Ensure only authorized modification of system settings
User Safety	Home Assistant connected Smart Lock	**Safety:** Lock can be unlocked during power Failure or fire to allow escape

Risk Assessment

Threat Identification

1. **Input:** List of Assets with related cybersecurity objectives
2. **Steps:**
   a. **Identify Threat Agents & Events**
   b. **Identify Attack Vectors & Failure Modes**
   c. **Map Threats to Assets**
3. **Result:** List of identified threats and failure events.

Asset Category	Specific Asset Example	Potential Threat Example
Data Assets	Authentication Tokens / Keys	**External Attacker:** Remote extraction of credentials via an unauthenticated API vulnerability
Functions	Product configuration	**Malicious Insider:** Unauthorized modification of system settings via local maintenance port
User Safety	Home Assistant connected Smart Lock	**Power Failure:** Sudden loss of energy causing lock mechanism not to unlock during fire emergency

Risk Assessment

Risk Estimation

1. **Input:** List of identified threats and failure events
2. **Steps:**
   a. **Estimate Likelihood and Impact, take MAX()**
   b. **Calculate Total Risk:** Likelihood (L) × Impact (I)
3. **Result:** Prioritized Risk Register with inherent risk scores for every identified threat

Threat / Event	**Likelihood (L)**	**Impact (I)**	**Inherent Risk (L×I)**
External Attacker: Remote API exploit (Mass Scale)	6 (High)	**9 (Scalability)**	**54 (Critical)**
Power Failure: Loss of unlock functionality	2 (Low)	**9 (Safety)**	**18 (Medium)**
Malicious Insider: Local system settings change	3 (Low)	5 (Medium)	**15 (Low)**

Risk Assessment

Risk Evaluation

1. **Input:** List of identified threats / failure events with inherent risk score
2. **Steps:**
   a. **Risk Acceptance Criteria**
   b. **Applicability of EU CRA Annex I requirements**
   c. **Document justification for accepted residual risks**
3. **Result:** List of identified threats and the treatment decision

Threat / Event	Inherent Risk (LxI)	Treatment
External Attacker: Remote API exploit (Mass Scale)	**6x9 = 54 (Critical)**	**Mitigate Likelihood + Impact**
Power Failure: Loss of unlock functionality	**2x9= 18 (Medium)**	**Mitigate Likelihood**
Malicious Insider: Local system settings change	**3x5 = 15 (Low)**	**Accept**

CRA Requirements Applicability

Risk Assessment

Now you know why you need a risk assessment

Example - Annex I Part 1 (j)

“be designed, developed and produced to limit attack surfaces, including external interfaces”

Does now every product need to protect against any physical local attacks?

What does your risk register say?

Risk Assessment

Evaluate EU CRA Annex I Applicability

Threat / Event	Inherent Risk (LxI)	Annex I Requirement	Applicable? Necessary?
External Attacker: Remote API exploit (Mass Scale)	**6x9 = 54 (Critical)**	(d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access (e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means (j) be designed, developed and produced to limit attack surfaces, including external interfaces (l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user	Yes Yes
Power Failure: Loss of unlock functionality	**2x9= 18 (Medium)**	(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks	Yes Yes
Malicious Insider: Local system settings change via local maintenance port	**3x5 = 15 (Low)**	(f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions (j) be designed, developed and produced to limit attack surfaces, including external interfaces	Yes No

Risk treatment

Risk Treatment

Treatment follows priority

Implement
CRA Annex I Requirements

1. **Avoid:** Don’t implement it this way. (eg. Hardware vs Software control loops)
2. **Mitigate:** Implement measures to reduce likelihood and/or impact
3. **Accept:** Inherent risk of the product that cannot be mitigated
4. **Transfer:** Transfers the risk to the user.
    a. **Officially via the User Instructions**

    Annex ANNEX II INFORMATION AND INSTRUCTIONS TO THE USER ”any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks”

Risk Treatment

Residual Risk Score

1. **Input:** List of identified threats / failure events with treatment decision
2. **Steps:**
   a. **Document risk treatment as evidence**
   b. **Repeat estimation of risk score to get residual risk**
3. **Result:** List of risks with treatment and residual risk score

Threat / Event	Inherent Risk (LxI)	Treatment	Residual Risk (L×I)
External Attacker: Remote API exploit (Mass Scale)	**6x9 = 54 (Critical)**	**Mitigate Likelihood + Impact**	**2 x 6 = 12 (Low)**
Power Failure: Loss of unlock functionality	**2x9= 18 (Medium)**	**Mitigate Likelihood**	**1 x 9 = 9 (Low)**
Malicious Insider: Local system settings change	**3x5 = 15 (Low)**	**Accept**	**15 (Low)**

Risk communication

Communication

Clearly communicate Risks to users of the product

1. **Speak the User's Language:** Use simple, non-technical terminology and accessible formats (like multi-modal or written) that match the stakeholder's specific needs.
2. **Be Honest About Residual Risks:** Clearly describe any remaining risks and the specific circumstances or contexts that could lead to a security issue.
3. **Give Clear "How-To" Instructions:** Provide actionable steps for safe onboarding, integration, and daily operation to help the user mitigate known threats.
4. **Put it in the Manual:** Ensure all risk treatment information and expectations for the user are officially included in the product's "Instructions for Use".

Risk monitoring and review

Learn to live with it!

1. **Prepare for lifelong risk management**
   a. Risk management needs to be applied over the support period. For some products this will be not 5 but 10-15 years (PLCs, IoT, Routers, …)
2. **Define review intervals**
3. **Define sources to find new vulnerabilities or threats that are applicable to your product**
4. **Update your risk register based on this information**
5. **Communicate new risks that are transferred to the user of the product**

Review + Monitor

Documents you should have in the end

1. **Product Context**
    a. Architecture, Design, Dependencies, User profile, purpose, …
2. **Acceptance Criteria + Risk Methodology**
    a. Risk Rating + Acceptance of risk
3. Documented **Risk Assessment** in a **Risk Register**
    a. **All Identified risks**: **inherent risk**, **treatment decision**, **residual risk**
4. **Risk Treatment Evidence** and mapping to **Risk Register**
    a. Pentests, Designs, PRs, …
5. **Essential Cybersecurity Requirements** Mapping to **Risk Register**
    a. Justification why a requirements does not need to be implemented based on the linked risks
6. **Review, Monitoring and Communication Plan** plus **Monitoring Evidence**
    a. Sources (CVE DBs), Vulnerability Scanners, Review Meeting recordings

Documentation

WAIT! I'VE SPENT MORE TIME DOCUMENTING
THE RISK THAN I DID CREATING IT

Thanks!

Harald Fischer

Security Aspect Lead @ balena

(ISO 27k[1/2/5], CRA, Cyber Compliance)

sometimes still Backend Software Engineer

harald@balena.io

Harald Fischer on Linkedin

@fisehara on github

🇩🇪 living in The Hague 🇳🇱