Medical Software Development

International standards requirements and practice

Elite Software R&D Services

Since 1990

What? A public health agency
Why? Protect American consumers
How? By enforcing the Federal Food, Drug and Cosmetic Act and several related public health laws

Administrative Enforcement Powers

Unannounced and Announced inspections
Inspectional observations
Warning letters
Adverse Publicity
FDA-Initiated recalls and monitoring Company-Initia
Delay, Suspension or Withdrawal of Production Approvals
Preclusion of Government contracts
Definition and Refusal of entry into U.S. Commerce of Imported Products

What is a medical device

Any instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of

diagnosis, prevention, monitoring, treatment or alleviation of disease

diagnosis, monitoring, treatment, alleviation of or compensation for an injury

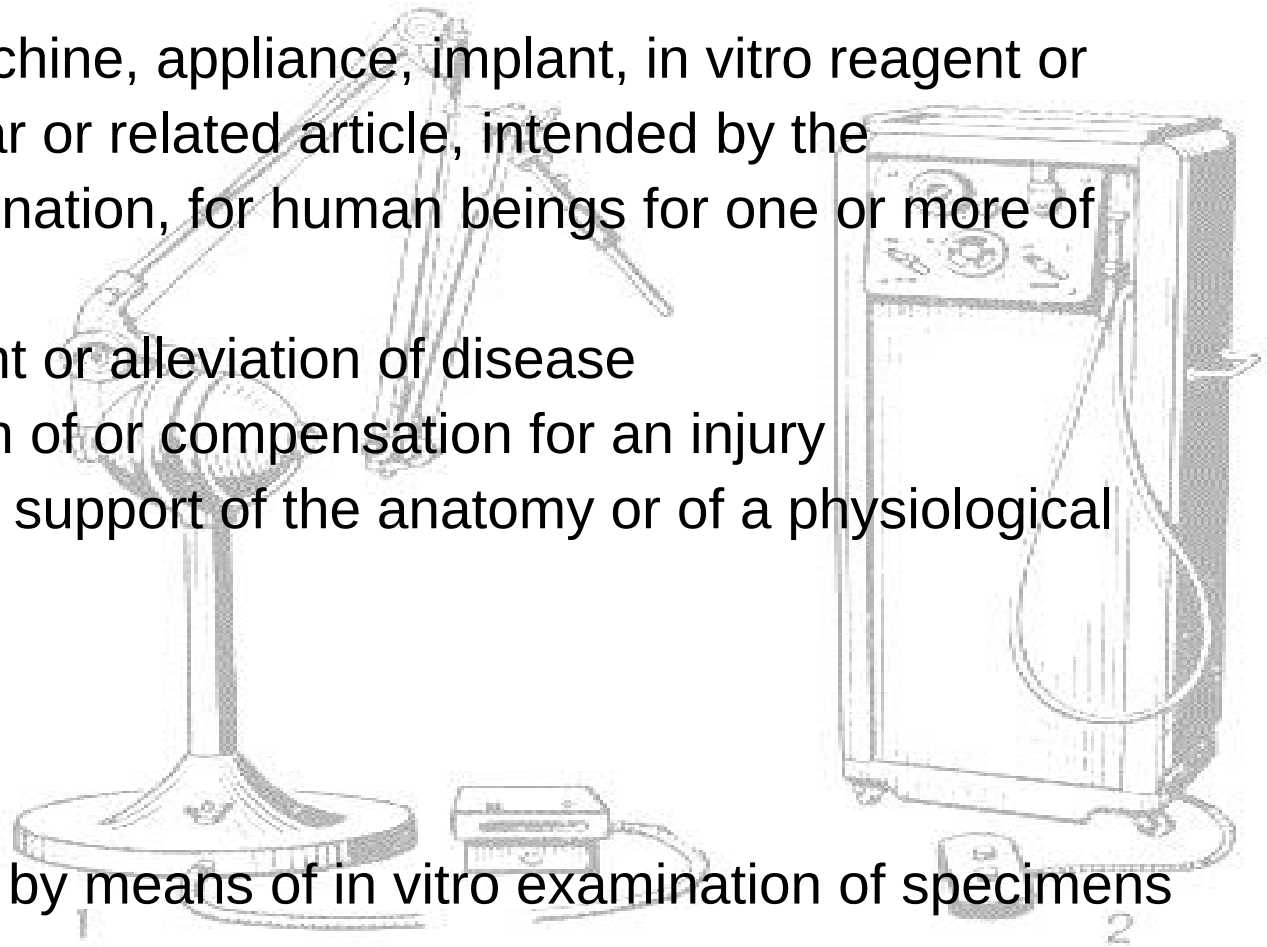
investigation, replacement, modification, or support of the anatomy or of a physiological process

supporting or sustaining life

control of conception

disinfection of medical devices

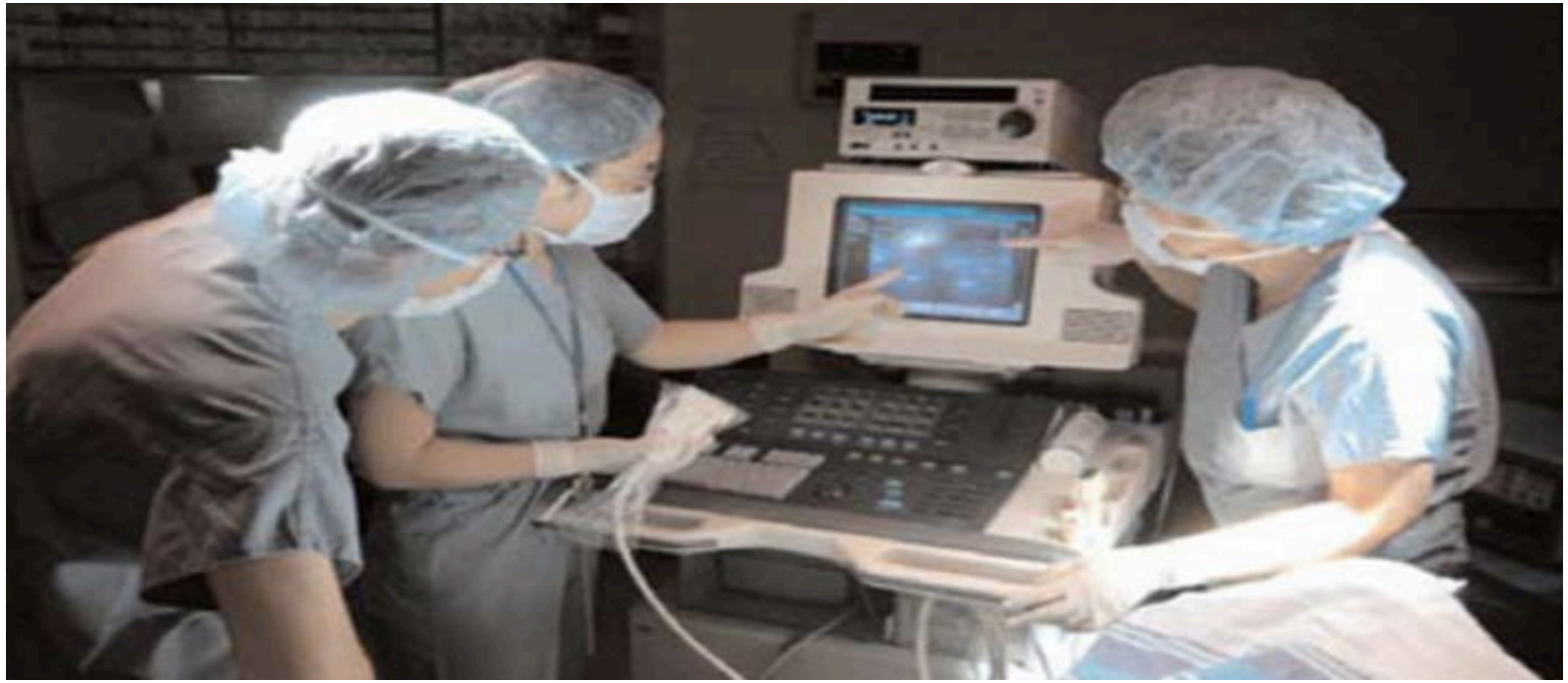
providing information for medical purposes by means of in vitro examination of specimens derived from the human body



What is not a medical device

… and which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means

Medical device software types



Software is a part of medical device
Software is an accessory for medical device
Software itself is medical device

Non-device software (regulated by FDA)

Production system
Quality system
System to create/maintain records required by FDA regulations

All medical devices must be approved by FDA before they can be sold in the US

Periodic inspections for manufacturers

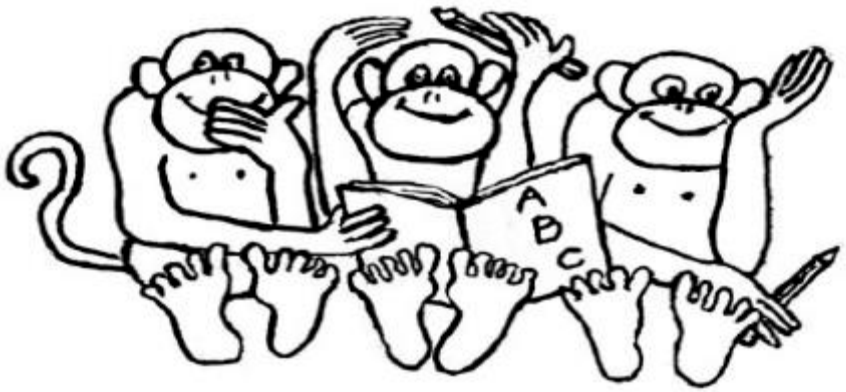
Manufacturers must control their suppliers, contractors and services providers to ensure the compliance

Concepts of hazard and harm

Harm is a physical injury or damage to the health of people or damage to property or the environment

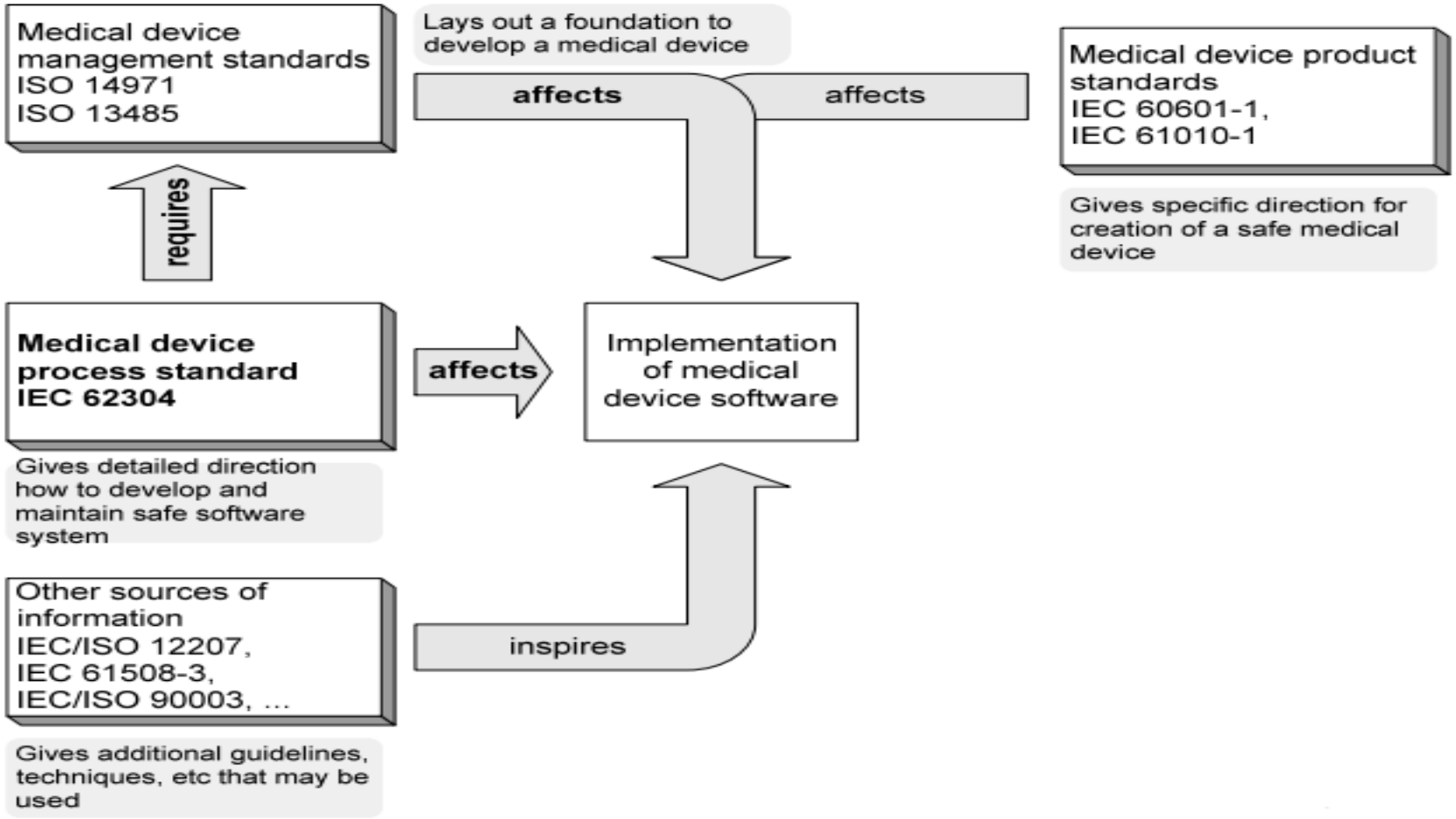
Hazard is a potential source of harm

Hazard/harm concept is used in risk management to define software safety class



IEC 62304 – Software life cycle processes
ISO 14971 – Application of risk management to medical devices
ISO 13485 – Quality management systems

Standards relationship



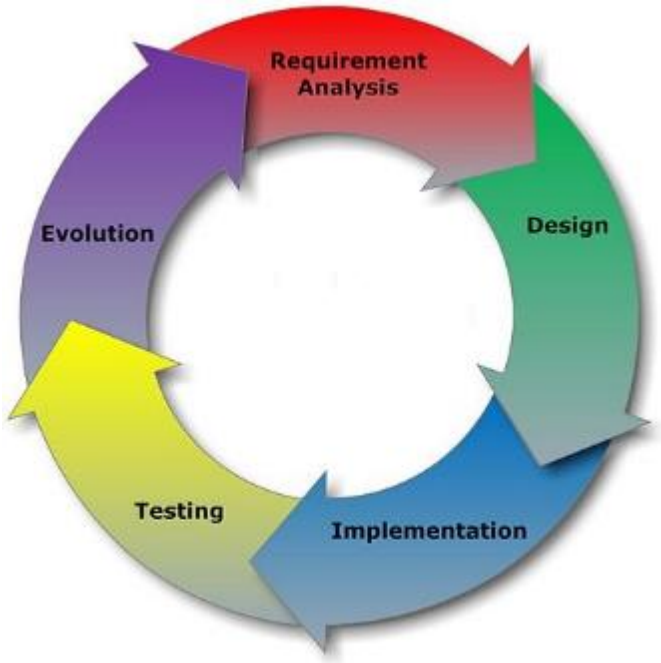
IEC 62304 (SW life cycle processes)

Defines the life cycle requirements for medical device software

Establishes common framework for medical device software life cycle processes:

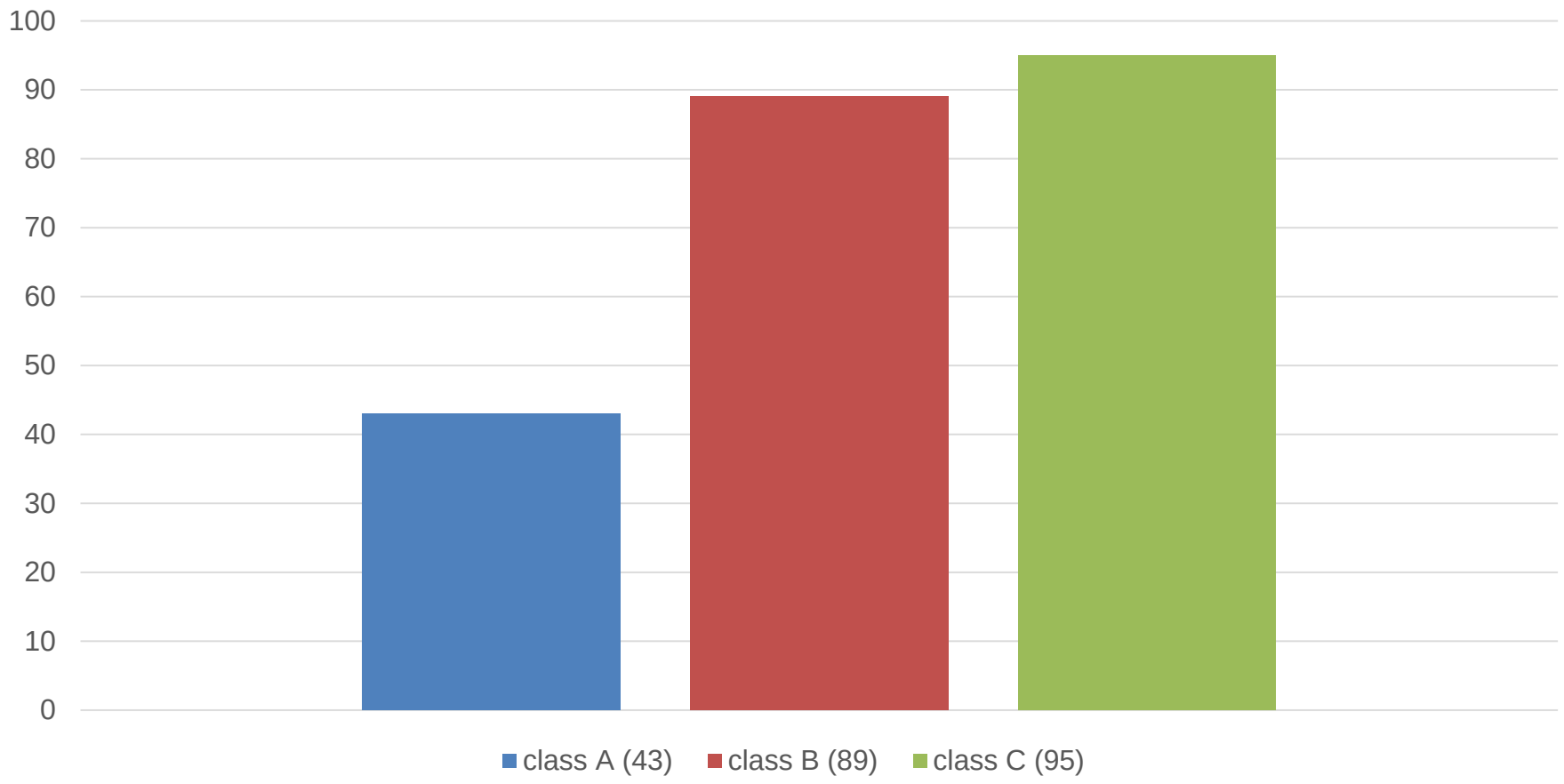
processes
activities
tasks

Applies to the development and maintenance of medical device software



Class A: No injury or damage to health is possible
Class B: Non-SERIOUS INJURY is possible
Class C: Death or SERIOUS INJURY is possible
Serious Injury is Injury or illness that directly or indirectly
is life threatening,
results in permanent impairment of a body function or permanent damage to a body structure, or necessitates medical or surgical intervention to prevent permanent impairment of a body function or permanent damage to a body structure.
Note: Permanent impairment means an irreversible impairment or damage to a body structure or function excluding trivial impairment or damage.

IEC 62304: A, B, C class activities



IEC 62304 (SW life cycle processes)

Compliance to the standard is defined as implementing **all** of the processes, activities and tasks identified in this standard in accordance with the software safety class – there is no “partial compliance”

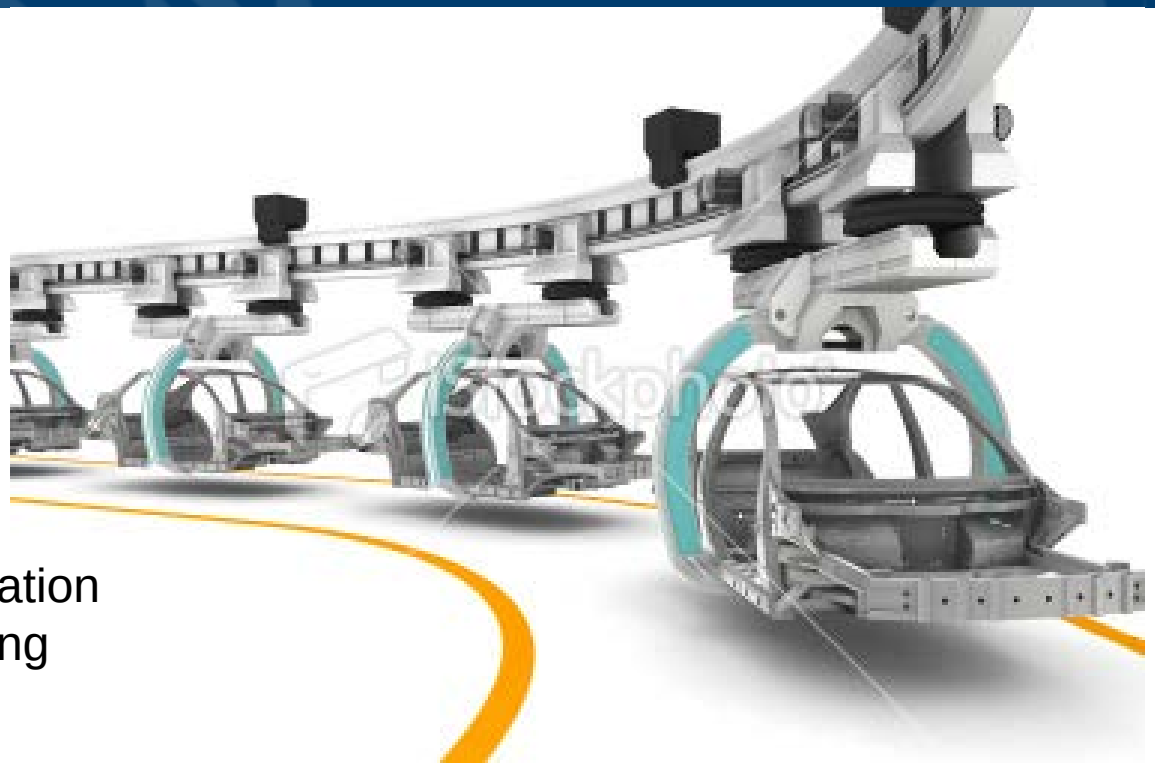
Doesn’t cover validation and final release

IEC 62304: processes covered

Software Development
Software Maintenance
Software Risk Management
Software Configuration Management
Software Problem Resolution

IEC 62304: Software Development

Planning
Requirements analysis
Architectural design
Detailed design
Unit Implementation and verification
Integration and integration testing
System testing
Release



IEC 62304: Software Maintenance

Plan
Analysis
Modification implementation

IEC 62304: Software Risk Management

Risk analysis
Risk control measures
Verification of risk control measures
Risk management of software changes

IEC 62304: Software Configuration Management

Configuration identification
Change control
Configuration status accounting

IEC 62304: Software Problem Resolution

Preparing problem reports
Investigation
Advising relevant parties
Using change control process
Maintaining records
Analyzing problems for trends
Verifying software problem resolution
Test documentation contents

ISO 14971 (Risk management)

Specifies a process for a manufacturer
to identify the hazards associated with medical devices, including in vitro diagnostic (IVD) medical devices
to estimate and evaluate the associated risks
to control these risks
to monitor the effectiveness of the controls
Applicable to all stages of the life-cycle of a medical device

ISO 14971 covers

Risk management process
Qualification of personnel
Risk management plan
Risk analysis
Risk evaluation
Risk control
Risk reduction
Risk management report
Production and post-production information

ISO 13485 (Quality management)

Specifies requirements for a quality management system that can be used by an organization for the design and development, production, installation and servicing of medical devices, and the design, development, and provision of related services

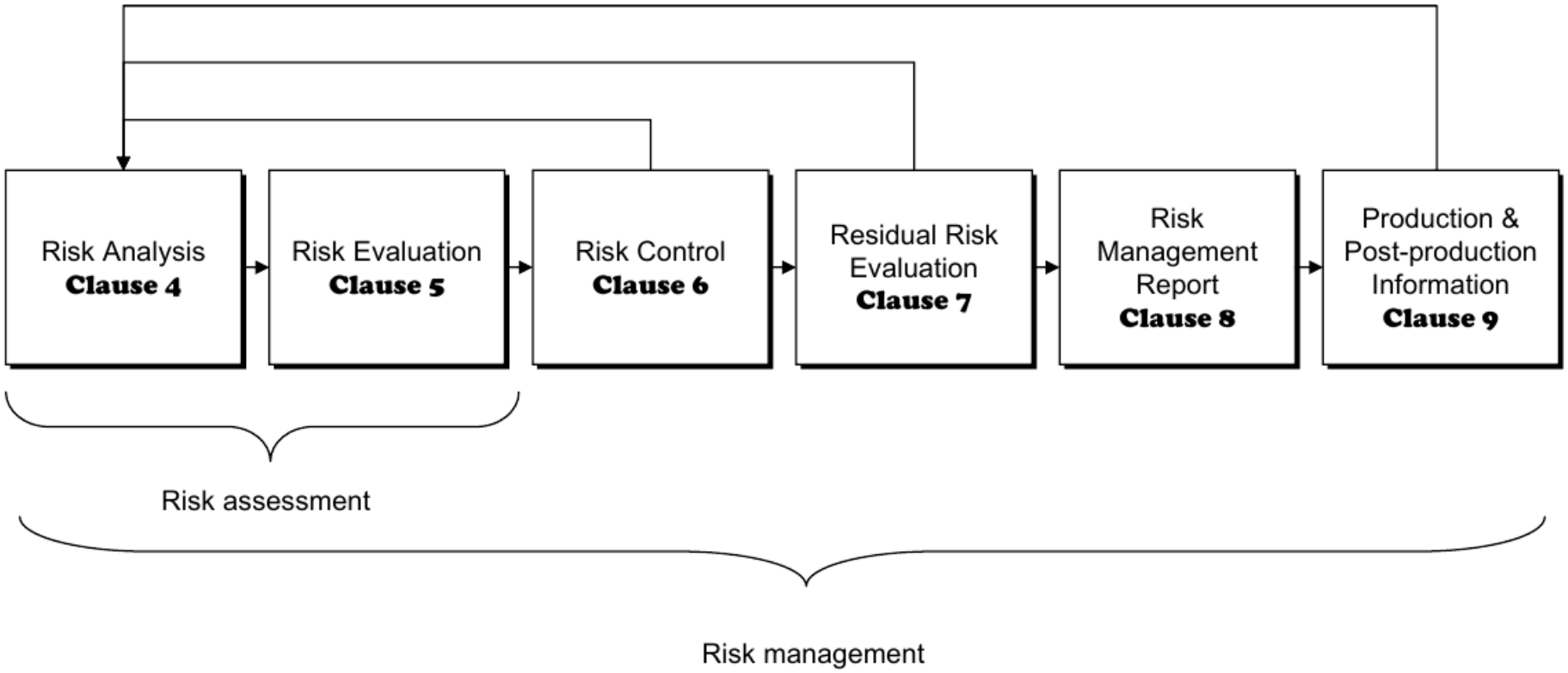
Applicable to organization of any size

ISO 13485 covers

Quality of the Planning process
Quality of the Documents
Quality of the Design
Quality of the Development
Quality of the Resources
Quality process monitoring
Quality improvements

- ISO 14971 (Risk management)

Risk management process



Risk management plan includes at least

- the **scope** of the planned risk management activities
- assignment of **responsibilities** and **authorities**
- **requirements for review** of risk management activities
- criteria for **risk acceptability**
- **verification** activities
- activities related to collection and review of **production and post-production information**

All team members should be familiarized with RM plan.

Risk management file

Contains **records** and **documents** generated during risk management process

Provides **traceability** for each hazard to

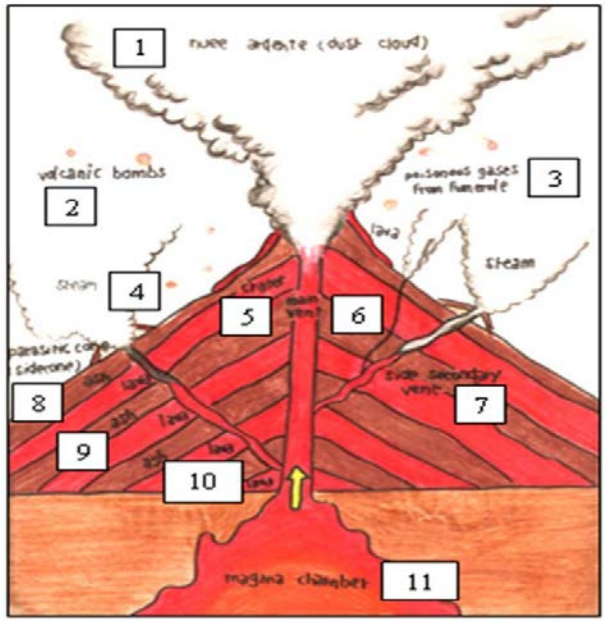
- the risk analysis
- the risk evaluation
- the implementation and verification of the risk control measures
- the assessment of the acceptability of any residual risks

Harm and hazard

Harm is a physical injury, damage, or both to the health of people or damage to property or the environment

Hazard is a potential source of harm

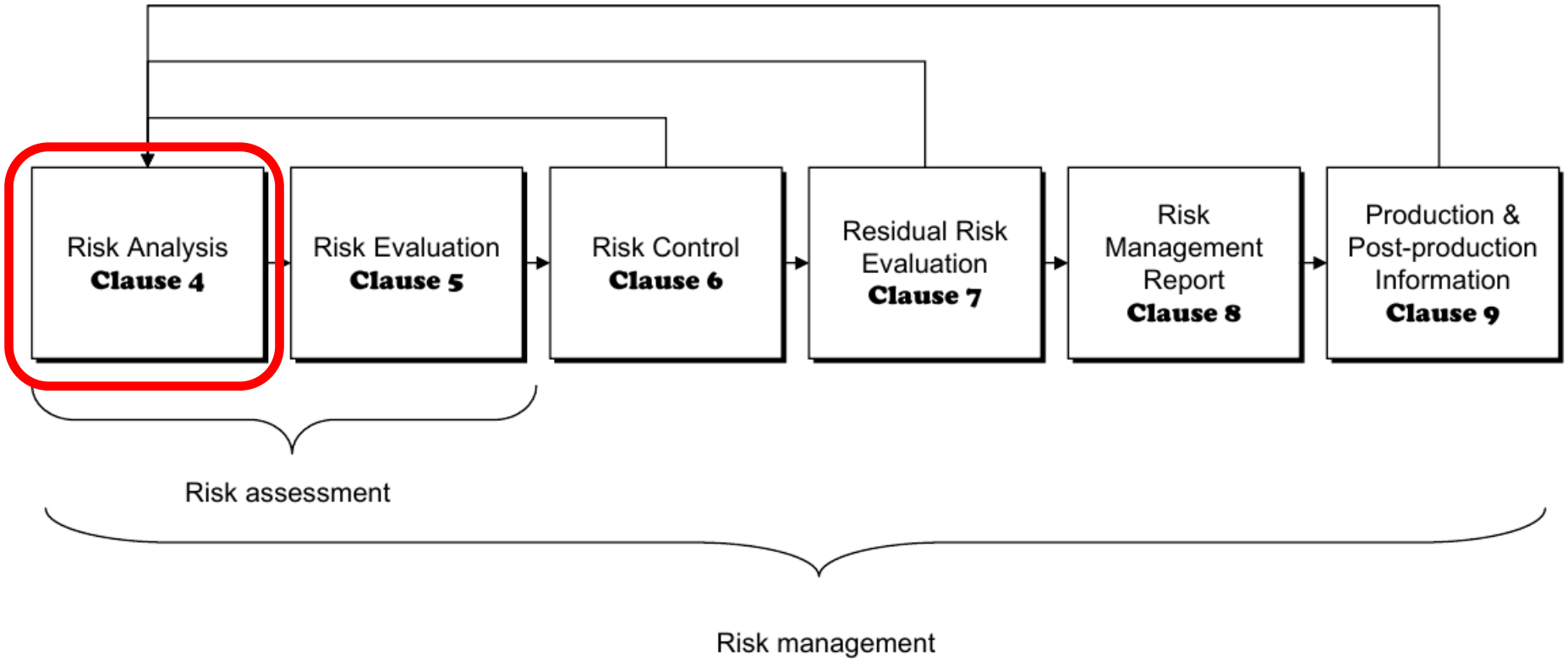
Risk definition: key concepts



Hazard + Sequence of events = Hazardous Situation

Severity × Probability = Risk

Risk management process



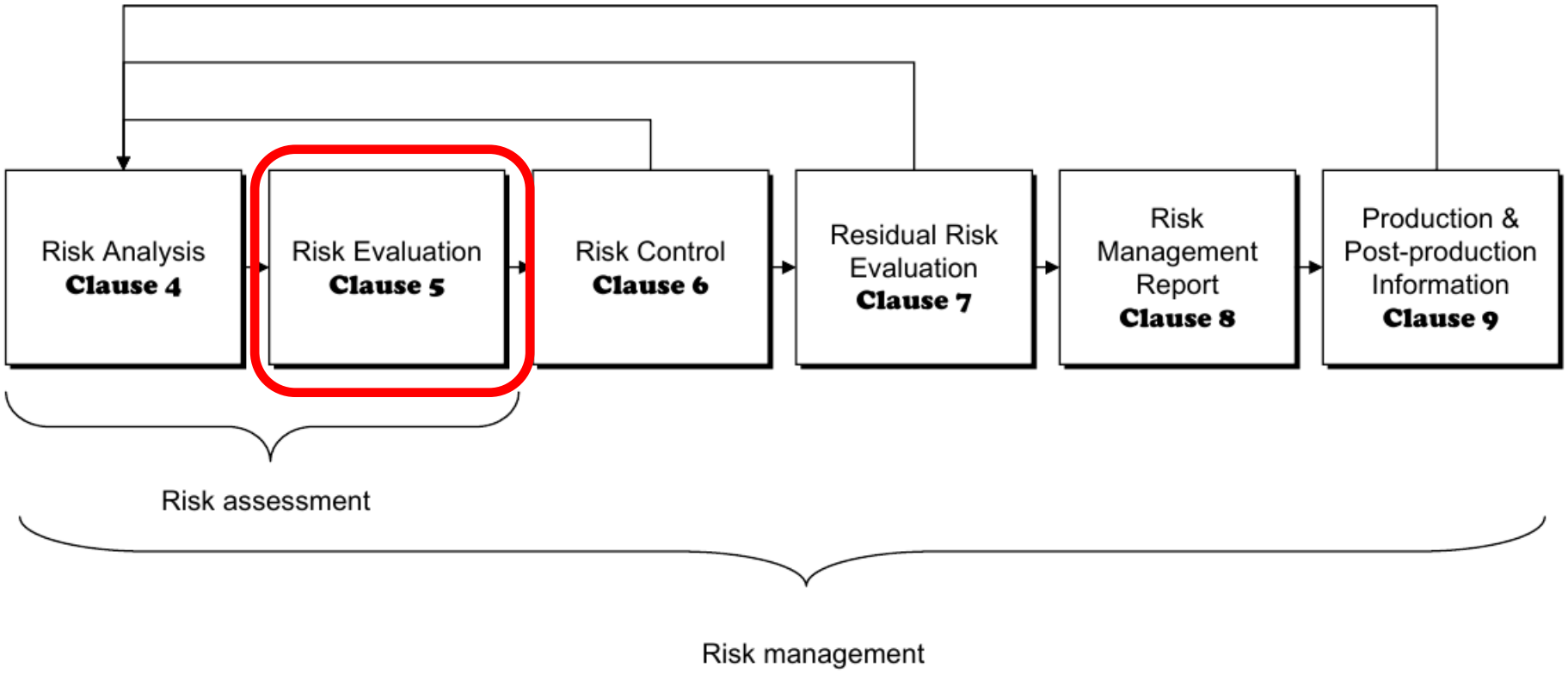
Risk analysis

- Document both the **intended use** and **foreseeable misuse** of the device
  - identify and document device characteristics that could affect the safety
- Identify and document known and foreseeable **hazards** associated with the device
- **Estimate the risk** for each hazardous situation

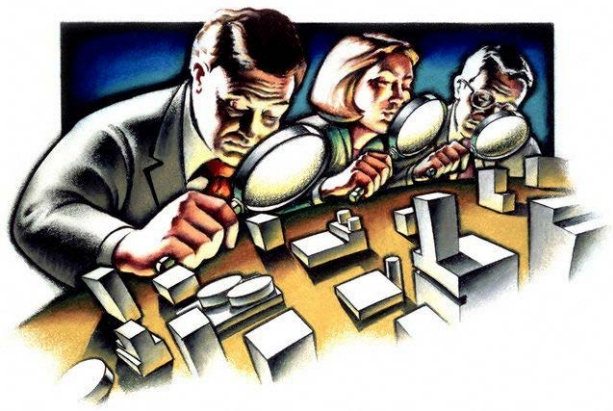
Risk estimation: possible sources of data

- published standards;
- scientific technical data;
- field data from similar medical devices already in use, including published reported incidents;
- usability tests employing typical users;
- clinical evidence;
- results of appropriate investigations;
- expert opinion;
- external quality assessment schemes.

Risk management process



Risk evaluation



- Risk evaluation criteria are defined in the risk management plan
- Each hazardous situation is evaluated against these criteria to decide if risk reduction is required
- Risk control measures should be applied if the risk is unacceptable

Risk evaluation: acceptance matrix

Qualitative probability levels	Qualitative severity levels: Negligible	Moderate	Significant
High	R_1	R_2	
Medium		R_4	R_5, R_6
Low		R_3	

Key

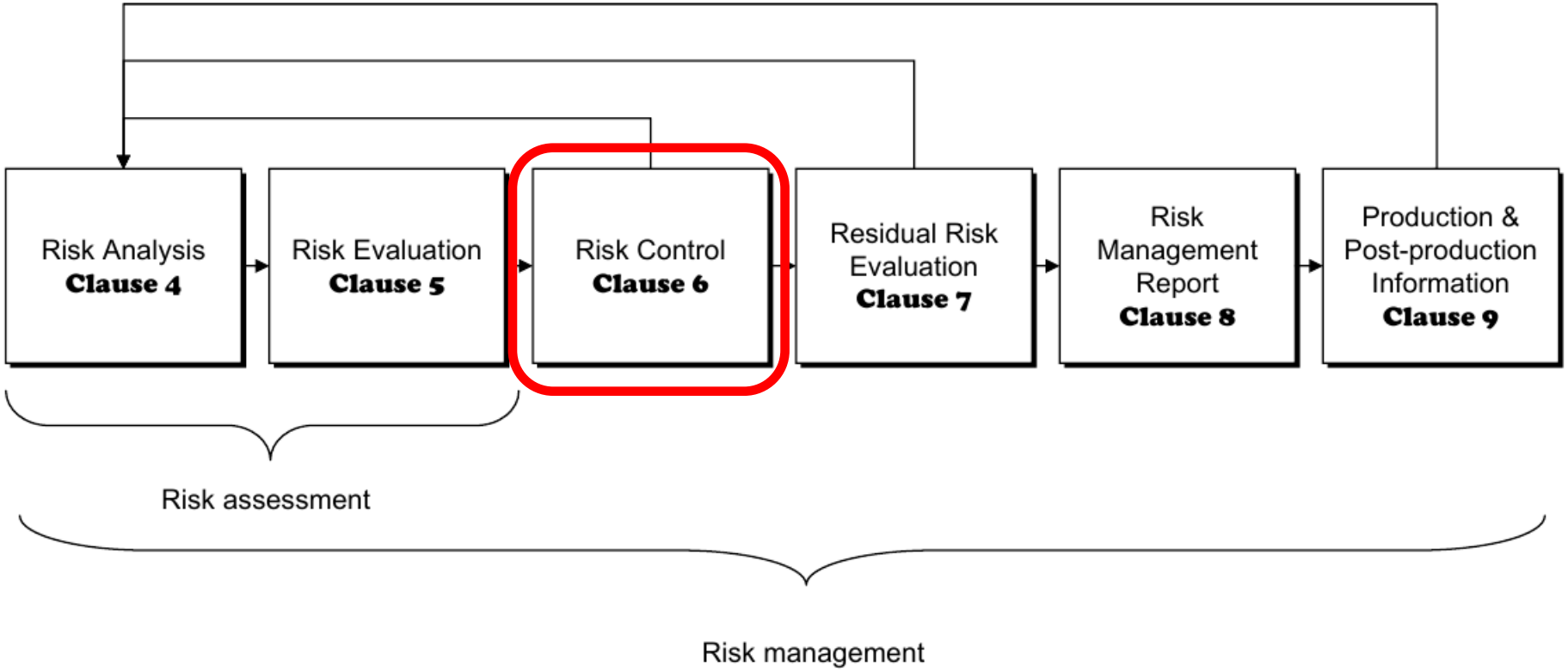
unacceptable risk

acceptable risk

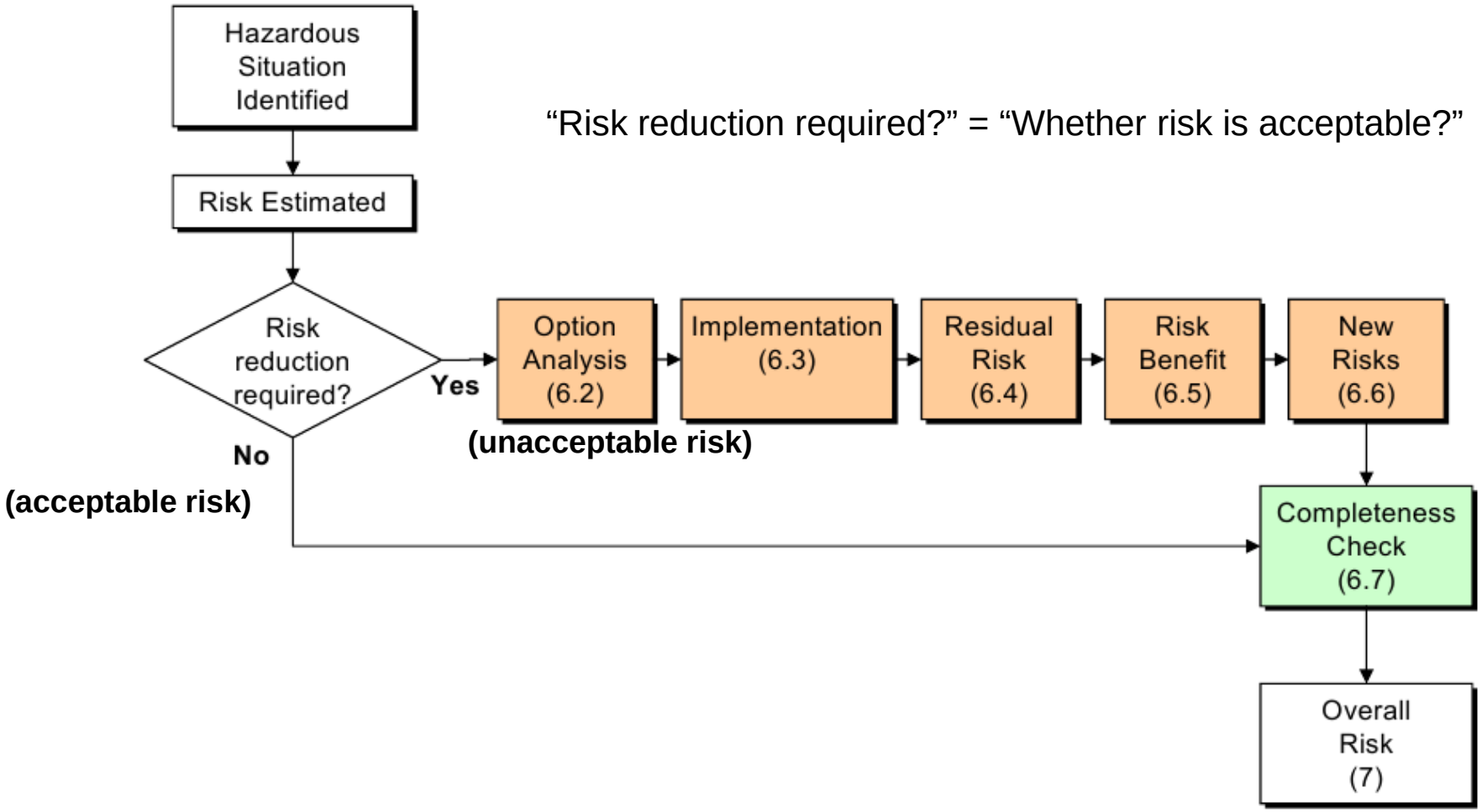
ALARP – As Low As Reasonably Practicable

Such charts are usually specific to a product and its particular intended use.

Risk management process



Risk control



"Risk reduction required?" = "Whether risk is acceptable?"

Risk control options

- inherent safety by design
- protective measures in the medical device
- protective measures in the manufacturing process
- information for safety

Inherent safety by design

- Removal of low-value features
- Safe architecture
- Clean user interface
- Software design rules
- Static structures

Protective measures implemented in the device

- Watchdog
- Timers
- Checksums
- Redundancy

Protective measures implemented in the process

- Peopleware (training etc.)
- Reviews
- Static analysis
- Test driven development
- Continuous integration
- Risk driven integration
- Iterations

Information for safety

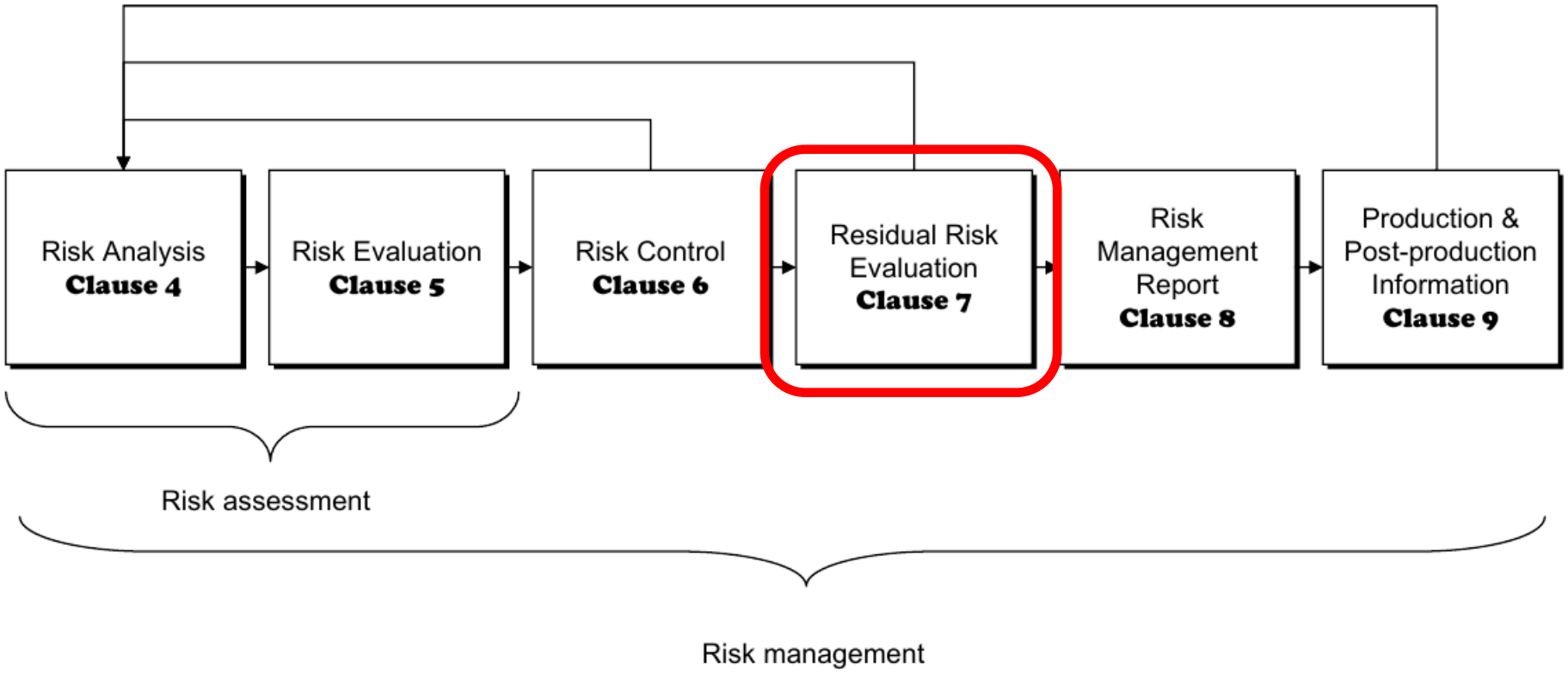
- Sound announcement of internal errors
  - Low on memory
  - Low on disk space
- Labeling
- User manuals

Risk control measure verification

- RCM is implemented in the final design
- The measure as implemented actually reduces the risk

Validation study can be used for verifying the effectiveness of the risk control measure.

Risk management process



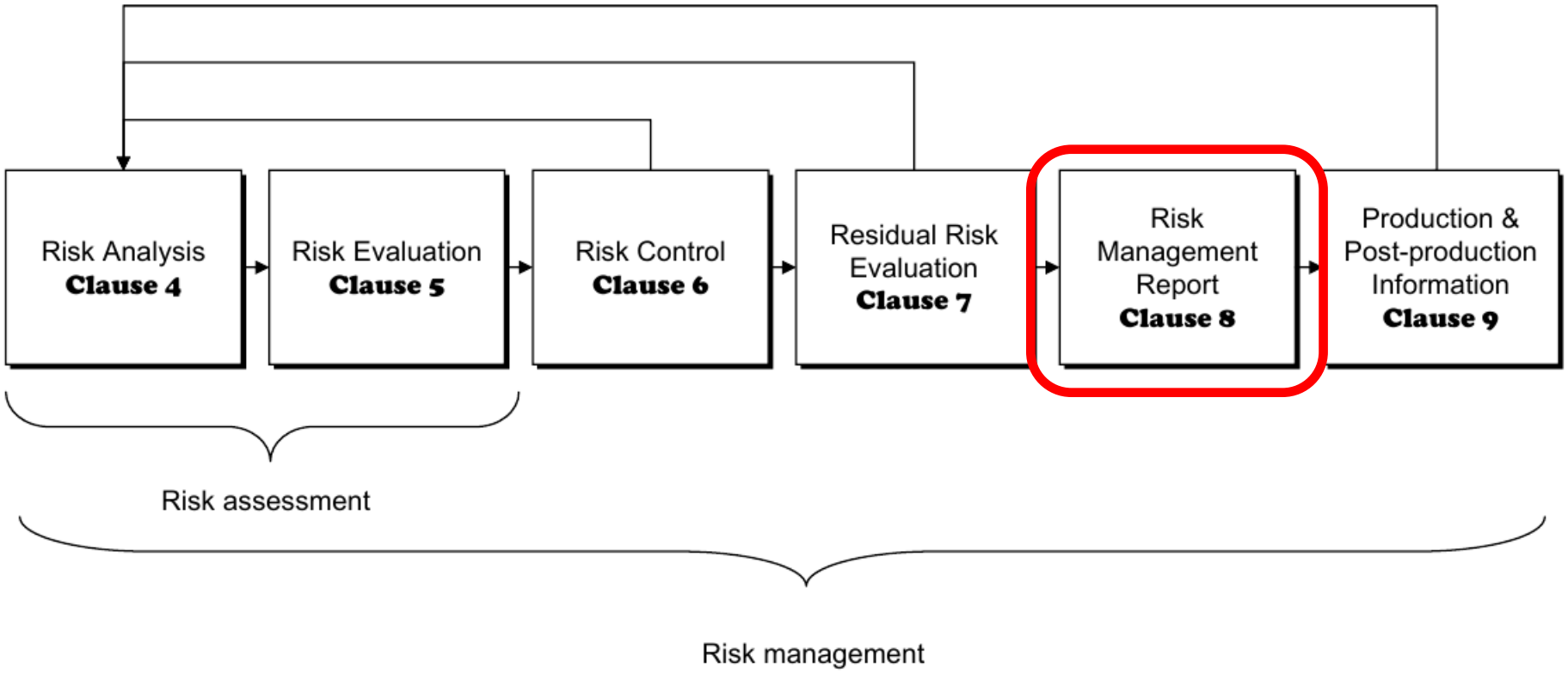
Overall residual risk evaluation

After **all** RCMs are implemented and verified, overall residual risk is evaluated for acceptability.

Unacceptable => risk/benefit analysis

Acceptable => information about the residual risk is disclosed in accompanying documents

Risk management process



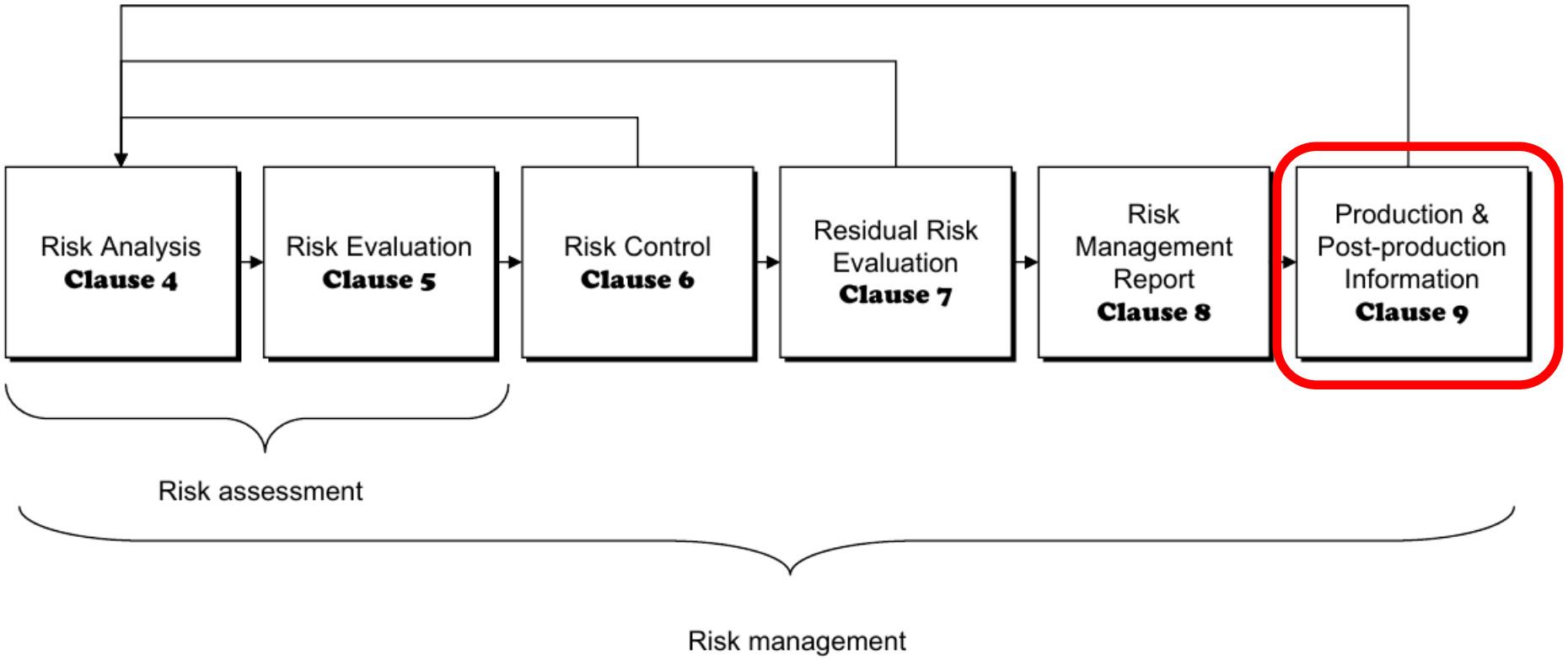
Risk management report

Before the release review risk management process to ensure:

- risk management plan implemented appropriately
- overall residual risk is acceptable
- appropriate methods are in place to obtain relevant production and post-production information

Review result are recorded as the risk management report

Risk management process

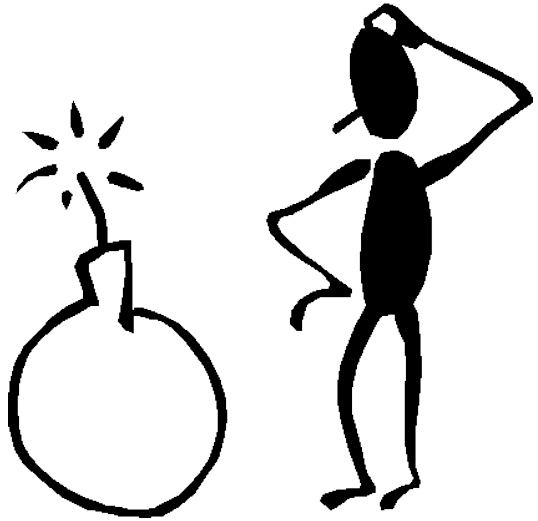


Production and post-production information

Must collect and review information about the medical device during production and post production phases:

- Installation and servicing reports
- Customer complaints
- New or revised standards
- Publicly available information about similar medical devices
- SOUP: updates, upgrades, bug fixes, obsolescence, anomaly lists

Production and post-production information: activities required



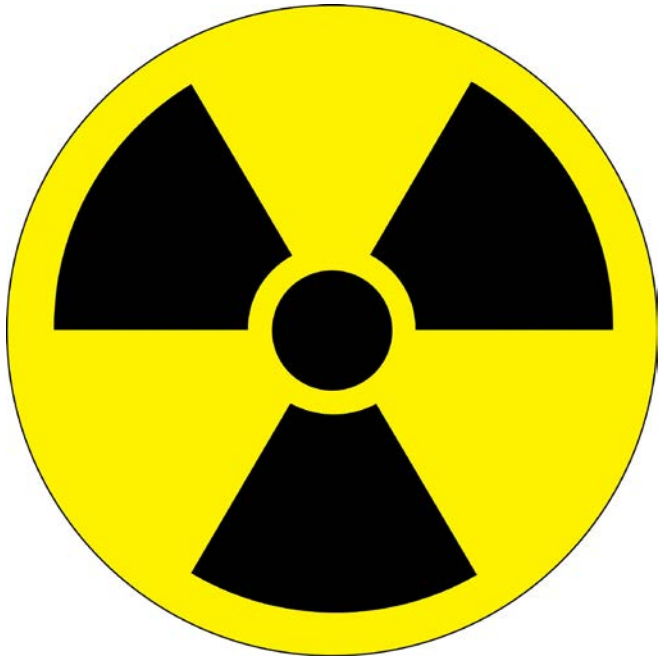
Evaluate safety:

- Any new hazards/hazardous situations?
- Estimated risk is no longer acceptable?

Yes:

- Evaluate the impact on previously implemented risk management activities
- Review all collected RM information; if possible that residual risks or acceptability has changed, evaluate the impact on previously implemented risk control measures

Energy hazards



- Electromagnetic energy
- Radiation energy
- Thermal energy
- Mechanical energy

Biological and chemical hazards

- Biological
- Chemical
- Biocompatibility

Operational hazards

- Function
- Use error

Information hazards

- Labelling
- Operating instructions
- Warnings
- Specification of service and maintenance

Thank you !

AURIGA®

Elite Software R&D Services

Since 1990