

# Risk Management from a Quality Standards Perspective

Alexander Crosby



- Increases the likelihood of achieving objectives
- Encourage proactive management
- Improve the identification of opportunities and threats
- Improve mandatory and voluntary reporting
- Improve governance & controls
- Establish a reliable basis for decision making and planning
- Improve operational effectiveness and efficiency
- Enhance health and safety performance, as well as environmental protection
- Improve loss prevention and incident management & minimize losses
- **Comply with relevant legal and regulatory requirements**

(ISO 31000:2009)

“...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**. (MDD annex 1, item 1)

“A medical device shall be designed and manufactured to be safe...the manufacturer shall...take reasonable measures **to identify the risks** inherent in the device; if the risks can be eliminated, **eliminate** them; if the risks cannot be eliminated, **reduce** the risks to the extent possible, **provide for protection** appropriate to those risks, including the provision of alarms, and provide, with the device, **information** relative to the risks that remain; and minimize the hazard from potential failures....” (SOR/98-282 10)

“Each manufacturer shall establish and maintain procedures for validating the device design. Design validation shall include... **risk analysis**.... “(CFR 820.30 Design Controls)



“The organization shall establish documented requirements for **risk management** throughout product realization.”

(ISO 13485:2003)

”A **risk management process** complying with ISO 14971 shall be performed.”

(IEC 60601-1 3<sup>rd</sup> edition)



## Risk Management Standards

- ISO 31000:2009: Risk management: Principles & guidelines
- ISO 14971:2009: Application of risk management to medical devices

## Standards that reference Risk Management

- ISO 13485:2003: Medical devices quality management systems
- IEC 60601-1 (3<sup>rd</sup> edition): Medical equipment medical electrical equipment - General requirements for basic safety and essential performance

## Regulatory Requirements for Risk Management

- FDA's Quality System Regulation (21 CFR 820)
- Canadian Medical Device Regulations (SOR/98-282)
- EU Medical Device Directive (93/42/EEC)

# ISO 31000: Risk management: Principles & guidelines



Valued Quality. Delivered.

- Grew out of Australia/New Zealand standards for risk management & corporate governance.
- Enterprise risk management – not industry specific
- Risk is effect of uncertainty on organization's objectives
- Risk is neutral – the effect can be positive and negative
- Risk = combination of the consequences of an **event** and the associated likelihood of **occurrence**.
- Risk Management: The culture, processes, and structures that are directed towards the effective management of potential opportunities and adverse effects

- Medical device specific
- ISO 14971 is a guidance document and a voluntary standard, but is “generally acknowledged state of the art” and integrated into other standards & recognized by regulatory agencies
- Risk is negative and expressed in terms of health & safety
- Risk = combination of the consequences of a **hazard** and the associated likelihood of occurrence (**harm**).
  - Single class of objective – safe, effective device
- Risk Management: The culture, processes, and structures that are directed towards the effective management of adverse effects

## Common -

- RM framework, policy, plan, process, etc.
- Risk source, identification, assessment,, analysis, etc.
- Tools

## 31000 -

- Risk attitude – org’s approach to assess, pursue, retain, take or turn away from risk
- Risk owner – accountable and authorized to manage a risk
- Internal & external contexts – environment in which organization seeks to achieve objectives

## 14971 -

- Device related terms: patient, clinician, intended use, etc.
- Risk File

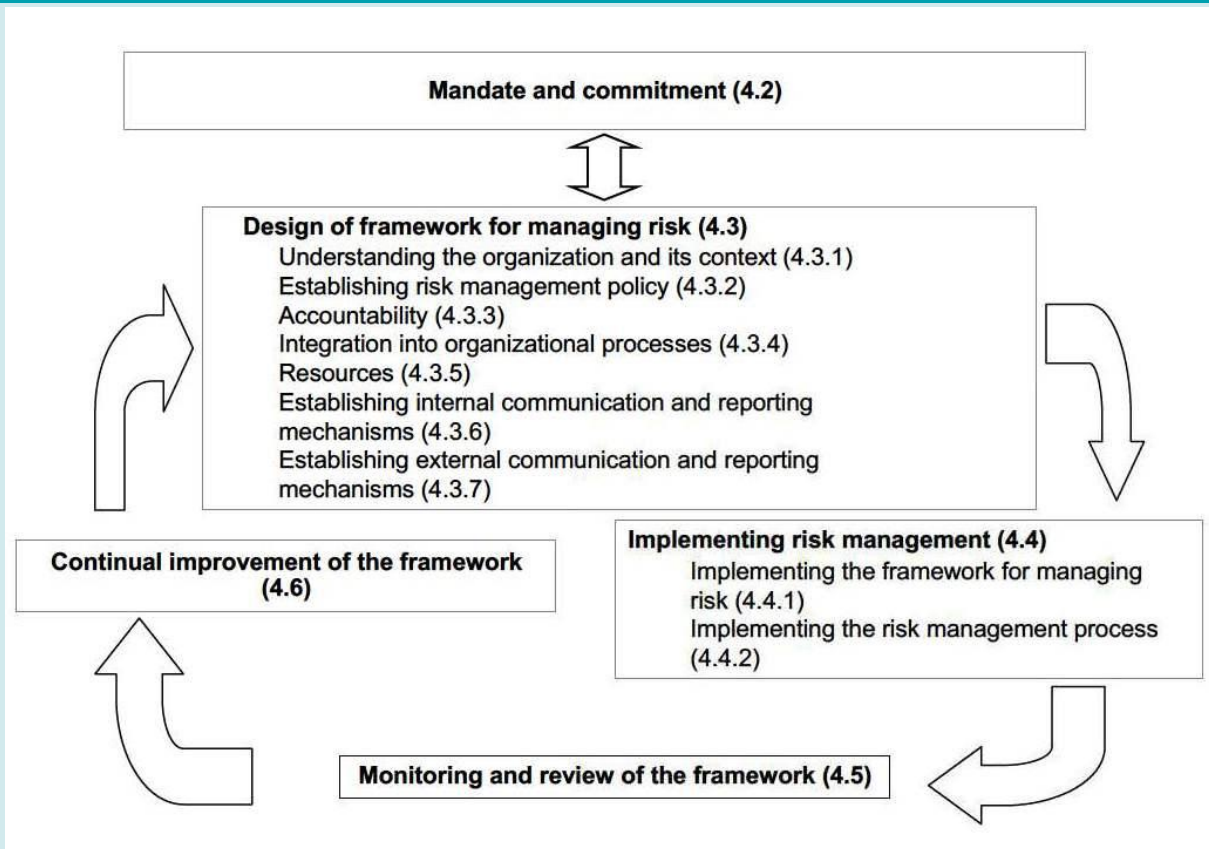


## Risk management

- creates and protects value
- is an integral part of all organizational processes
- is part of decision making
- explicitly addresses uncertainty
- is systematic, structured and timely
- is based on the best available information
- is tailored
- takes human and cultural factors into account
- is transparent and inclusive
- is dynamic, iterative and responsive to change
- facilitates continual improvement of the organization

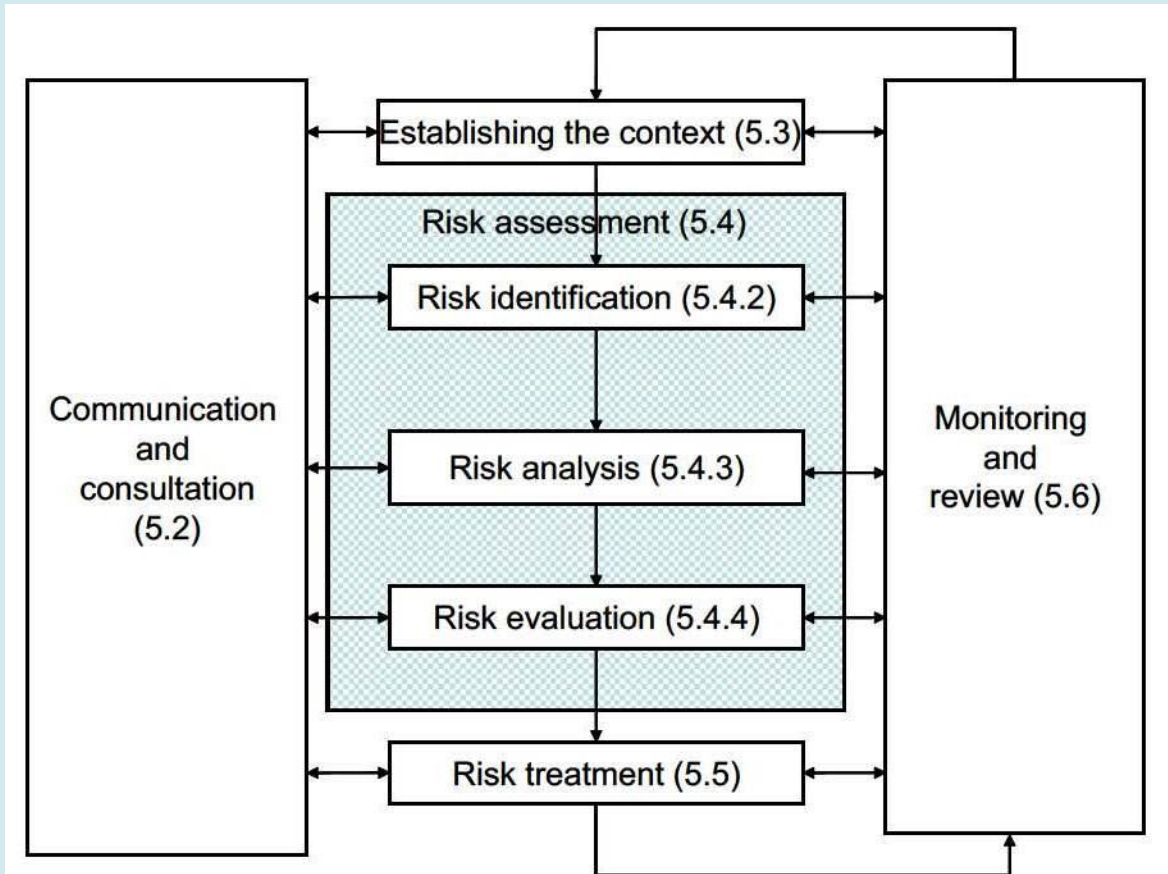
## ISO 31000

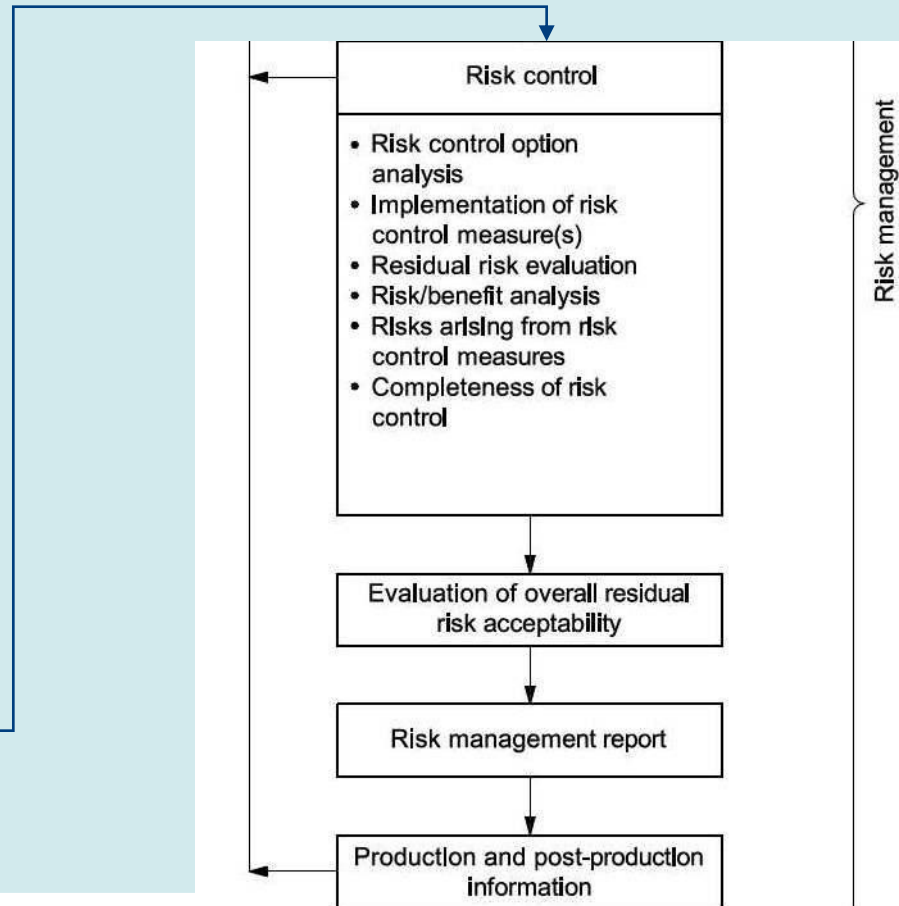
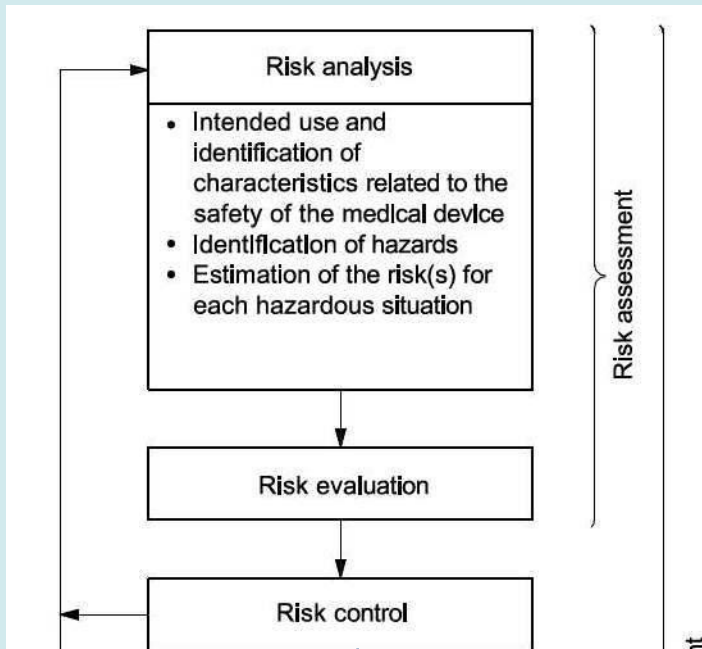
## ISO 14971



## QMS (QSR/ISO 13485)

- General
- Management Responsibility
- Resources
- Product Realization
  - Purchasing
  - Design & development
- Measurement, Analysis & Improvement
  - Audit
  - Corrective Actions
  - Improvement





## Process, Plan & File

## ISO 14971 3.2 Management Responsibility

Top management shall provide evidence of its commitment to the risk management process by:

- provision of adequate resources
- the assignment of qualified personnel
- define risk policy

## ISO 31000 4.2 Mandate and commitment

The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained. commitment by management of the organization. Management should

- assign accountabilities and responsibilities at appropriate levels within the organization
- ensure that the necessary resources are allocated to risk management
- Define risk policy



## ISO 14971 3.2 Management Responsibility

Management shall “document the policy for determining criteria for risk acceptability” taking into account

- National and regional regulations
- Relevant international standards
- Generally accepted state of the art
- Known stakeholder concerns: Patient, clinical user, manufacturer, supplier, employee, community

## ISO 31000

### 4.3.1 – Understanding of the organization and its context

- Internal factors: Governance, objectives, risk tolerance, culture, etc.
- External factors: Social, cultural, legal, regulatory, stakeholders, etc.

### 4.3.2 – Establish risk policy

### 5.2. – Communication & consultation

### 5.3 – Establishing the context: define risk criteria

# Medical Device Risk Management Policy: Example

## Risk acceptance criteria sources:

- The intended use of the medical device
- The requirements of relevant national and regional regulations
- Input from international standards
- Input from technical, scientific and clinical experts
- Input from the stakeholders, foremost being the patient.

## The organization's risk acceptability policy is the following:

- Generally acceptable – the organization will address risks through professional and patient information via IFU, website and clinical training.
- “Moderate” & “severe” - the organization has a “an as-low-as reasonably-practicable approach.
- If after “ALARP,” there are risks that are still deemed “severe,” then the organization will perform a risk/benefit analysis and determine whether the risk can be accepted or product changes are required.
- If the overall residual risk exceeds the acceptability criteria, a device risk/benefit analysis, which employs input from objective and knowledgeable clinical professionals, will be performed, and a determination made whether the overall residual risk can be accepted.



# Application of Risk Policy: Generation of Risk Acceptance Criteria



Valued Quality. Delivered.

MedCo has developed a new tissue cardiac valve product. Below please find our risk policy and risk acceptance criteria, along with the sources of these criteria. The MedCo tissue cardiac valve must meet all the following risk acceptance criteria.

## Intended Use (Source: MedCo)

MedCo's tissue valve heart is a tissue engineered valve replacement device for aortic replacements, with the following parameters.

- Tissue Annulus Diameter (TAD): 8.5 mm
- Valve Outer Diameter (OD): 27.5 mm
- Durability & Fatigue: The valve must pass durability and fatigue testing via accelerated wear testing (AWT) methods and meet the requirement for 600 million cycles for rigid valves and 200 million cycles for flexible valves, using a back pressure between 125 and 150 mmHg.





### Stakeholders

A review of forums dedicated to user issues, including the following sources, generated the following risk acceptance criteria: American Heart Foundation, Valvreplacement.org & Ehealthforum.com

### Risk Acceptance Criteria:

- The device must have a shelf life of 1 year.
- The device must be able to remain viable and sterile in transit (up to 12 hours).
- Services associated with device must include professional education and this education should take no longer than 4 hours of non-operating room time.





No risk management policy

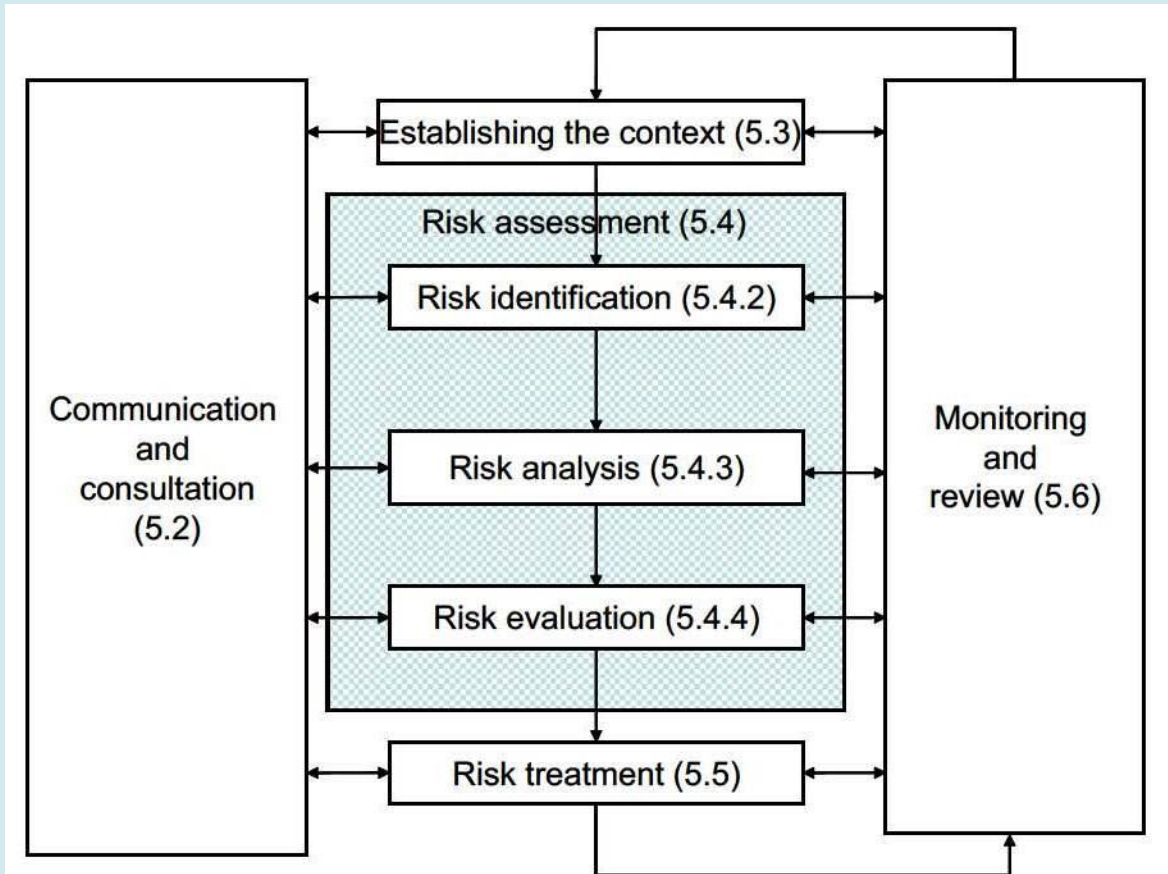
Policy is “ALARP.”

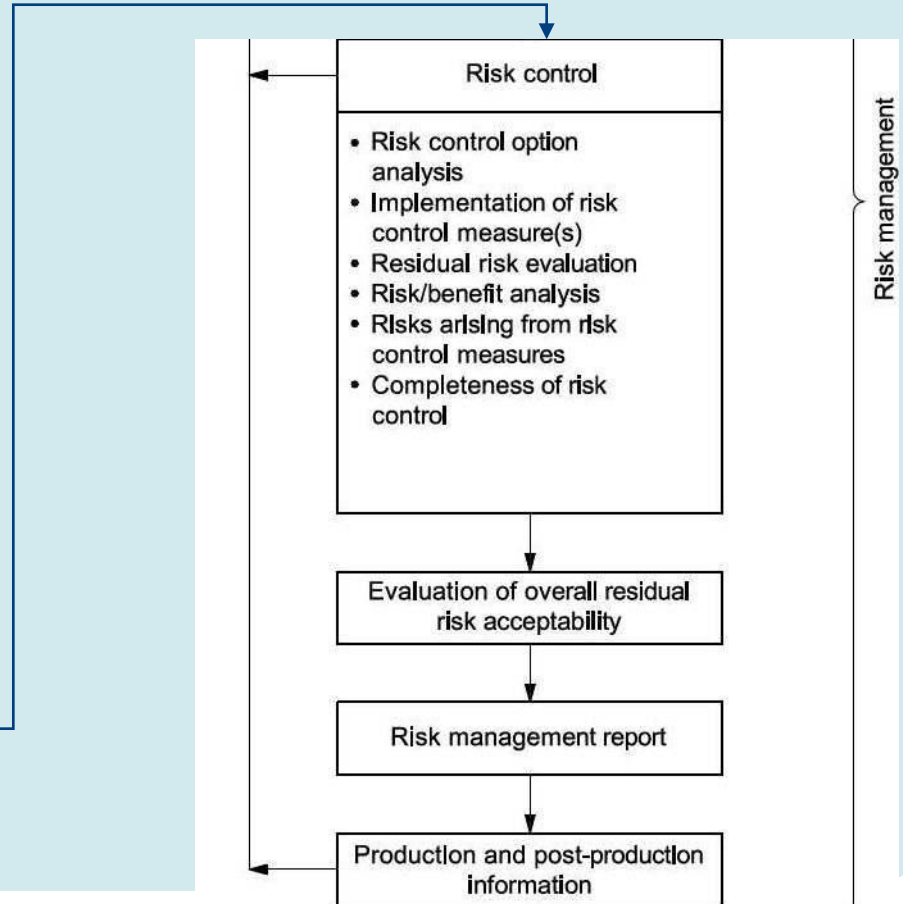
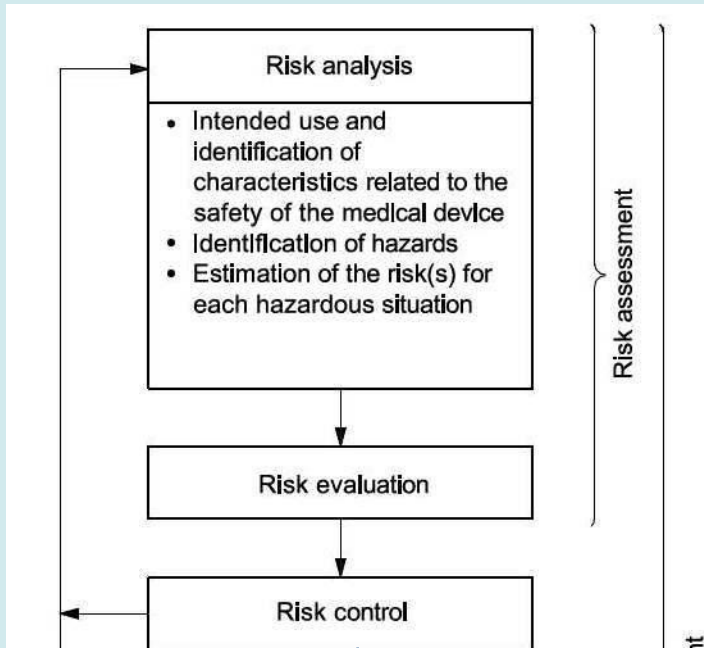
Policy is:

		Qualitative severity levels				
		Negligible	Minor	Serious	Critical	Catastrophic
Semi-quantitative probability levels	Frequent					
	Probable	$R_1$	$R_2$			
	Occasional		$R_4$		$R_5$	$R_6$
	Remote					
	Improbable			$R_3$		

**Key**

	unacceptable risk
	acceptable risk





## ISO 31000

## ISO 14971

Risk Assessment (5.4)

Risk Identification (5.4.2)

Risk Analysis (5.4.3)

Risk Evaluation (5.4.4)

Risk Treatment (5.5)

- avoiding the risk not by not starting/continuing
- taking/increasing the risk to pursue opportunity
- removing the risk source
- changing the likelihood
- changing the consequences
- sharing the risk with another party or parties (including contracts and risk financing)
- retaining the risk by informed decision.

Post Risk Control Process

Risk Analysis (4.0)

Identification of hazards (4.3)

Estimation of the risk (4.4)

Risk Evaluation (5.0)

Risk Control (6.0)

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

Evaluation of overall residual risk

Post Risk Control Process

- 14971 Common issues and deficiencies
  - Choice of tools: FMEA vs. others
  - 4.2 “Reasonably foreseeable misuse” vs. user error
  - 4.4 The systems used for the quantitative or qualitative categorization of probability should be recorded
  - 4.4 Use of available information to estimate risk: Variety and documentation of information sources
  - Priority of risk controls –
    - Inherent safe design
    - Protective measures
    - Information for safety
  - Verification of the implementation & effectiveness of risk controls (which can include validation)



- Per risk: Residual risk review & risk/benefit analysis (if required)
- Risks arising from risk controls: Documentation of this review
- Completeness of risk controls: Documentation of this activity
- Evaluation of overall risk: Documentation of Review & Risk/benefit analysis (if required)
- Risk management plan updated prior to release with a review of RM process to ensure RMP has been appropriately implemented;
  - Overall residual risk is acceptable;
  - Mechanisms to gather production/post-production information are in place
- Review Risk File for “completeness of risk controls”



## ISO 31000

- Monitor & Review (5.6)
- Recording (5.7)

## ISO 14971

- Risk Management Report (8.0)
- Production & Post-Production (9,0)



## ISO 14971 9 Production and post-production

Collect and review information about the device and similar devices in production and post-production phases

## ISO 13485 7 Purchasing, Customer-Related, Monitoring & Measurement - “Throughout the lifecycle”

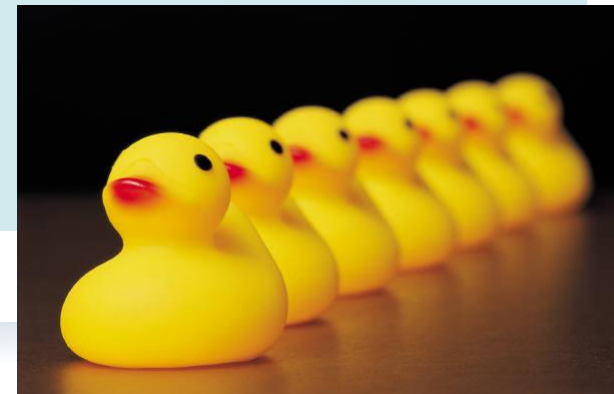
- Are these processes established?
- Are they integrated with processes for CAPA, complaints and MDD clinical and non-post-market surveillance?
- Integrated findings: “...including provisions for risk management.”
- What actions arise from the review?
  - New risks or changes the severity and probability of known risks
  - Changes to risk controls
  - Changes to risk acceptance criteria



- Risk policy
- Risk Management Plan
  - Activities
  - Responsibilities and authorities
  - Requirements for review
  - Criteria for risk acceptance per the risk policy
  - Verification Activities
- Risk analysis
- Risk evaluation
- Implementation and verification of the risk controls
- Assessment of residual risk
- Risk Management report
- Post-production information



- What are the requirements – supplier vs. medical manufacturer
- How are the risk management systems and the quality management systems related?
  - Range from standalone to fully integrated
  - What are the interfaces between the systems?
  - GHTF/SG3/N15R8: Implementation of risk management principles & activities within a Quality Management System
- Has the organization adopted a risk management standard?
- Was the implementation planned, and how is it maintained?
  - Resources: People, tools, systems, time
  - Training: Methods, tools, standards, etc.



## ISO 14971 3.2 Management Responsibilities

Management shall review the suitability and effectiveness of the risk management process.

- Is this meeting part of a documented process? Is it part of Management Review?
- Is there consideration of management's knowledge of risk and risk related tools and systems?
- Is Management "risk literate."
- What risk information is management reviewing?
- How is suitability being determined?
- Is RMS effectiveness being determined? How?
- Can effectiveness be determined by presence (or absence) of post-production issues?



## Reviewing for Suitability and Effectiveness (cont)

- Does your organization's risk management system actually manage risk?
- Identify?
  - Throughout the organization?
  - Throughout the lifecycle?
- Classify? Mitigate? Communicate?
- Does the RMS system produce an accurate record of the organization's due diligence?
- Does it protect the organization and its stakeholders?



## Contact Information

Alexander Crosby

Lead Auditor, Medical Devices

Business Assurance

Intertek

434 242 4341

[alexander.crosby@intertek.com](mailto:alexander.crosby@intertek.com)

