Regulatory Affairs for Hackers

What happens when you get regulated hard?

Leon Holub - OWASP Frankfurt Meetup 26.02.2025

Regulatory Affairs for Hackers

Leon Holub - OWASP Frankfurt Meetup 26.02.2025

- I’m Leon, my background is in Software Development
- Product Owner at Johner Institut GmbH
  - Regulatory Consulting for Medical Device Manufacturers
  - I work on the Regulatory Intelligence platform „Regulatory Radar“
  - We’re hiring security professionals ;)

Regulatory affairs (RA), is a profession that deals with an organization’s adherence to regulatory compliance.

https://en.wikipedia.org/wiki/Regulatory_affairs

They [devices] shall be safe and effective […] taking into account the generally acknowledged state of the art.

Regulation (EU) 2017/745 (MDR) ANNEX I Chapter I (1) - GENERAL SAFETY AND PERFORMANCE REQUIREMENTS

Regulatory goals for Medical Devices

- Performance

  ➡ ‘performance’ means the ability of a device to achieve its intended purpose as stated by the manufacturer;
  European Medical Device Regulation (MDR) Article 2 (22)

- Safety

  ➡ Freedom from unacceptable risk
  ISO/IEC 51:1999, definition 3.1

Harmonized standards

I came, ISO, I conquered

- Can be used to prove regulatory compliance
- Are written by industry committees
- Are recognized (harmonized) by the European Commission and European Standards Organizations

See https://single-market-economy.ec.europa.eu/single-market/european-standards/harmonised-standards_en

Core Concepts

Core Concepts

- Quality Management
- Risk Management
- Post-Market Surveillance
- Clinical Evaluation
- Risk based approach
  - Not all products have to undergo the same efforts

See also: https://www.johner-institut.de/blog/category/qualitaetsmanagement-iso-13485/

Core Concepts - Quality Management

Core Concepts

Quality Management (ISO 13485)

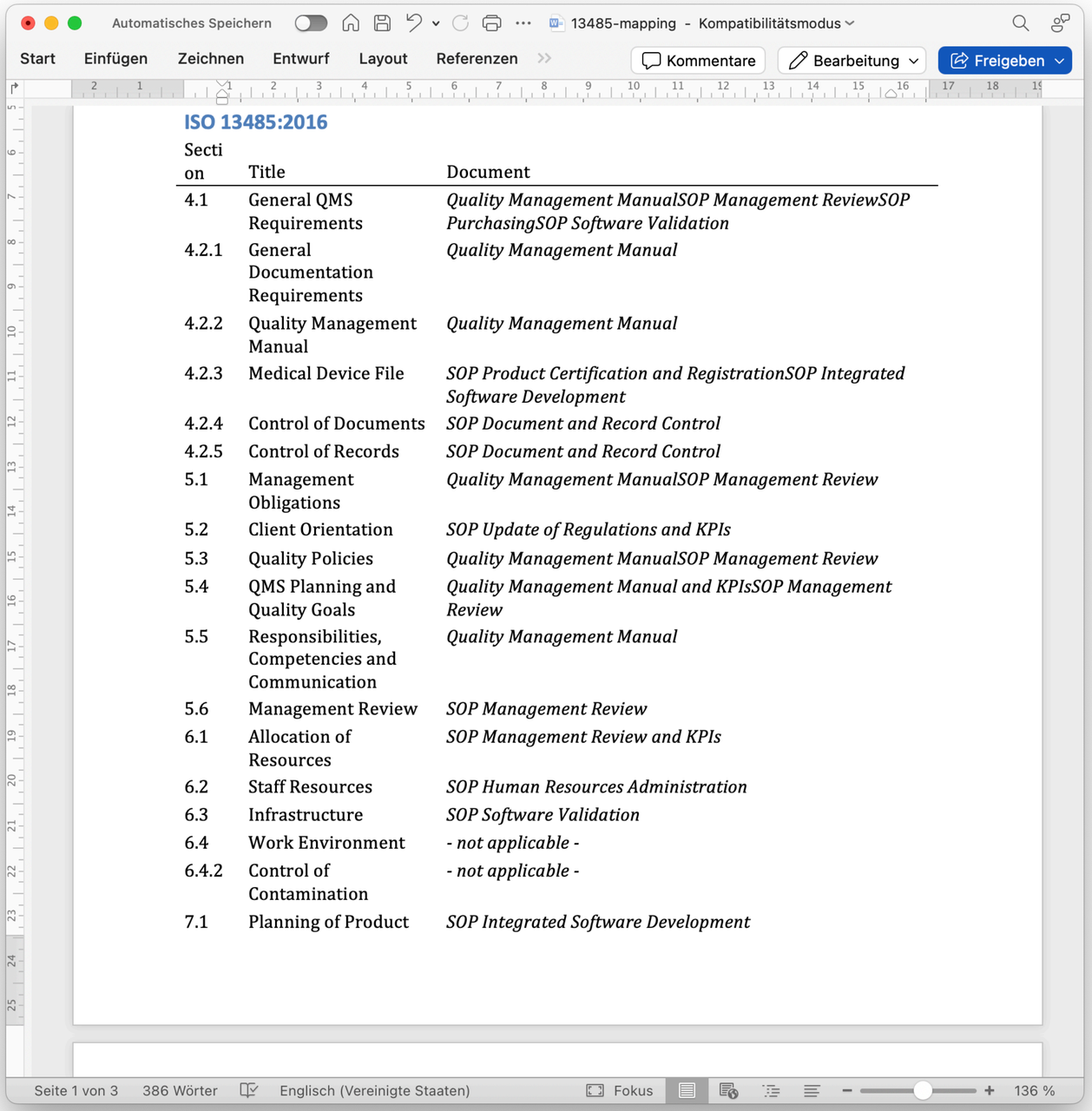
- PDCA Cycle
  - Plan - Do - Check - Act
  - Continuous Improvement
- Quality Management System
  - „If it’s not documented it does not exist“
  - Everything critical is defined in a process

See also: https://www.johner-institut.de/blog/category/qualitaetsmanagement-iso-13485/

Quality Management

Quality Management Systems in Practice (Excerpt)

- Product development
- HR & Training
- Software validation
- Corrective and preventive actions



Section	Title	Document
4.1	General QMS Requirements	*Quality Management ManualSOP Management ReviewSOP PurchasingSOP Software Validation*
4.2.1	General Documentation Requirements	*Quality Management Manual*
4.2.2	Quality Management Manual	*Quality Management Manual*
4.2.3	Medical Device File	*SOP Product Certification and RegistrationSOP Integrated Software Development*
4.2.4	Control of Documents	*SOP Document and Record Control*
4.2.5	Control of Records	*SOP Document and Record Control*
5.1	Management Obligations	*Quality Management ManualSOP Management Review*
5.2	Client Orientation	*SOP Update of Regulations and KPIs*
5.3	Quality Policies	*Quality Management ManualSOP Management Review*
5.4	QMS Planning and Quality Goals	*Quality Management Manual and KPIsSOP Management Review*
5.5	Responsibilities, Competencies and Communication	*Quality Management Manual*
5.6	Management Review	*SOP Management Review*
6.1	Allocation of Resources	*SOP Management Review and KPIs*
6.2	Staff Resources	*SOP Human Resources Administration*
6.3	Infrastructure	*SOP Software Validation*
6.4	Work Environment	*- not applicable -*
6.4.2	Control of Contamination	*- not applicable -*
7.1	Planning of Product	*SOP Integrated Software Development*

Source: https://openregulatory.com/or_template/iso-13485-mapping-of-requirements-to-documents/

Core Concepts - Risk Management

Core Concepts

Risk Management

- Risk

  ➡ Combination of the probability of occurrence of harm and the severity of that harm - ISO 14971:2022 3.18

See also: https://www.johner-institut.de/blog/category/iso-14971-risikomanagement/

Core Concepts

Risk Management

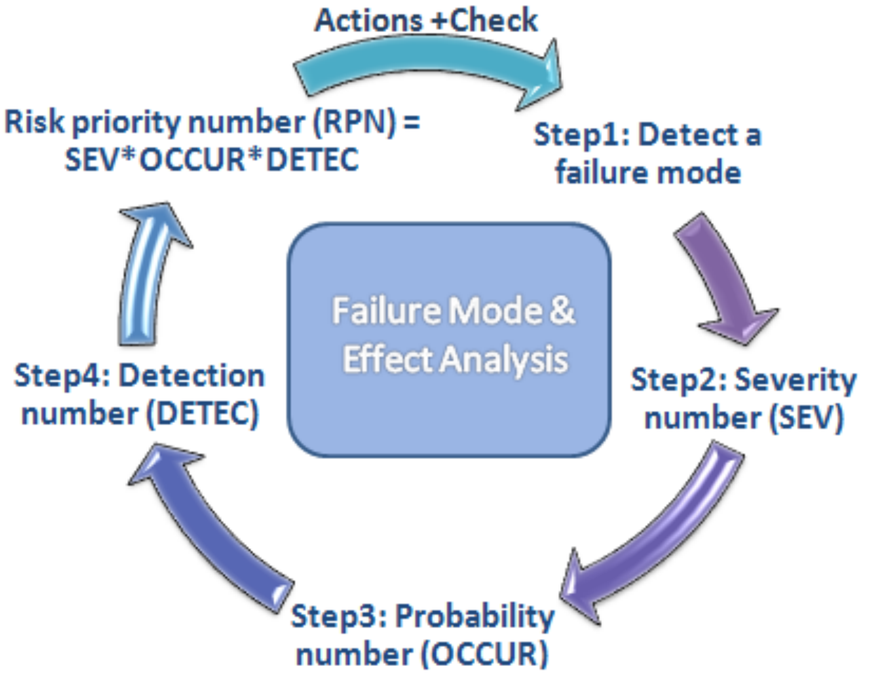
- Risk Management Plan
- Hazard(/Risk) Analysis
- Risk assessment
- Risk acceptance
- Post-Market Phase
- No Standard way
  - Laws, Standards and Guidances provide multiple options

See also: https://www.johner-institut.de/blog/category/iso-14971-risikomanagement/

Risk Management

Hazard Analysis Methods - FMEA

- Systematic method to identify potential failures before they occur
- Used in both product design (Design FMEA) and processes (Process FMEA)
- Proactive tool for risk assessment and mitigation
  - You work your way from cause to effect
- Results documented in worksheet



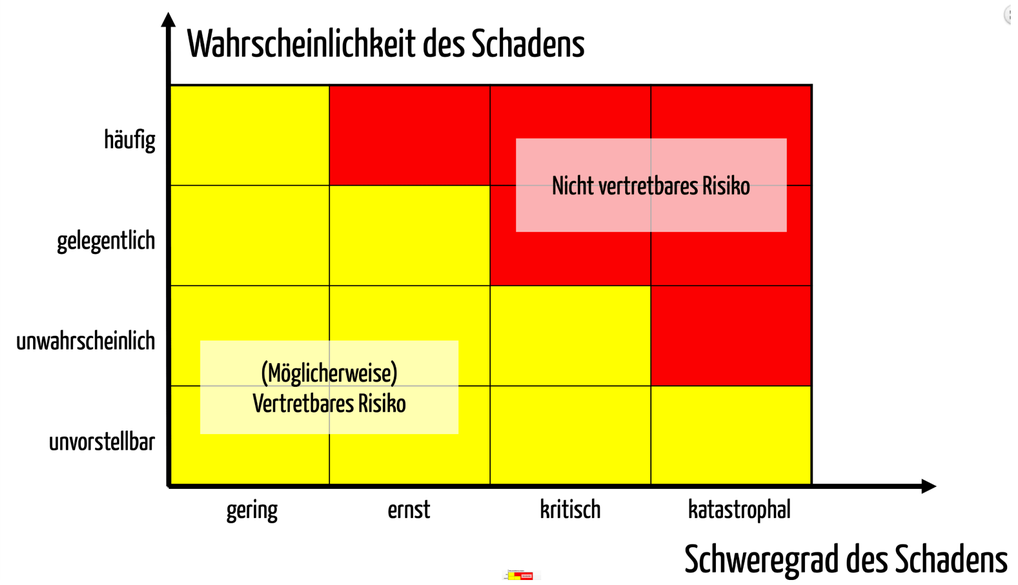
Source: https://en.wikipedia.org/wiki/File:FMEA.png

See also: https://www.johner-institut.de/blog/iso-14971-risikomanagement/fmea-bei-medizinprodukten/

Risk Management

Risk Acceptance Matrix

- 2D grid combining severity and probability
- Shows acceptable vs. unacceptable risks
- Risk needs to be „as low as reasonable possible“



Source: https://www.johner-institut.de/blog/iso-14971-risikomanagement/risikoakzeptanzmatrix-risikobewertungsmatrix/

See also: https://www.johner-institut.de/blog/iso-14971-risikomanagement/risikoakzeptanzmatrix-risikobewertungsmatrix/

Other Requirements

Other Requirements

Product Safety - Electrical/Cyber/etc.

- Lets focus on Cybersecurity
  - SBOM
  - Security Risk Management
  - Secure Software Development Lifecycle
  - Post-Market Surveillance
    - Includes monitoring of Security Databases (NIST NVD etc.)

Cybersecurity

State of the art (Examples)

- Standards
  - Software Lifecycle Processes (IEC 62304)
  - Vulnerability disclosure (ISO/IEC 29147)
  - Secure health software (IEC 81001-5-1)
- FDA or MDCG Guidances
- OWASP Documents (https://owasp.org/)
- NIST Cybersecurity (https://www.nist.gov/cyberframework)
- and more..

Outlook

Outlook

What can it mean for us cybersecurity professionals?

- More pressure on management
- Frameworks for us to work with
  - International Standards
  - Guidance Documents
- Chances to learn
- Chances to participate in discussions
- Don’t get overwhelmed, organize, structure, learn, participate

Outlook

- Product Liability Directive
- AI-Act
- Cyber Resilience Act

What Now?

- Feedback and planned revisions of EU Regulations
- Estonia offers EU Standards for cheap https://www.evs.ee/en
- Free access to important harmonized standards
  - https://www.harmonisierte-normen-in-europa.de/
  - So far not much cybersecurity :(lots of standards for cranes?

Questions?