Meeting EU CRA Obligations: A Practical Guide to Cybersecurity Risk Assessment

Harald Fischer
Security Aspect Lead @ balena

Who needs a Cybersecurity Risk Assessment?

Every manufacturer of products with digital elements, including software only products, placed on the EU market needs to conform with the EU Cyber Resilience Act.

Every manufacturer needs to perform and maintain a cybersecurity risk assessment for their product to demonstrate conformity with essential cybersecurity requirements from EU CRA Annex I

What is a risk assessment anyway?

Risk assessment is the core process driving a risk-based decision approach.

Its primary function is to enable and demonstrate informed decision-making based on risks, directly guiding product and service preparation for market resilience, resistance to potential attacks, and prevention of supply chain fraud.

Benefits of Risk Assessment

- **Informed Decision-Making**
- **Demonstrable Due Diligence**
- **Robust Innovation**
- **Increased Confidence & Accountability**
- **Market Access & Trust**

The Principle of Risk Management is Not New in EU Legislation

EU CRA - …manufacturers shall undertake an assessment of the cybersecurity risks associated with a product… Article 13

EU AI Act - A **risk management system** shall be established, implemented, documented and maintained in relation to high-risk AI systems. Article 9

Medical Device Regulation - Manufacturers shall establish, document, implement and maintain a system for **risk management. Risk management** … continuous iterative process throughout the entire lifecycle of a device, requiring regular systematic updating. MDR Annex I

Machinery Directive - The manufacturer of machinery … must ensure that a **risk assessment** is carried out in order to determine the health and safety requirements which apply to the machinery. The machinery must then be designed and constructed taking into account the results of the **risk assessment**. Annex I

Do I have to invent risk assessment?

Existing standards for the rescue!

Guides and Standards for Risk Management

- ISO 31000:2018 - Risk management — Guidelines
- **ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks**
- ISO 14971:2019 - Medical devices — Application of risk management to medical devices
- ANSI/ISA-62443-3-2-2020 - Security for Industrial Automation and Control Systems – Part 3-2: Security Risk Assessment for System Design
- ISO/IEC 23894:2023 - Information technology — Artificial intelligence — Guidance on risk management
- **NIST SP 800-30 Rev. 1 - Guide for Conducting Risk Assessments**
- NIST SP 800-37 Rev. 2 - Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy

What's about the Cybersecurity Risk Assessment Standard for Products with Digital Elements?

ENISA – Risk Management Standards – March 2022

Recommendation 3:

- When there isn't an appropriate risk management tool for a **specific sector**, the EU should ask for one to be made, using ISO 27005 and ISO 31000 as the starting points

Recommendation 9:

- ESO(European Standardisation Organisations)s should adopt ISO 31000 and ISO 27005 as European Norms.

Recommendation 10:

- ETSI (European Telecommunications Standards Institute) should harmonise its TS 102 165-1 with ISO 31000 and ISO 27005

Experts (ENISA) state
ISO 27005 & ETSI TS 102 165-1
as the closest, most relevant guidance today

Risk Assessment Candidates

ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Guidance on **managing** information security risks

- Provides the overall framework for managing information security risks.

ETSI TS 102 165-1 V5.3.1 - Technical Specification - Cyber Security (CYBER); Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)

- Offers a specific methodology (TVRA) for product-focused threat and vulnerability analysis.

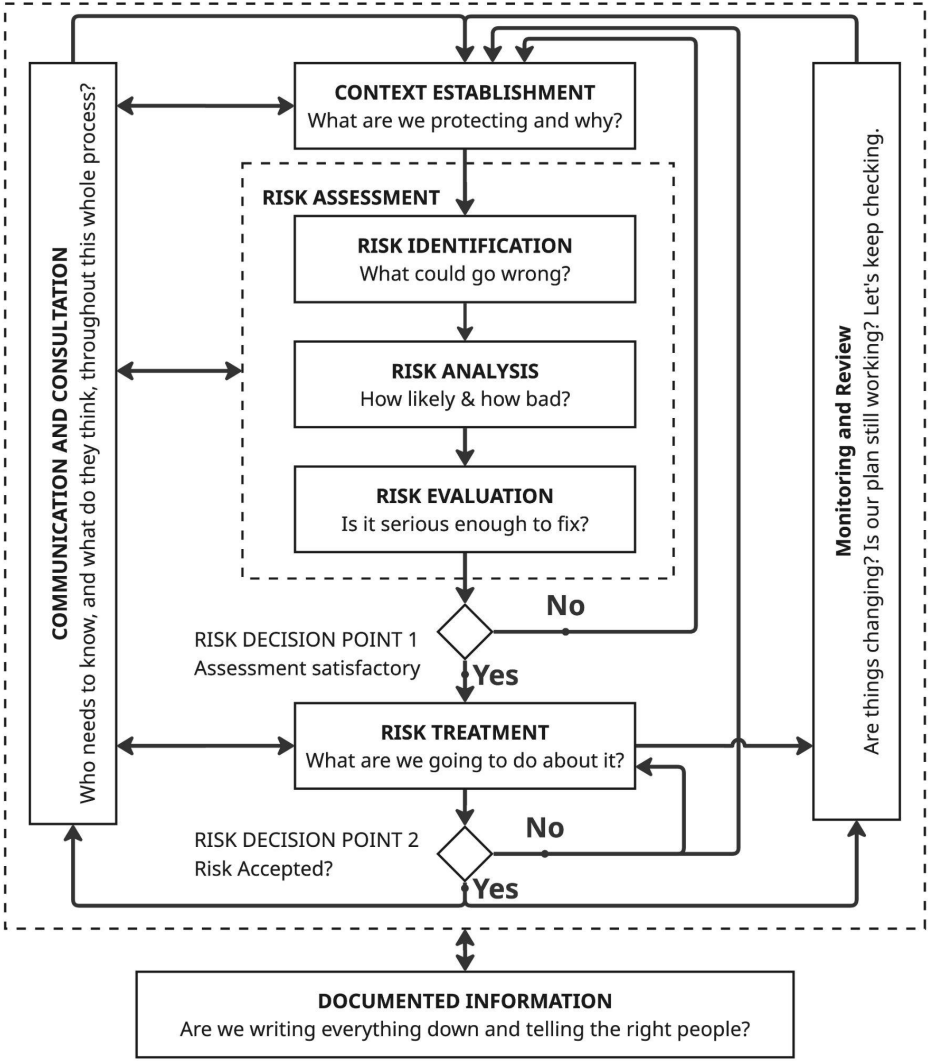
What do I need to learn:
Risk Management or Risk Assessment?

ISOs
Risk Assessment in Information Security

ISO 27005:2022

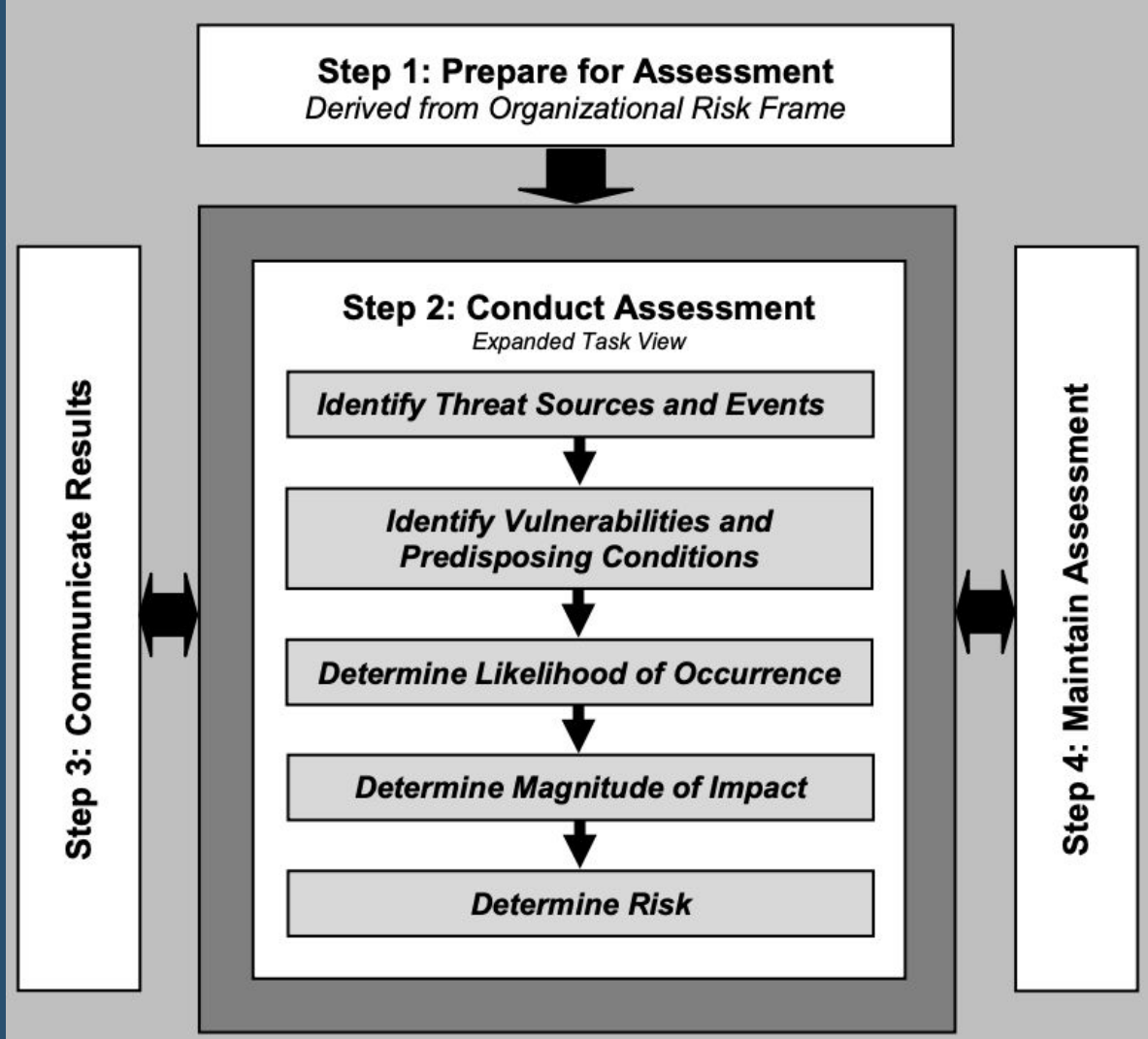
ISOs
Information security risk management process

ISO 27005:2022



NISTs Risk Assessment in Information Security

NIST 800-30 Rev 1.



Let us map the ISO 27005 with the EU Cyber Resilience Act

Article 13(2) - Obligations of manufacturers

For the purpose of complying with paragraph 1, **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**.

⇒ **Risk Assessment**

Article 13(3) - Obligations of manufacturers

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**.

⇒ **Context Establishment**

Article 13(7) - Obligations of manufacturers

The manufacturers shall **systematically document**, in a manner that is proportionate to the nature and the cybersecurity risks, relevant **cybersecurity aspects** concerning the products with digital elements, including **vulnerabilities** of which they **become aware** and any relevant information provided by **third parties**, and **shall**, **where applicable**, **update** the **cybersecurity risk assessment** of the products.

⇒ Communication and Consultation

⇒ Monitor and Review

ANNEX I - ESSENTIAL CYBERSECURITY REQUIREMENTS

(2) On the basis of the **cybersecurity risk assessment** referred to in Article 13(2) and where applicable, products with digital elements **shall:**

(a) be made available on the market without known exploitable vulnerabilities;

(b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;

…

⇒ **Risk Treatment**

ANNEX VII - CONTENT OF THE TECHNICAL DOCUMENTATION

The technical documentation referred to in Article 31 shall contain at least the following information, as applicable to the relevant product with digital elements:

...

3. an **assessment** of the **cybersecurity risks** against which the product with digital elements is **designed**, **developed**, **produced**, **delivered** and **maintained** pursuant to Article 13, including how the **essential cybersecurity requirements** set out in Part I of Annex I are **applicable**;

⇒ **Documented Information**

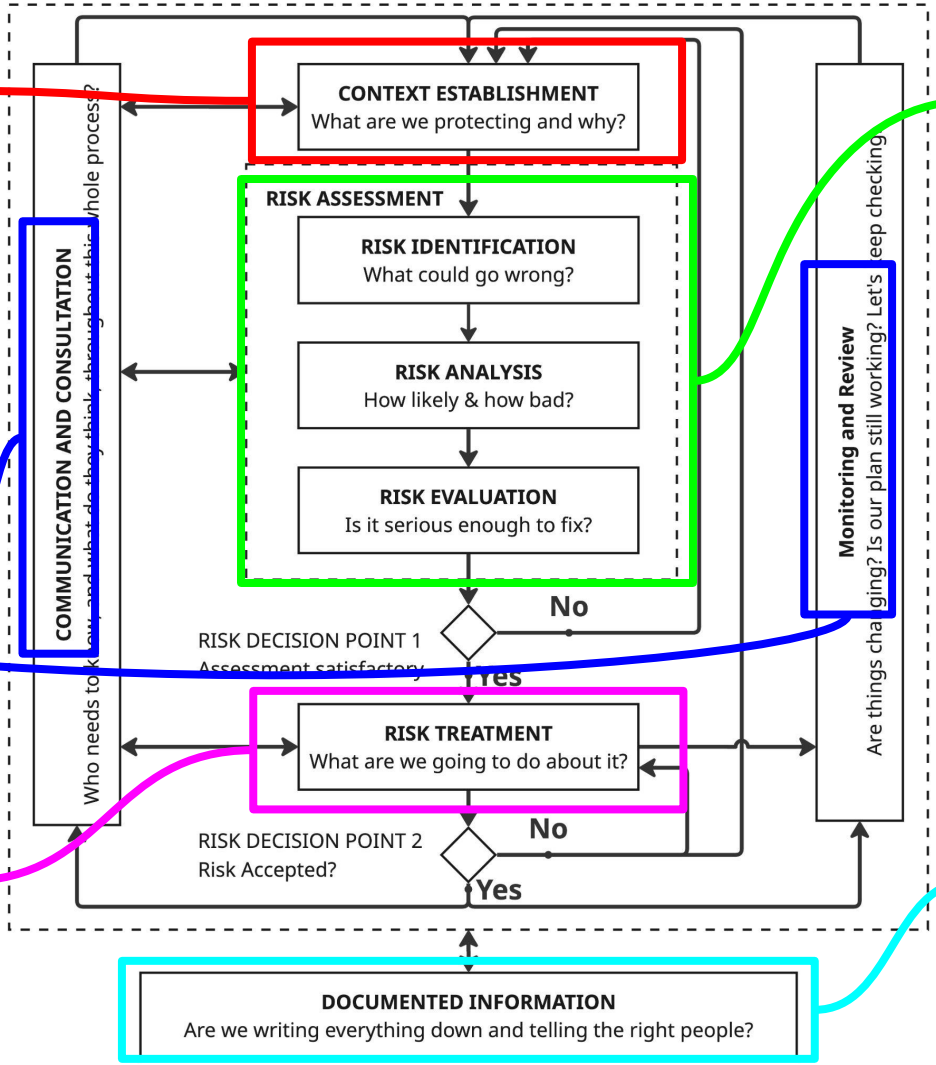
EU CRA Art. 13(3)

EU CRA Art. 13(2)

EU CRA Art. 13(7)

EU CRA Annex I

EU CRA Annex VII



The ISO 27005 Risk Management maps the requirements, but needs to be executed for products and not for services or organisations.

So what do I need to do?

Let’s get inspired by standards and understand the necessary steps.

- **ISO 27005:2022** is about information security risk management not product security or safety
- **ETSI TS 102 165-1** is a technical specification guiding the assessment for product security
- **ETSI EN 303 645 V3.1.3** - References 27005 but doesn’t define a risk management process

#1: Establish Context - Know Your Product & Its World

- What is the product's exact intended purpose and functionality?
- Who are the users, and how are they expected to use it?
- Any foreseeable misuse?
- What is the operational environment?
- What are the critical assets we need to protect?
- What is the product's expected operational lifetime and support period?
- What are our risk acceptance criteria, appetite and tolerance?

Output: Definition of Risk Assessment Context

#2: Risk Identification - What’s in Your Product

- **Initial risk identification should consider vulnerabilities before current mitigations are applied**
- What are the product's components?
- What are its interfaces?
- What known vulnerabilities exist(ed) in similar technologies?
- Is it a threat actor or system involved in the vulnerability?
- How to aggregate, overlap and specifically separate risks?

Output: List of identified inherent unmodified risks ⇒ Risk Register

#3: Risk Analysis - What can happen to your product?

For each identified risk scenario

- How likely is this to occur?
  - Consider threat actor capability/motivation, Vulnerability exploitability
- What would be the impact if it did occur?
  - Consider impact on confidentiality, integrity, availability, safety, financial, …
- Define **risk level** (likelihood + impact score)

Output: A list of risks with level values assigned

5x5 Heatmap of Risk Levels

Likelihood	Consequence				
	Catastrophic (5)	Critical (4)	Serious (3)	Significant (2)	Minor (1)
Almost certain (5)	Very High (25)	Very High (20)	High (15)	High (10)	Medium (5)
Very likely (4)	Very High (20)	High (16)	High (12)	Medium (8)	Low (4)
Likely (3)	High (15)	High (12)	Medium (9)	Medium (6)	Low (3)
Rather unlikely (2)	High (10)	Medium (8)	Medium (6)	Low (4)	Very Low (2)
Unlikely (1)	Medium (5)	Low (4)	Low (3)	Very Low (2)	Very Low (1)
Consequence x Likelihood	Very High (20-25)	High (10-16)	Medium (5-9)	Low (3-4)	Very Low (1-2)

#4: Risk Evaluation - How risky is your product now

For each identified and analyzed risk in risk register

- Compare each risk level against our pre-defined risk acceptance criteria.
- Is this risk acceptable as-is, or does it require treatment?
- Prioritize the unacceptable risks for treatment.

Output: A list of actions regarding the management of all identified risks

#5: Risk Treatment - How risky will your product be

For each unacceptable risk, what are our options?

- **Treat:** Implement security controls ⇒ **Primary goal for CRA.**
- **Terminate:** Change plans to eliminate the risk
- **Transfer:** Less common for product CRA - even possible?
- **Tolerate:** Only if the residual risk is within acceptable criteria. You can't just accept a high risk because it's expensive to fix if it violates essential CRA requirements.

Output: List of Risk Treatment & List of Applicability of Essential Cybersecurity Requirements from EU CRA Annex I

Risk Management - Maintain your product risks

Ongoing Step: Recording & Reporting (Documentation)

- Document every step: context, identified risks, analysis, evaluation, treatment decisions, and residual risks.

Ongoing Step: Monitor & Review

- How will we monitor for new vulnerabilities in our product post-launch?
- How often will we review and update the risk register?

Ongoing Step: Communication & Consultation

- How will we communicate risk information and updates to stakeholders?

What should I remember from all of this?

- **Start Fresh:** Initial risk identification should consider vulnerabilities before current mitigations are applied (to understand inherent risk).
- **Living Document:** Risk assessment is a continuous lifecycle activity, not a one-off checkbox. Update it!
- **Data-Informed (Eventually):** Aim to gather data to refine likelihood estimations over time. Start with qualitative, move towards quantitative where feasible.

- **Compliance & Safety First:** Cost is a factor in treatment, but risks leading to non-compliance with CRA essential requirements or unacceptable safety impacts generally cannot be 'accepted' without mitigation.
- **Beyond Data:** Consider Health & Safety: Explicitly assess risks that could impact user health and safety, not just data breaches.
- **Standards:** There is no single standard yet existing, but ISO 27005 is a strong candidate, either becoming harmonised or used as source for a harmonized new standard.

Thanks!

Harald Fischer

Security Aspect Lead @ balena

(ISO 2700[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 🇳🇱