

Introduction to the MDR and the European Regulatory Landscape for Medical Device Software

Stef Rommes - VITO



Regulatory Landscape

Regulatory Landscape – Vertical & Horizontal

Medical
Device
Regulation

In Vitro
Diagnostic
Regulation

AI Act

Cyber
Security Act

~~Cyber
Resilience
Act~~

European
Health Data
Space

GDPR

Data Act /
NIS2 / ...

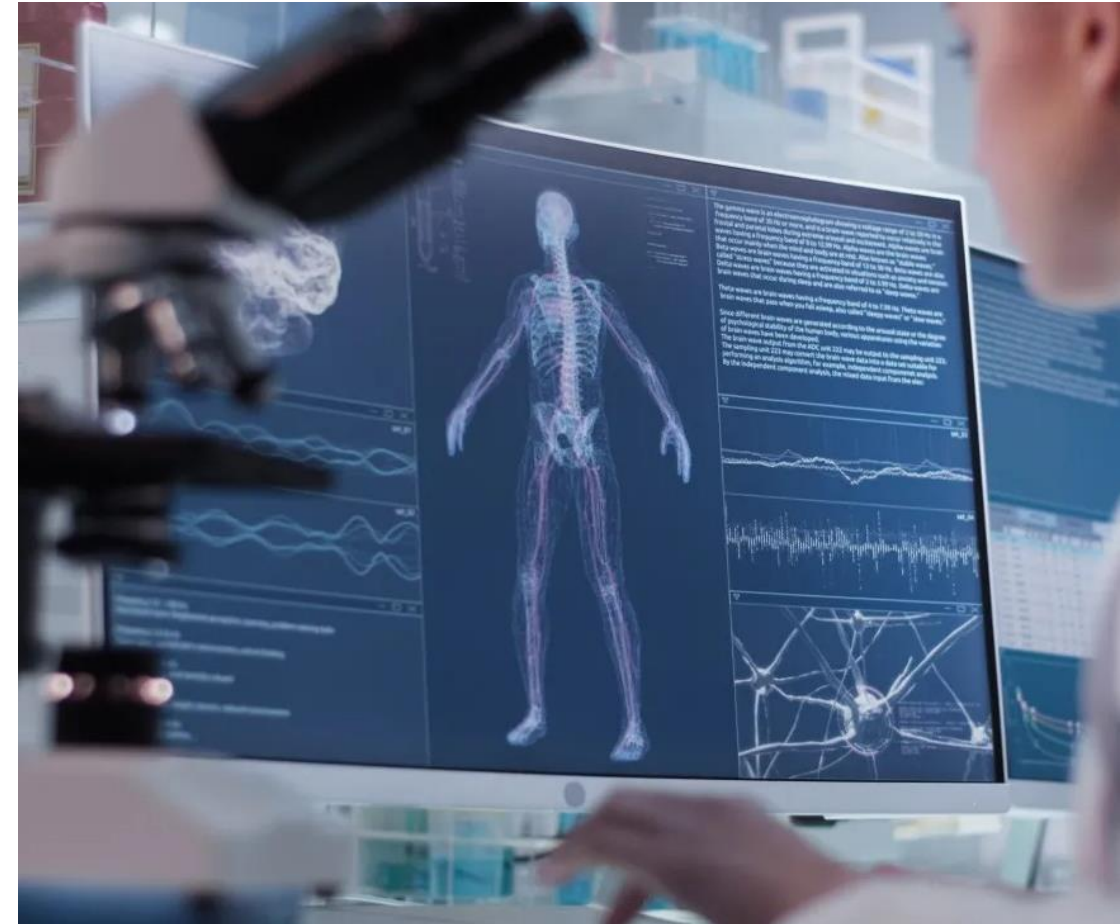


Medical Device Regulation

Medical Device Regulation (MDR)

- Medical Device Directive
→ Medical Device Regulation
- PIP breast implant scandal
/ Increasing device complexity
- Defines requirements for placing medical devices on the market
 - Also covers in-house developed devices
- Covers the entire life cycle, including design, development, certification, and post-market

Its purpose is to ensure medical devices are **safe, effective, and properly controlled throughout their life cycle.**





Actors

Actors & Pathway to Device

- **Regulators:**
Set rules, guidance, and policy frameworks
- **Notified Bodies:**
Conformity assessment, certification and ongoing audits
- **Competent Authorities:**
Market surveillance, vigilance, enforcement, NB designation, ...
- **Manufacturers:**
Manufacture devices according to MDR requirements
 - Commercial → CE marking
 - Health institutions → MDR 5(5) or CE marking
- **Hospitals**
- **Patients**





CE Marking

CE Marking

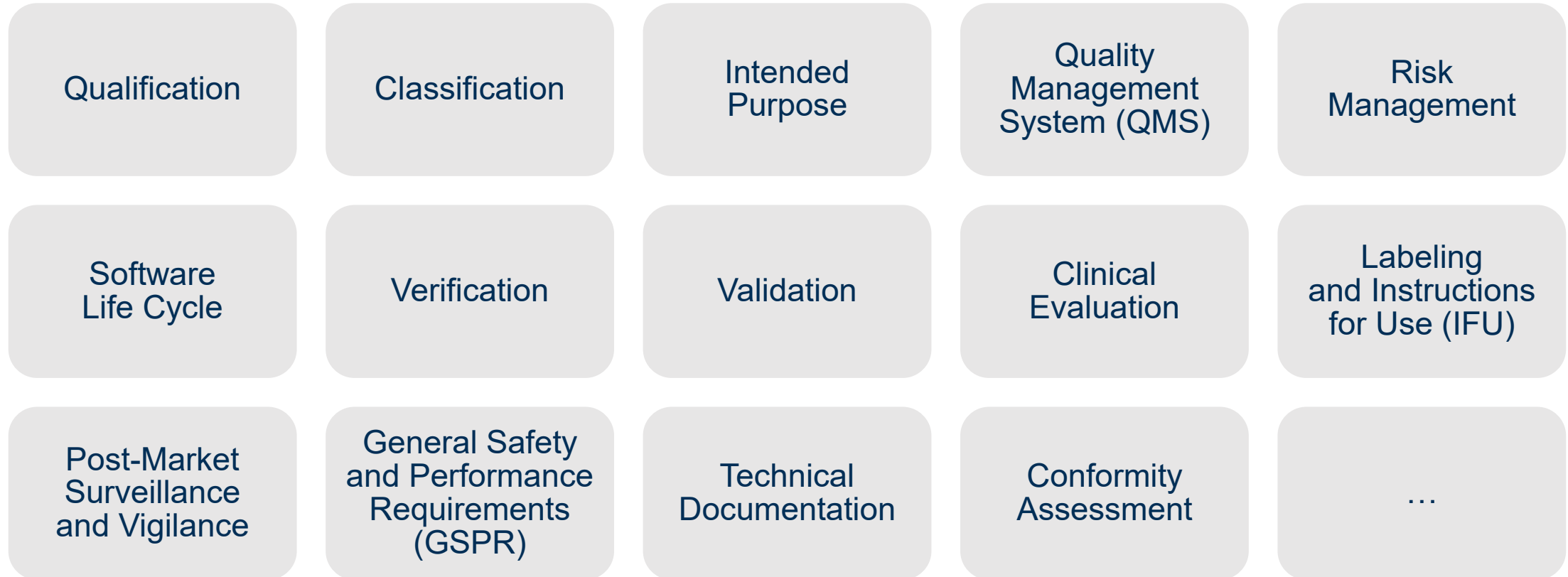
- Certification that a device **complies** with the applicable regulations
- **MDR** / **IVDR** / **AI Act** / **EHDS**
- Safe and performs as intended
- Market authorization
- Notified body involvement for conformity assessment
 - Quality Management System
 - Technical Documentation





Compliance

Steps in the Pathway to CE Marking





'In-House' Devices

Article 5(5)

With the exception of the relevant **general safety and performance requirements** set out in Annex I, the requirements of this Regulation shall not apply to devices, manufactured and used only within health institutions established in the Union, provided that all of the following conditions are met:

- No CE marking
- No conformity assessment
- No notified body
- ...
- Still needs to ensure medical devices are **safe, effective, and properly controlled throughout their lifecycle.**

Article 5(5)

- ...
- (b) manufacture and use of the devices occur under appropriate **quality management systems**,
- ...
- (f) the health institution draws up **documentation** that makes it possible to have an understanding of the manufacturing facility, **the manufacturing process, the design and performance data of the devices, including the intended purpose**, and that is sufficiently detailed to enable the competent authority to ascertain that the general safety and performance requirements set out in Annex I to this Regulation are met;
- ...
- (h) the health institution **reviews experience** gained from clinical use of the devices and takes all necessary corrective actions.
- ...

General Safety and Performance Requirements (GSPR)

Highlights

Manufacturers shall establish, implement, document and maintain a **risk management system**. Risk management shall be understood as a continuous iterative process throughout the **entire lifecycle** of a device, requiring regular systematic updating.

For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of **development life cycle, risk management, including information security, verification and validation**.

Evidence



Article 5(3) - Demonstration of conformity with the general safety and performance requirements shall include a **clinical evaluation** in accordance with Article 61.

Highlights

Intended
Purpose

Quality
Management
System (QMS)

Risk
Management

(Software)
Development
Life Cycle

Information
Security

Verification

Validation

Clinical
Evaluation



How

How?

- **Harmonized standards:**

- Gold standard – presumption of conformity
- ISO 13485: Medical devices – Quality management systems – Requirements for regulatory purposes
- ISO 14971: Medical devices – Application of risk management to medical devices
- IEC 62304: Medical device software – Software life cycle processes
 - Verification
- IEC 62366-1: Application of usability engineering to medical devices
 - Validation

- **Be inspired by MDR**

- Clinical evaluation, ...



**Intended
Purpose**

Intended Use/Purpose

Intended
Purpose/Use

Indications

Contra-
Indications

Warnings

Patient Target
Group

Intended User

Intended Use
Environment

Performance
Characteristics

Intended Use/Purpose

Example

The manufacturer of an AIAMD product for detecting diabetic retinopathy is generating their intended purpose statement. They state that their product is for “monitoring disease progression in patients with diabetes to alert users when to be referred for treatment”.

This statement should be augmented by additional detailed information:

- “patients with diabetes” is a **broad cohort** for an intended use population. The data used to train the AI algorithm was exclusively from patients with Type 2 diabetes between the ages of 40 and 70 years old and was not demonstrated to generalise beyond this range. Therefore, it should be specified as such within the intended purpose statement. People with type 1 diabetes should also be contraindicated in this case. Additionally, the product may only be suitable for early stages of disease progression, and this should also be specified.
- Both the **users and the environment** should be specified with further detail in the intended purpose statement. The manufacturer should include information on these factors. For example, software is for use in the community by appropriately trained optometrists for referral to specialist care, is a different situation than use within a specialist hospital department by a consultant optometrist for determining treatment decisions. The equipment used, training, and experience expectations on the users will require different evidence based on the use case and without explicit evidence it cannot be assumed that such evidence will generalise even to other parts of the same patient pathway.

An example expanded statement could be:

Optometrists who are trained in the use of the SuperEyeScan9000 software can use the system to assist in the identification of stage 1 diabetic retinopathy in adults between 40 and 70 years old with confirmed type 2 diabetes. The SuperEyeScan9000 software package is suitable for use with Scantastic scanners utilising running operating systems 2.0 or 3.0 and achieves a minimum performance of 97% sensitivity and 88% specificity



Quality Management

Quality Management System

- ISO 13485: Quality Management Systems
- Standard Operating Procedures (SOPs)
 - Not just from ISO 13485
 - Also based on IEC 62304/ISO 14971/MDR
- Other documents
- Certification

SOPs

- Document and record control
- **Design and Development**
- **Software Verification and Validation**
- **Usability Engineering**
- **Risk Management**
- **Clinical Evaluation**
- **Nonconformance and Corrective Actions**
- **Post-market Surveillance**
- Complaints
- Training and Competence
- Vigilance and Reporting
- Change Control
- Software Maintenance and Update
- Configuration Management
- Traceability
- ...



Risk Management

Risk Management

- **GSPR:** “The requirement in this Annex to reduce risks as far as possible means the reduction of risks as far as possible without adversely affecting the benefit-risk ratio.”
- **ISO 14971** - Application of risk management to medical devices
- Link to **IEC 62304**
- Failure Mode and Effect Analysis (**FMEA**)

		Inherent Risk Ranking				
Likelihood	Imminent 5	Low	Moderate	High	Critical	Critical
	Frequent 4	Low	Moderate	High	High	Critical
	Occasional 3	Very Low	Low	Moderate	High	High
	Infrequent 2	Very Low	Very Low	Low	Moderate	Moderate
	Rare 1	Very Low	Very Low	Low	Low	Moderate
		1 Very Low	2 Low	3 Moderate	4 High	5 Critical
		Impact				

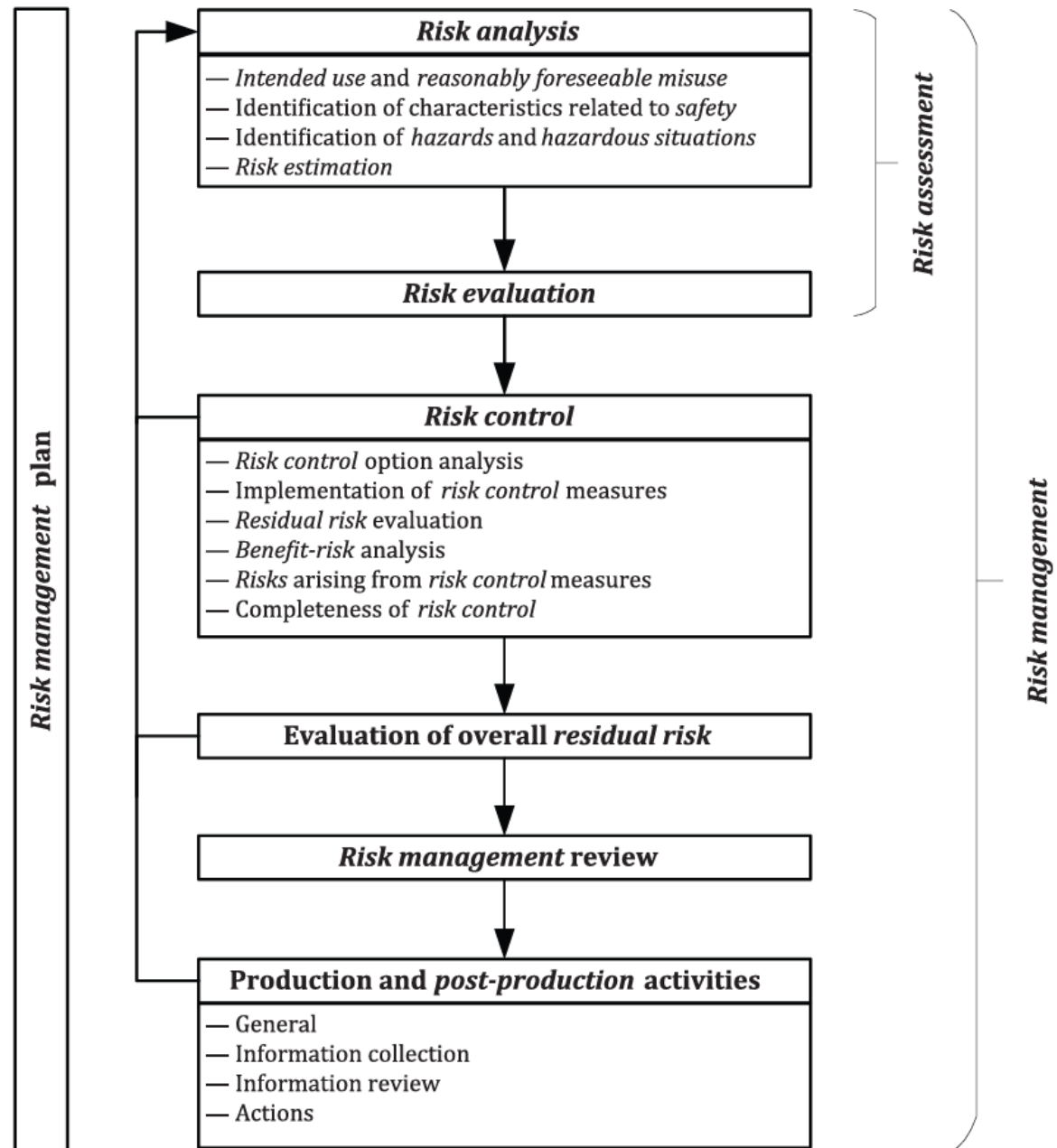
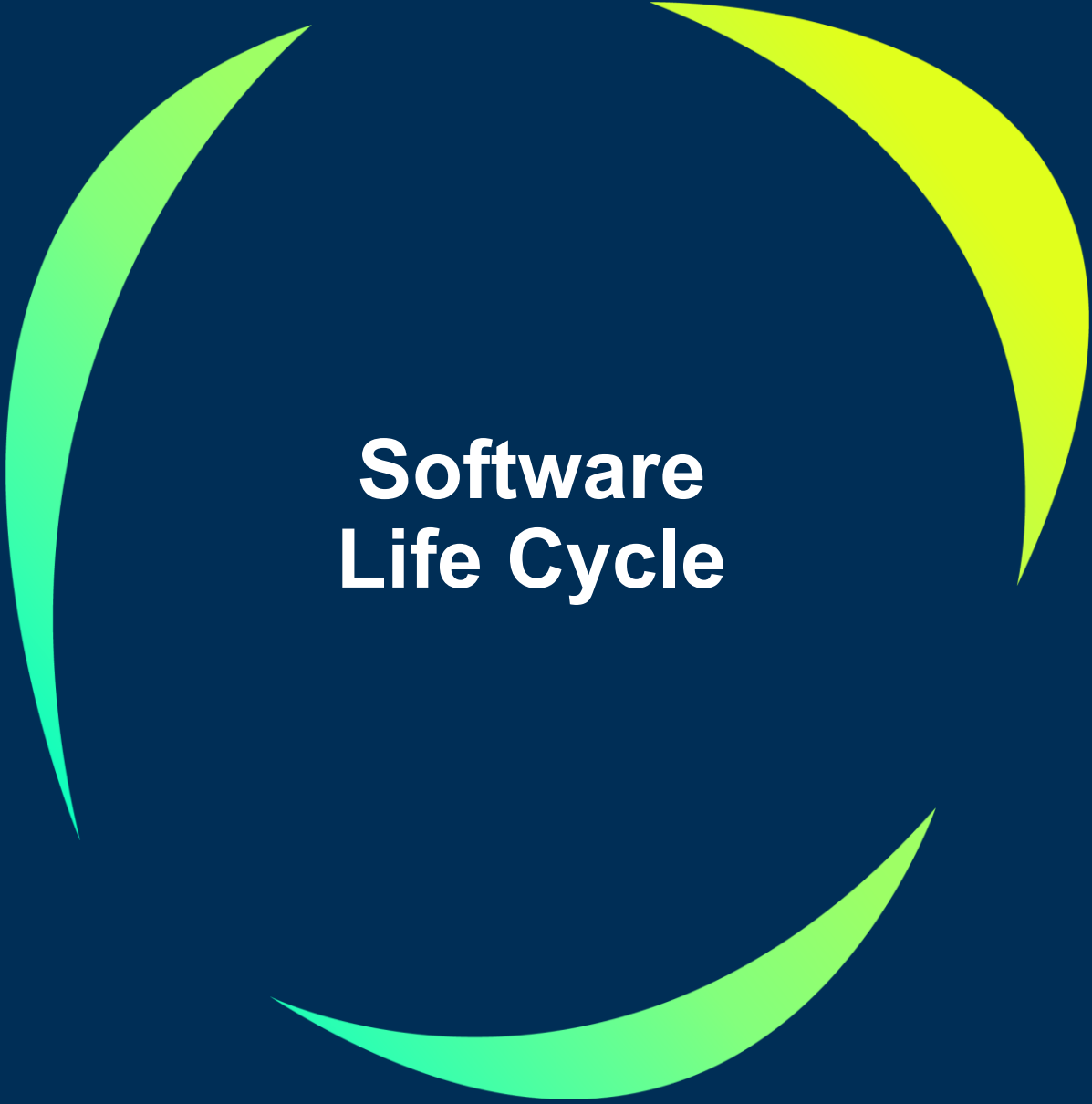


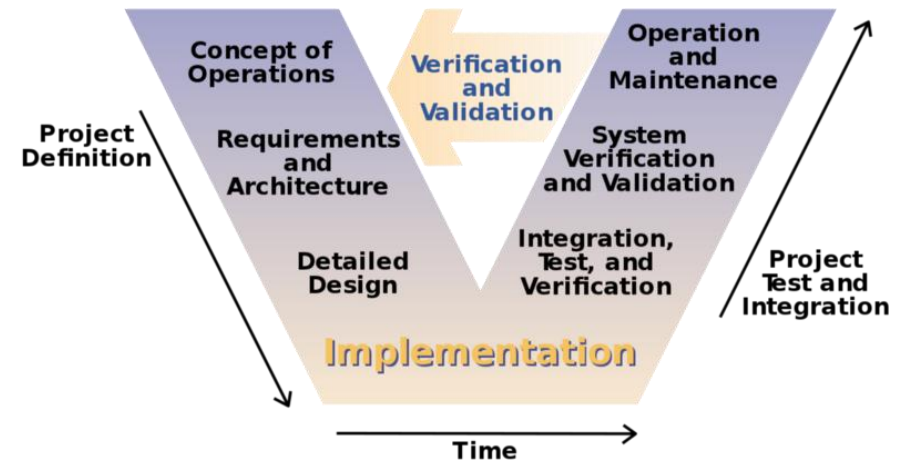
Figure 1 — A schematic representation of the *risk management process*



Software Life Cycle

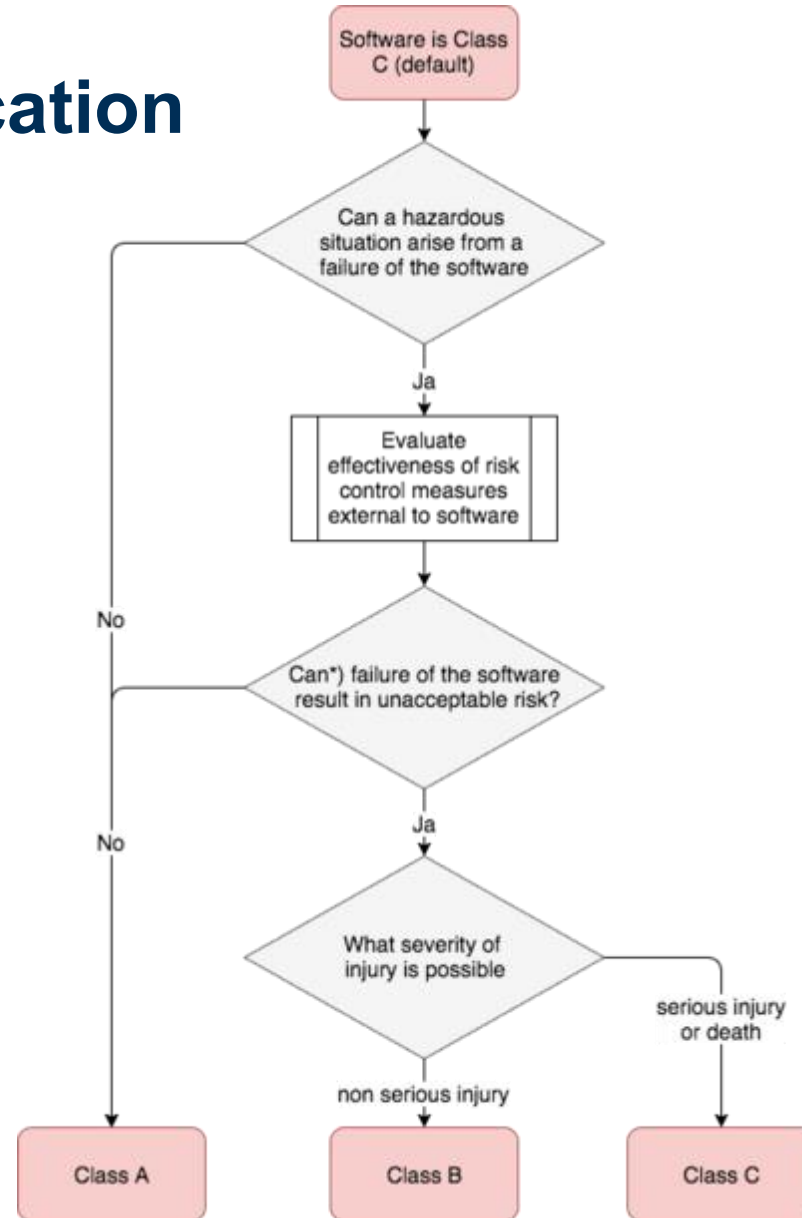
Software Life Cycle

- Best achieved through **IEC 62304 / IEC 82304**
 - IEC82304 Health Software
 - IEC62304 Medical device software life cycle processes
- **SOPs:**
 - Design and Development
 - Planning & Requirements
 - Software **Verification and Validation**
 - Usability Engineering (IEC 62366-1)
 - Maintenance
 - ...
- Can be **Waterfall / Agile / Other**
- **How elaborate** should documentation be?



<https://medium.com/merantix/certifying-a-medical-device-as-a-startup-part-2-v-model-doesnt-mean-waterfall-development-41a927480278>

Software Safety Classification

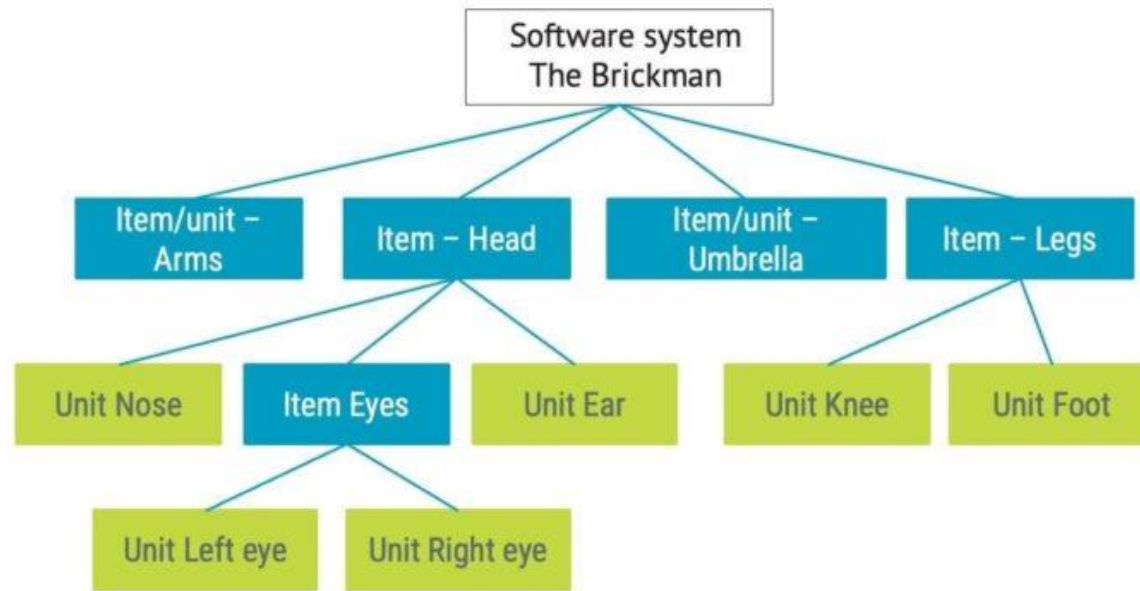


Sub-Division

A, B, C travels up!

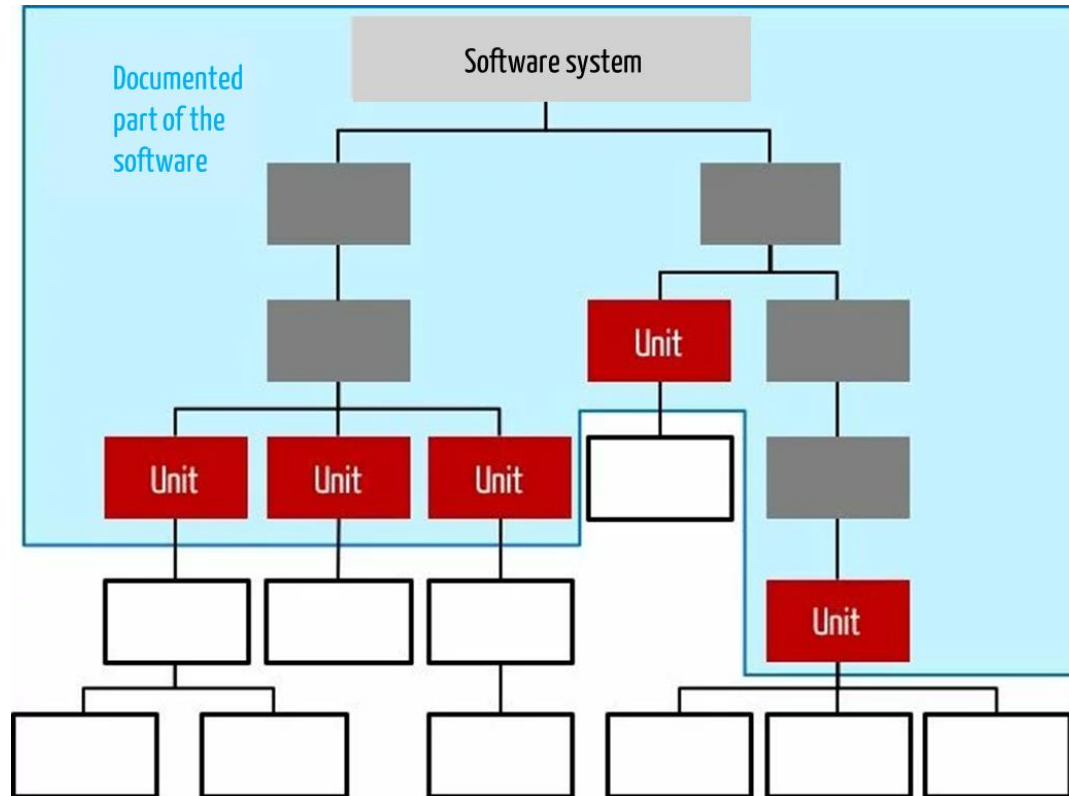


Software system, item, and unit



medicaldeviceHQ

Software Safety Classification





Verification and Validation

Software Verification and Validation

IEC 82304 Health software - General requirements for product safety

- Helps understand software (product) is safe, secure for its intended use

IEC 62304 Medical device software - Software life cycle processes

- Helps understand that software works/was built correctly

IEC 62366 Usability Engineering

IEC 81001-5-1 (Cyber) Security


Verification: 'Did we build the software right?'

Validation: 'Did we build the right software for its intended use?'

Software Verification and Validation of AI systems

- How should AI systems be verified and validated?
- **No explicit guidance** in MDR / IEC 62304 / IEC 82304
 - No reason not to follow IEC 62304/IEC 82304 process
 - New version of IEC 62304 in the making!
- Some new ISO standards and many under development



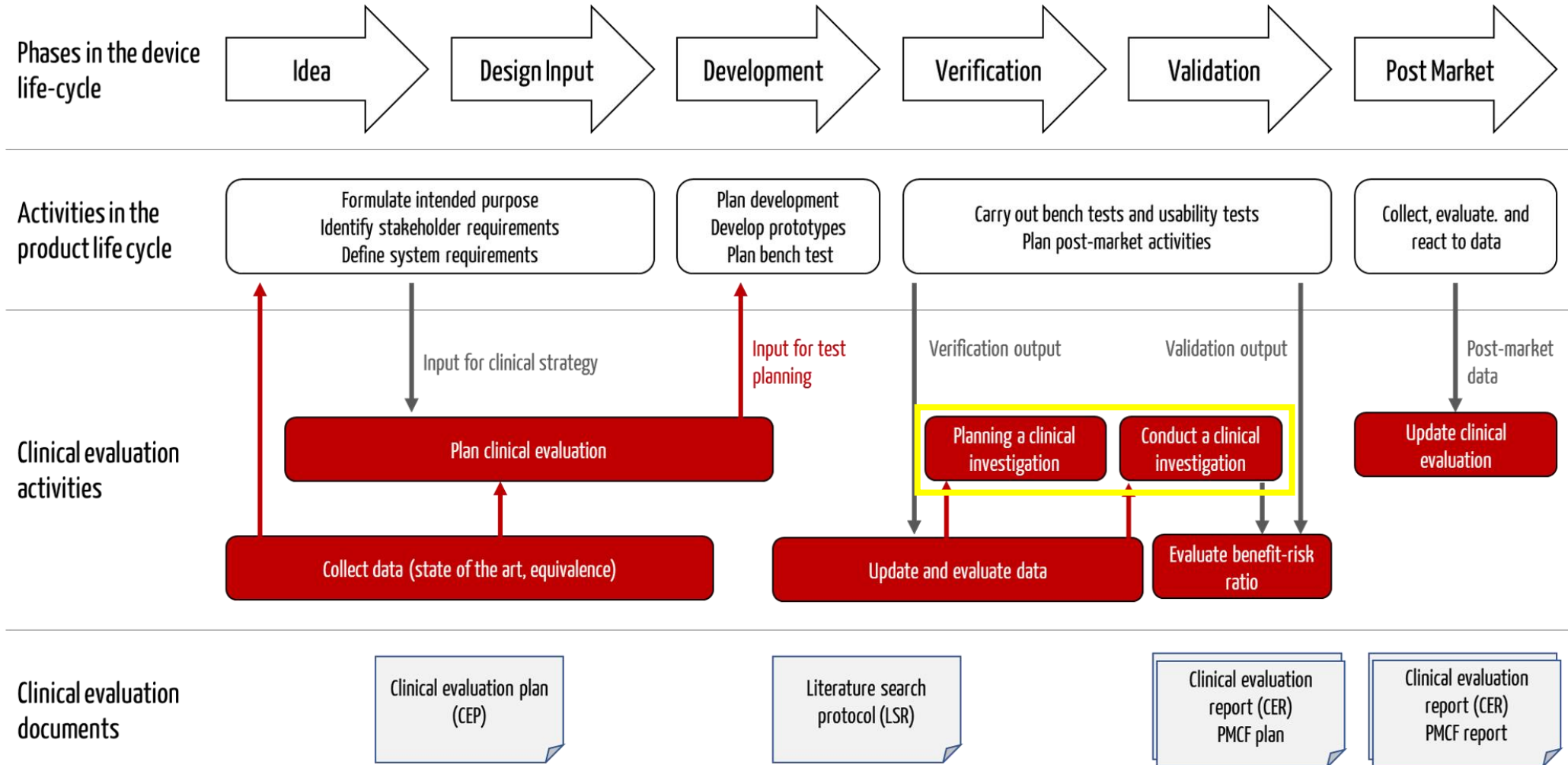


Clinical Evaluation

Clinical Evaluation

MDR Article 2: “clinical evaluation”
means a systematic and planned process
to continuously generate, collect, analyse, and assess
the clinical data pertaining to a device
in order to **verify the safety and performance**,
including clinical benefits, of the device
when used as intended by the manufacturer

Clinical Evaluation & Clinical Investigation



Clinical Investigation

MDR Article 2: “clinical investigation”
any systematic investigation involving one or more human subjects, undertaken to assess the safety or performance of a device

PMS vs PMCF

Post-Market Surveillance = reactive + proactive

- Contains PMCF
- Monitor clinical studies, registries and literature
- Handle complaints
- Could lead to updates in PMCF plan (trend in complaints)

Post-Market Clinical Follow-up = proactive

- Follow-up on clinical registries
- Plan to test known differences in software performance
- Plan to assess residual risks from risk management
- Monitor long term performance (performance drift)
- Detecting new risks



MDCG 2023-1

Guidance on the Health Institution Exemption under Article 5(5)

- Changes the intended purpose of a **CE-marked device** → Article 5(5) applies
- Ascribe a medical intended purpose to a **RUO product** → Article 5(5) applies





AI Act

AI Act

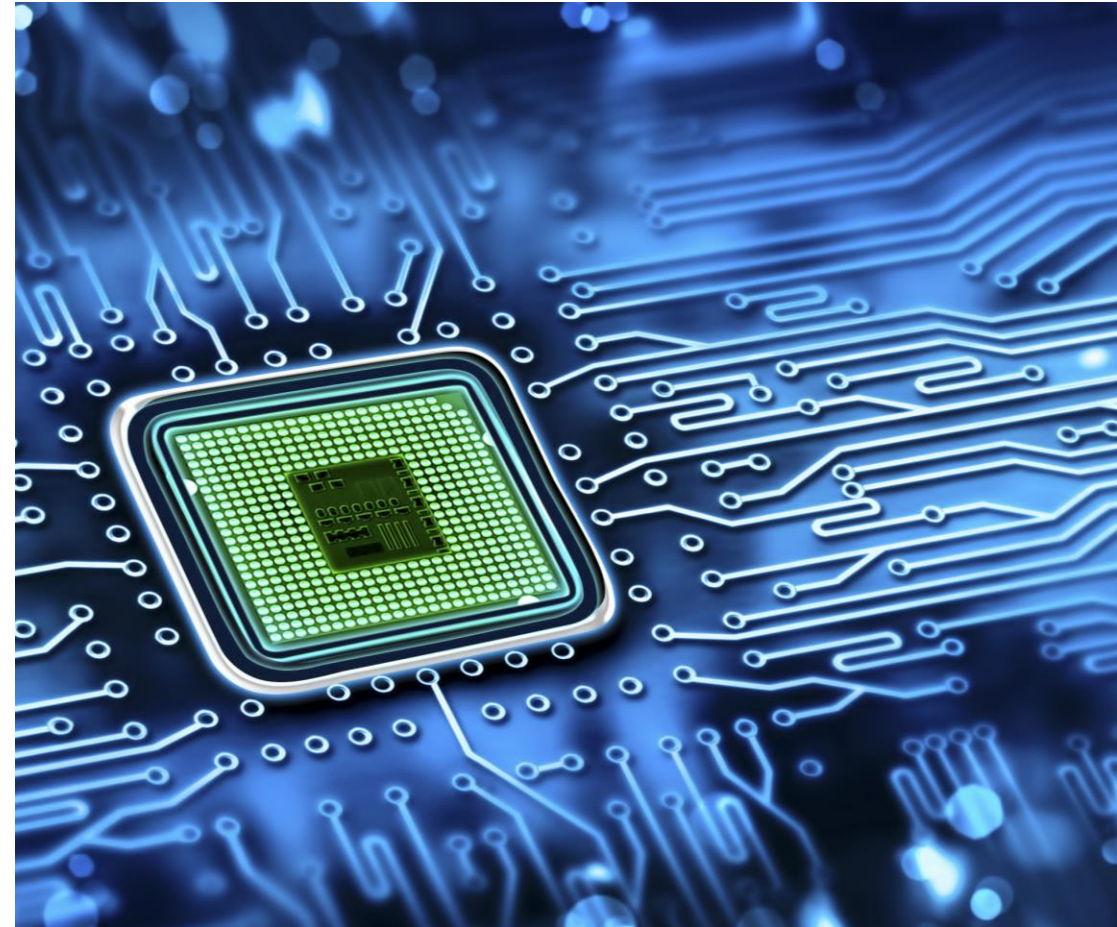
Definition

The aim of the rules is
to **foster trustworthy AI**
in Europe.

Classification









High-risk AI if:

1. The MDAI is a **safety component**, or the AI system is itself a **medical device** and
 2. The MDAI is subject to a **third-party conformity assessment** by a notified body in accordance with the MDR/IVDR.
- In-house devices?
 - Annex III



The AIA

High-risk AI systems shall comply with a set of specific requirements, established by the AIA (European Commission, 2021).

-  Data quality & Governance
-  Record keeping & Logging
-  Human oversight
-  Risk management system
-  Conformity assessment
-  Transparency and provision of information to users "IFU"
-  Accuracy, robustness, and cybersecurity *(one for each)*
-  Quality management system

Trustworthiness

Requirements

Risk
Management
System

Technical
Documentation

Record-Keeping

Transparency

Human
Oversight

Accuracy,
Robustness, and
Cybersecurity

Obligations for
Providers

Obligations for
Deployers

...

Compliance

- **Overlap with MDR**
 - Integrate with existing procedures
- **Proposal for a regulation** to simplify rules on medical and in vitro diagnostic devices
- Obligations for **providers** and obligations for **deployers**





**Other
Regulations**

Other Regulations

EHDS

Cyber
Security Act

GDPR

NIS 2

ISO/IEC
27000
Family

...

Thank you!

Stef Rommes

VITO, Industriezone Vlasmeer 7,
Europawijk, 2400 Mol, Belgium

stef.rommes@vito.be

[linkedin.com/in/stefrommes](https://www.linkedin.com/in/stefrommes)

