Regulatory, quality and clinical affairs

NX-451 – What to know when working with medical devices

Session 5

Kim Rochat

last update 2025-03-20

Risk Management – in general

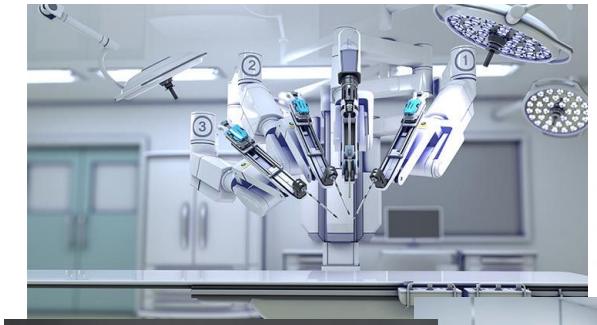
This is never going to happen to us…

Risk Management is part of our organization and sometimes… it fails….

Some well known examples:

- Nuclear industry : Chernobyl, Fukushima
- Shipping industry : Titanic, Costa Concordia
- Space industry: Space Shuttle Challenger
- Oil industry: Deepwater Horizon Oil Spill
- Banking industry : UBS had 3’500 «Risk Managers», Credit Suisse was “well controlled” by Finma

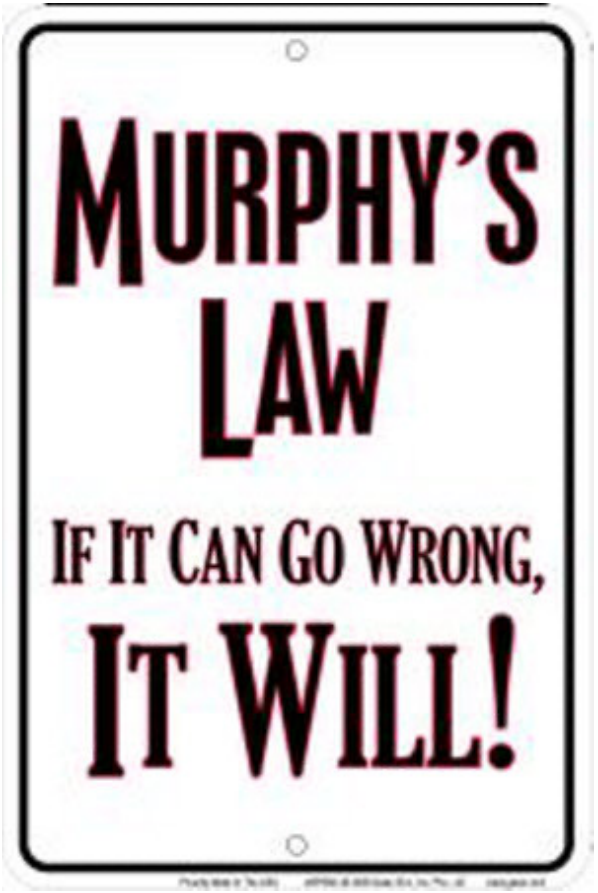
Risk Management – in general



Medical devices are used to treat patients, but they also represent a great deal of risks for them

Risk Management – in general

- **Safety of patients and users** is highest and primary objective for Medical Device Manufacturers.
- Medical Devices are designed by **humans** to be used by **humans.** Human activities are not free from fault (To Err Is Human (report)).
- Medical Device Manufacturers **shall prove** that the benefits of using their device are greater than the associated risks. An objective method is necessary to achieve this.



Risk Management – in general

GENERAL REQUIREMENTS

1. Devices shall achieve the performance intended by their manufacturer and shall be designed and manufactured in such a way that, during normal conditions of use, they are suitable for their intended purpose. They shall be safe and effective and shall not compromise the clinical condition or the safety of patients, or the safety and health of users or, where applicable, other persons, provided that any risks which may be associated with their use constitute acceptable risks when weighed against the benefits to the patient and are compatible with a high level of protection of health and safety, taking into account the generally acknowledged state of the art.

Design and development process shall ensure the devices are:

- Safe to use
- Risk vs benefit is favourable
- High level of protection

⇒ Risks must be acceptable

Risk Management – in general

GENERAL REQUIREMENTS

2. 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.

3. 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. In carrying out risk management manufacturers shall:

(a) establish and document a risk management plan for each device;

(b) identify and analyse the known and foreseeable hazards associated with each device;

(c) estimate and evaluate the risks associated with, and occurring during, the intended use and during reasonably foreseeable misuse;

(d) eliminate or control the risks referred to in point (c) in accordance with the requirements of Section 4;

(e) evaluate the impact of information from the production phase and, in particular, from the post-market surveillance system, on hazards and the frequency of occurrence thereof, on estimates of their associated risks, as well as on the overall risk, benefit-risk ratio and risk acceptability; and

(f) based on the evaluation of the impact of the information referred to in point (e), if necessary amend control measures in line with the requirements of Section 4.

Risk Management – in general

4. Risk control measures adopted by manufacturers for the design and manufacture of the devices shall conform to safety principles, taking account of the generally acknowledged state of the art. To reduce risks, Manufacturers shall manage risks so that the residual risk associated with each hazard as well as the overall residual risk is judged acceptable. In selecting the most appropriate solutions, manufacturers shall, in the following order of priority:

   (a) eliminate or reduce risks as far as possible through safe design and manufacture;

   (b) where appropriate, take adequate protection measures, including alarms if necessary, in relation to risks that cannot be eliminated; and

   (c) provide information for safety (warnings/precautions/contra-indications) and, where appropriate, training to users.

   Manufacturers shall inform users of any residual risks.

5. In eliminating or reducing risks related to use error, the manufacturer shall:

   (a) reduce as far as possible the risks related to the ergonomic features of the device and the environment in which the device is intended to be used (design for patient safety), and

   (b) give consideration to the technical knowledge, experience, education, training and use environment, where applicable, and the medical and physical conditions of intended users (design for lay, professional, disabled or other users).

Risk Management – in general

The manufacturer shall reduce the risks associated with the device **as far as possible by**

- Implementing a risk management system
- Developing a risk management plan for each device
- Evaluating risk associated with the device
- Taking the necessary action to reduce the risk
- Informing the users on residual risks

⇒ The concept of risk is central in the regulation, with the term **"risk"** appearing **234 times** in the document, emphasizing its importance in ensuring the safety and performance of medical devices.

Risk Management – permanent requirement

ISO 14155 Clinical Investigation	*IEC 62304* *MD Software Design*	ISO 11607 Packaging	
IEC 62366 Usability Engineering	IEC 60601 Medical Electric Equipment	EN 1041 Labelling / IFU	More risk-based standards..
ISO 13485 Quality Management	IEC 60601-2-x Medical Electric Equipment Pdt Requirements	ISO 10993 Biocompatibility	EN 556 Sterilization of Medical devices

ISO 14971
Risk Management

Risk Management – permanent requirement

ISO 13485

7.1 Planning of product realization

The organization shall document one or more processes for risk management in product realization. Records of risk management activities shall be maintained (see 4.2.5).

IEC 62304

4.2 * RISK MANAGEMENT

The MANUFACTURER shall apply a RISK MANAGEMENT PROCESS complying with ISO 14971.

IEC 62366

5.2 * Identify USER INTERFACE characteristics related to SAFETY and potential USE ERRORS

The MANUFACTURER shall identify USER INTERFACE characteristics that could be related to SAFETY as part of a RISK ANALYSIS performed according to ISO 14971:2007, 4.2. This

IEC 60601

4.2 * RISK MANAGEMENT PROCESS for ME EQUIPMENT or ME SYSTEMS

A RISK MANAGEMENT PROCESS complying with ISO 14971 shall be performed.

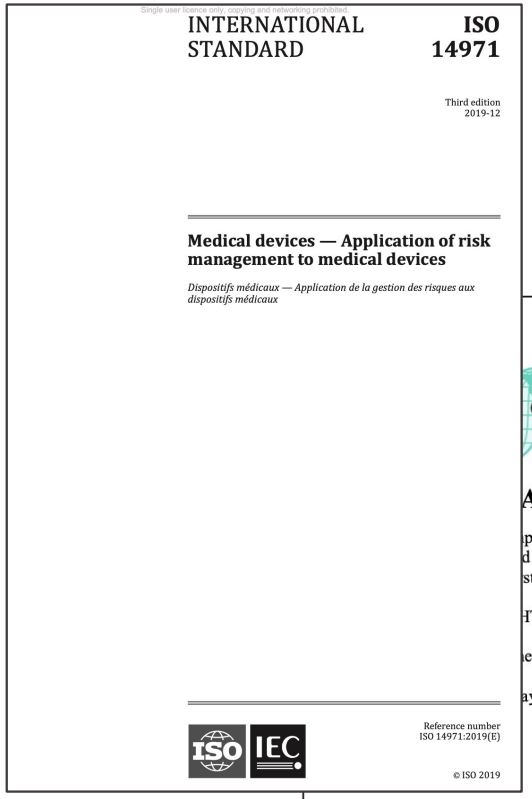
Risk Management – applicable guidance

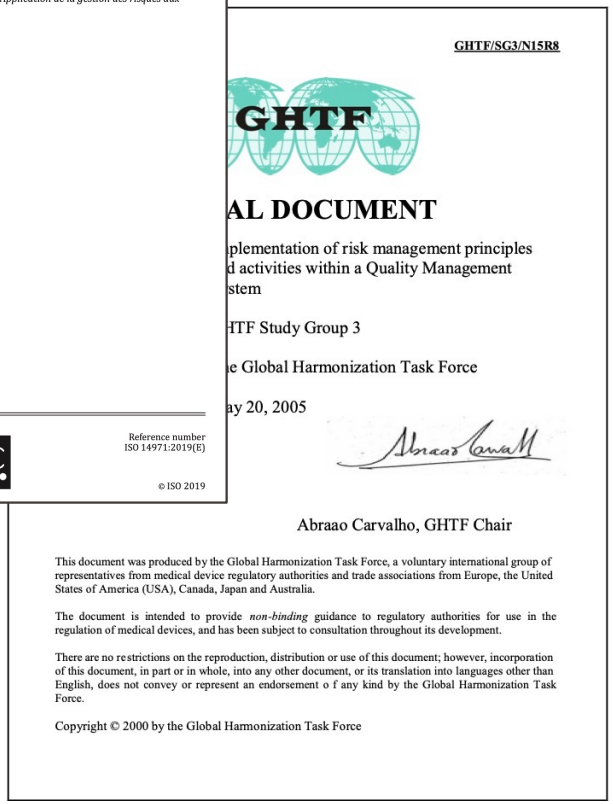
ISO 14971 - Medical devices — Application of risk management to medical devices

Provides a framework for manufacturers to identify, assess, control, and monitor risks throughout the entire lifecycle of a medical device.

GHTF/SG3/N15R8 – Implementation of risk management principles and activities within a QMS

Provides guidelines on integrating risk management principles into quality management systems for medical devices, focusing on identifying, evaluating, controlling, and monitoring risks throughout the device lifecycle to ensure safety and compliance with international standards.

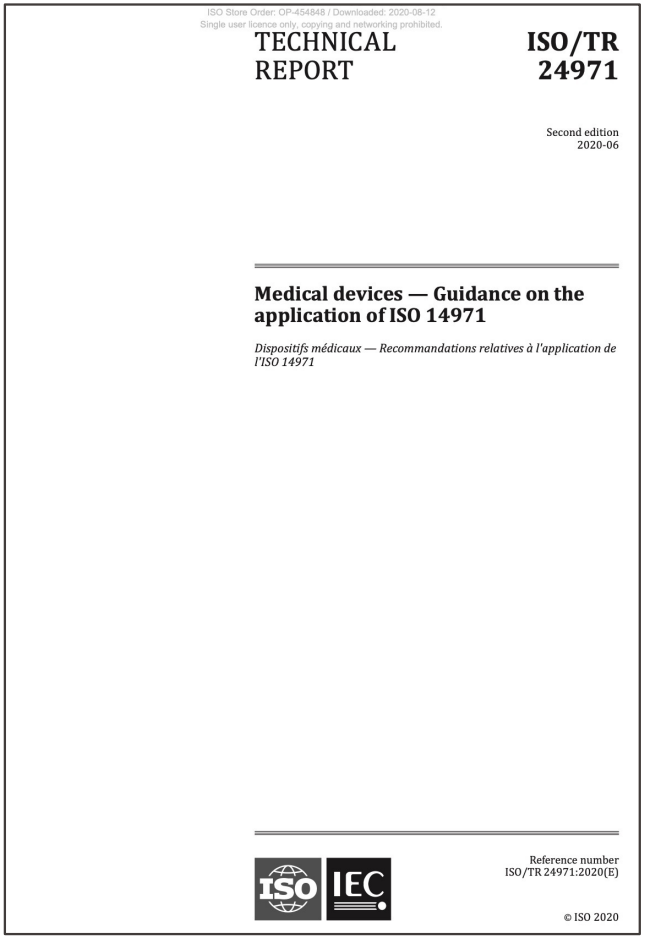




Risk Management – applicable guidance

ISO/TR 24971:2020 Guidance on the application of ISO 14971

provides comprehensive guidance on applying ISO 14971 for the risk management of medical devices, including risk analysis, evaluation, control measures, and post-market surveillance, ensuring compliance with regulatory requirements and best practices.



TECHNICAL REPORT

ISO/TR 24971

Second edition
2020-06

Medical devices — Guidance on the application of ISO 14971

Dispositifs médicaux — Recommandations relatives à l'application de l'ISO 14971

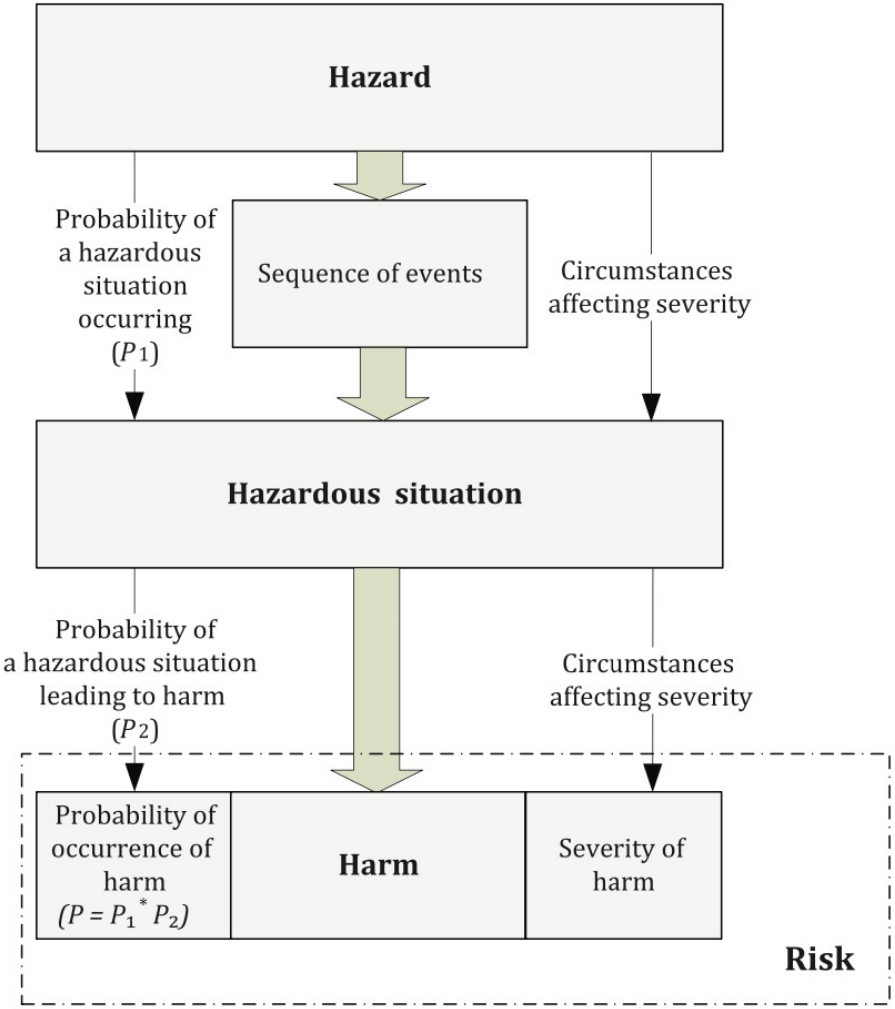
Reference number
ISO/TR 24971:2020(E)

Risk Management – definitions

Harm:	injury or damage to the health of people, or damage to property or the environment
Hazard:	potential source of harm
Hazard situation:	circumstance in which people, property or the environment is/are exposed to one or more hazards
Risk:	combination of the probability of occurrence of harm and the severity of that harm
Severity:	measure of the possible consequences of a hazard
Risk estimation:	process used to assign values to the probability of occurrence of harm and the severity
Risk analysis:	systematic use of available information to identify hazards and to estimate the risk
Risk control	process in which decisions are made and measures implemented by which risks are reduced

Source: ISO 14791:2019

Risk Management – Risk analysis concept



Kim Rochat

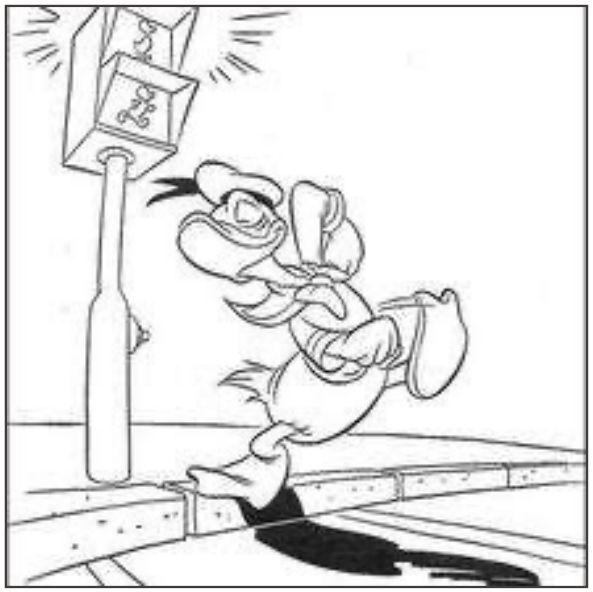
Risk Management – Risk analysis concept

Risk identification

Hazard

potential source of harm

Hazardous Situation



circumstance in which people, property or the environment is/are exposed to one or more hazards

Harm

injury or damage to the health of people, or damage to property or the environment

Risk Management – Risk analysis concept

Type of hazards

- **Physical Hazards**
  - Mechanical failure
  - Electrical shock or burns
- **Biological Hazards**
  - Infection risk
  - Toxicity from materials
- **Chemical Hazards**
  - Leaching of harmful substances
  - Reaction with body fluids or tissues
- **Software & Cybersecurity Hazards**
  - Malfunction due to software bugs or errors
  - Cybersecurity vulnerabilities
- **Ergonomic & Human Factors Hazards**
  - User interface design flaws
  - Complexity leading to misuse
- **Environmental Hazards**
  - Electromagnetic interference
  - Exposure to extreme environmental conditions
- **Functional Hazards**
  - Failure to deliver therapy
  - Incorrect dosing or measurement errors
- **Radiation Hazards**
  - Ionizing radiation exposure(e.g., X-ray, CT scan)
  - Non-ionizing radiation risks (e.g., ultrasound, MRI)
- **Social & Ethical Hazards**
  - Breach of patient confidentiality
  - Ethical concerns with AI decision-making

Risk Management – Risk analysis concept

Potential Harm Associated with Medical Devices

- **Physical Harm**
  - **Injury** (burns, electrical shocks, crushing injuries)
  - **Tissue damage** (implant migration, pressure sores, perforations)
  - **Fractures or muscle damage** (caused by orthopaedic implants or assistive devices)
  - **Radiation burns** (from overexposure to imaging or therapy devices)
- **Biological & Chemical Harm**
  - **Infection** (from contaminated devices, surgical implants, catheters)
  - **Allergic reactions** (to device materials, adhesives, coatings)
  - **Toxicity & poisoning** (from battery leaks, material degradation, drug-device interactions)
- **Psychological & Emotional Harm**
  - **Severe anxiety or distress** (due to device malfunction, misdiagnosis, or fear of failure)
  - **Reduced quality of life** (chronic pain, discomfort, or reliance on malfunctioning devices)
  - **Psychological trauma** (from permanent injury, disability, or incorrect treatment outcomes)
- **Data & Cybersecurity-Related Harm**
  - **Privacy violations** (unauthorized disclosure of sensitive medical data)
  - **Medical identity theft** (leading to financial fraud or incorrect medical records)

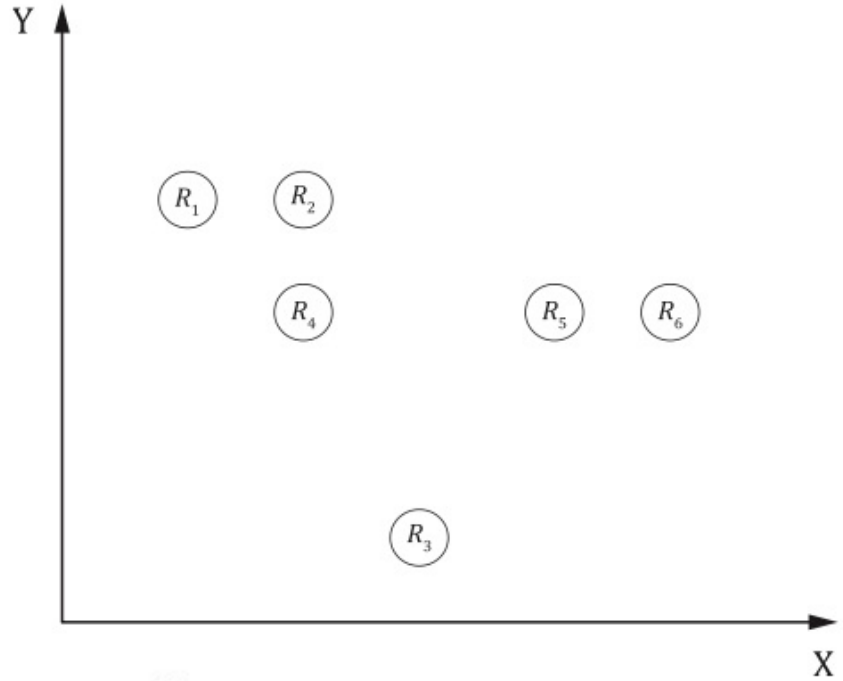
Risk Management – Risk analysis method

Risk estimation

Various methods can be used to estimate risk, for example:

- the circumstances in which a hazard is present;
- the sequence of events leading to a hazardous situation;
- the probability of a hazardous situation occurring;
- the probability of a hazardous situation leading to harm;
- the nature of the harm that could result.

Risk should be expressed in terms that facilitate decision making on risk acceptability and the need for risk control, for example, using severity and probability scales.



Key

X probability of occurrence of *harm*

Y *severity* of *harm*

Source: ISO 24971:2020

Risk Management – Risk analysis method

Risk = ***probability of occurrence (P)*** *of harm x* ***severity (S)*** *of that harm*

Hazard: sharp blade

Hazardous Situation: attach blade to holder

Harm: patient is cut

Risk = P_1 X P_2 X Severity

P_1 *is probability of hazardous situation occurring*

P_2 *is probability of hazardous situation leading to harm*

Often P is used which integrates directly $P_1 x P_2$

Risk Management – Risk analysis method

In risk analysis, probability refers to the **likelihood** that a hazardous event will occur and lead to harm.

Quantitative Probability

- Expressed in numerical values (e.g., percentages, failure rates, statistical models).
- Often derived from historical data, reliability testing, or failure mode analysis.

Failure Mode: Battery failure in an external defibrillator.
Observed Failure Rate: **1 in 10,000 uses** or **0.01%** of the use

Qualitative Probability

- Expressed in descriptive terms (e.g., rare, unlikely, possible, frequent).
- Used when numerical data is unavailable or insufficient.

Failure Mode: Battery failure in an external defibrillator.
Qualitative Probability: **Remote** (very rare, but still possible).

Risk Management – Risk analysis method

Quantitative vs Qualitative Probability

Qualitative Probability	Quantitative Probability	Description	Example in Medical Devices
Frequent	>1 in 10 (>10%)	Expected to occur regularly	Sensor failure in a wearable heart monitor happens often.
Probable	1 in 100 (1%)	Likely to occur over time	Battery failure in an infusion pump is likely over its lifetime.
Occasional	1 in 1,000 (0.1%)	Possible, but uncommon	A ventilator software error can happen, but it is rare.
Remote	1 in 10,000 (0.01%)	Very rare, but still possible	MRI machine emitting excessive RF energy is very unlikely.
Improbable	1 in 1,000,000 (0.0001%)	Extremely unlikely, almost negligible	Pacemaker total electronic failure is almost impossible.

Risk Management – Risk analysis method

Severity in risk analysis refers to the **degree of harm** or **impact** that a hazardous event can cause when it occurs.

- **Patient Harm & Health Impact**
  - The potential harm to a patient can range from **minor discomfort** (low severity) to **life-threatening injury or death** (high severity).

  Example: A mild skin irritation caused by a medical adhesive is a **low severity** injury, while organ failure due to a malfunctioning pacemaker is a **high severity** outcome.

- **Clinical Outcome & Treatment Delay**
  - Device failure can cause delays in diagnosis or therapy, leading to a worsening of the patient's health condition. The severity depends on how critical the delay is to the clinical outcome, ranging from **slight delays with minimal effect** (low severity) to **delayed life-saving interventions** (high severity).

  Example: A slight delay in a diagnostic test result causing a minor inconvenience to the patient is **low severity**, while a delayed diagnosis of a serious illness like cancer that worsens the patient's prognosis is **high severity**.

Risk Management – Risk analysis method

- **Damage to the Device**
  - Physical or functional damage to the device can range from **minor cosmetic damage** (low severity) to a **total failure of critical device functions** (high severity).

  Example: A cosmetic scratch on the surface of a medical device is a **low severity** issue, while a total failure of a defibrillator during use, leading to a patient's death, is a **high severity** event.

- **Privacy Breach**
  - The severity of a privacy breach is determined by the extent and sensitivity of the exposed data, ranging from **minimal exposure** of non-sensitive information (low severity) to **extensive leakage of highly sensitive data** (high severity).

  Example: The exposure of a patient's name and general information due to a breach is **low severity**, whereas the unauthorized release of detailed medical records, including personal health information, is a **high severity** breach.

Risk Management – Risk analysis concept

Severity levels

Severity Level	Description	Example
Negligible	No injury, no significant harm.	A minor software glitch in a fitness tracker.
Minor	Temporary discomfort, no medical treatment needed.	Slight skin irritation from an adhesive bandage.
Serious	Requires medical intervention, possible long-term effects.	Defective insulin pump delivering incorrect dosage.
Critical	Life-threatening or permanent injury.	Ventilator failure leading to respiratory distress.
Catastrophic	Death or severe disability.	Pacemaker malfunction causing cardiac arrest.

Risk Management – Risk analysis concept

Definition of probability and severity scale for my risk analysis

Severity Level	Factor (score)
Negligible	1
Minor	2
Serious	3
Critical	4
Catastrophic	5

Probability Level	Quantitative Probability
Improbable	1
Remote	2
Occasional	3
Probable	4
Frequent	5

Risk = Probability X Severity

Kim Rochat

Risk Management – Risk analysis concept

Risk = Probability X Severity

	Severity (S)				
Probability of Occurrence (O)	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very high (5)
Improbable (1)	1	2	3	4	5
Remote (2)	2	4	6	8	10
Occasional (3)	3	6	9	12	15
Probable (4)	4	8	12	16	20
Frequent (5)	5	10	15	20	25

⇒ **frequent risk with a moderate severity = Level of 15**

Risk Management – Risk analysis concept

Definition of risk acceptability

Risk Level	Common Terms	Interpretation
RL ≥ 10	Unacceptable risk	Risks too severe to be accepted. A risk above this limit shall be reduced through mitigation measure(s) or risk control(s).
10 > RL > 4	Significant risk	The risks in this range are deemed acceptable, only if the reduction is not technically possible. If the risk may be reduced, then a mitigation measure or a risk control shall be implemented. Risk can be acceptable only with a favourable Risk/Benefit ratio.
4 ≥ RL	Acceptable risk	Risk is acceptable. It represents the low-risk area where a mitigation measure would not result in significant risk reduction. When this level is achieved during initial evaluation, if possible, it should be further mitigated. This status is when the risk is reduced As Far As possible

Example of risk acceptability level

Kim Rochat

Risk Management – Risk analysis concept

Risk evaluation

Risk Identification				Initial risk level		
ID #	Cause / Failure Mode	Hazardous situation / effect(s) of failure	Harm / Damage	S	P	Score
1	The glue selected for the medical adhesive is not biocompatible	The glue is absorbed by the skin provoking an allergic reaction	Mild skin irritation	2	4	8
2	Battery of the external defibrillator is not certified for the define used	The battery explode when defibrillator at maximum power	Sever injury to patient and medical personnel	5	3	15

⇒ My risk 1 has a level of 10, it is a Significant risk

⇒ My risk 2 has a level of 15, it is unacceptable

Q&A