Risk Management

SCSD 11th March 2024
Introduction

This document is for use by people who create and protect value in organizations by managing risks, making decisions, setting and achieving objectives and improving performance.

Organizations of all types and sizes face external and internal factors and influences that make it uncertain whether they will achieve their objectives.

Managing risk is iterative and assists organizations in setting strategy, achieving objectives and making informed decisions.

Managing risk is part of governance and leadership, and is fundamental to how the organization is managed at all levels. It contributes to the improvement of management systems.

Managing risk is part of all activities associated with an organization and includes interaction with stakeholders.

Managing risk considers the external and internal context of the organization, including human behaviour and cultural factors.

Managing risk is based on the principles, framework and process outlined in this document, as illustrated in Figure 1. These components might already exist in full or in part within the organization, however, they might need to be adapted or improved so that managing risk is efficient, effective and consistent.
Clauses 4, 5 and 6 – Main elements of 31000

Figure 1 — Principles, framework and process
Definitions

- **risk**: effect of uncertainty on objectives
- **risk management**: coordinated activities to direct and control an organization with regard to risk
- **stakeholder**: person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity
- **risk source**: element which alone or in combination has the potential to give rise to risk
- **event**: occurrence or change of a particular set of circumstances
- **consequence**: outcome of an event affecting objectives
- **likelihood**: chance of something happening
- **control**: measure that maintains and/or modifies risk
ISO 31000 Principles (Clause 4)

a) **Integrated:** Risk management is an integral part of all organizational activities. 

b) **Structured and comprehensive:** A structured and comprehensive approach to risk management contributes to consistent and comparable results.

c) **Customized:** The risk management framework and process are customized and proportionate to the organization’s external and internal context related to its objectives.

d) **Inclusive:** Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.

e) **Dynamic:** Risks can emerge, change or disappear as an organization’s external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.
ISO 31000 Principles (Clause 4)

f) **Best available information:** The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.

g) **Human and cultural factors:** Human behaviour and culture significantly influence all aspects of risk management at each level and stage.

h) **Continual improvement:** Risk management is continually improved through learning and experience.
ISO 31000 Framework (Clause 5)

- Leadership and commitment are the key elements to ensure:
  - Risk management is integrated into all activities
  - Aligned to the needs of the organization and pursued systematically and engages with all in the organization
  - Top management is accountable for the management of risk and oversight bodies oversee risk management
Integration of Risk Management

- Risk management takes place in all parts of an organization
- Risk management should be incorporated into governance of the organization
- Management structure translates governance into objectives and strategies
- Risk management accountability and oversight roles are a key part of governance
- Integration is iterative, dynamic and ongoing.
Design of the risk management framework

- Understanding the organization and its internal and external context.
- Commitment to articulating risk management.
- Assigning organizational roles, authorities, responsibilities and accountabilities.
- Allocating resources.
- Establishing communication and consultation
Integration, Evaluation, Improvement

• Implementation:
  • Plans that include timing and resources
  • Identifying roles – where, when, how, and by whom different types of decision are taken
  • Processes are well defined and aligned with risk management.

• Evaluation:
  • is the risk management framework good at managing risk? (How to measure?)
  • Decide if it is still fit for purpose in supporting business objectives

• Improvement:
  • Adapting to take account of internal and external change
  • Continually improving to strengthen risk management
ISO 31000: Process (Clause 6)

- Communication and consultation: good risk management need to bring people and information from across the organization.

- Scope, context, criteria: frames risk assessment by establishing what risk assessment is supposed to be doing, where it comes from and how to decide on how serious a risk is.
Risk Identification

• Finding risks
• Look for uncertainties and the different possibilities arising from these.
• Use techniques like SWOT (Strengths, Weaknesses, Opportunities, Threats) to evaluate the organization and identify uncertainty.
• Possible internal and external events should be identified and their consequences outlined, ...
Risk Analysis

• Refine the analysis of risks
• Estimate likelihood of events
• Estimate the consequences of events
• Explore complexity and connectivity of the collection of risks
• Explore timing and volatility
• Estimate sensitivity to change and confidence in estimates
• Estimate the effectiveness of existing controls
Risk Evaluation

• Support decisions with recommendations:
  • No further action
  • Consider risk treatment options
  • Do additional analysis
  • Maintain existing controls
  • Reconsider the risk management objective for this class of risk
Risk Treatment

• Overall: consider treatment options, plan and implement treatment, assess effectiveness, decide if further treatment is necessary.

• Treatment options:
  • Avoid the risk by not doing the risky activity.
  • Deciding the risk/opportunity balance justifies the risk
  • Changing the risk by removing the source; changing likelihood, changing consequences OR deciding the risk is acceptable.

• Preparing and implementing risk treatment plans
  • Explain the plan, who is responsible for approving and implementing
  • Actions, resources, performance measures, constraints, reporting and measurement, timing
Monitoring, review, recording, reporting

- Establish indicators and expected values
- Establish mechanisms to collect indicator values
- Review against expected values and implement change if risk management needs improvement.
- Establish a reporting framework and what will be reported and how this is retained and acted on.
ISO 31000 is Generic

- This covers all types of risk.
- ISO 14971 is specifically about the management of risk in Medical Devices
- ISO 14971 is more specific both in context and process
ISO 14891: Risk Management of Med Devices

• Oriented towards manufacturers.
• Aiming at controlling hazards by assessing probability of occurrence and severity.
Hazards can be exemplified

<table>
<thead>
<tr>
<th>Energy hazards</th>
<th>Biological and chemical hazards</th>
<th>Performance-related hazards</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Acoustic energy</strong></td>
<td>Biological agents</td>
<td>Data</td>
</tr>
<tr>
<td>— infrasound</td>
<td>Bacteria</td>
<td>— access</td>
</tr>
<tr>
<td>— sound pressure</td>
<td>Fungi</td>
<td>— availability</td>
</tr>
<tr>
<td>— ultrasonic</td>
<td>Parasites</td>
<td>— confidentiality</td>
</tr>
<tr>
<td><strong>Electric energy</strong></td>
<td>Prions</td>
<td>— transfer</td>
</tr>
<tr>
<td>Electric fields</td>
<td>Toxins</td>
<td>— integrity</td>
</tr>
<tr>
<td>Leakage current</td>
<td>Viruses</td>
<td><strong>Delivery</strong></td>
</tr>
<tr>
<td>— earth leakage</td>
<td><strong>Chemical agents</strong></td>
<td>— quantity</td>
</tr>
<tr>
<td>— enclosure leakage</td>
<td>Carcinogenic, mutagenic, reproductive</td>
<td>— rate</td>
</tr>
<tr>
<td>Magnetic fields</td>
<td>Caustic, corrosive</td>
<td><strong>Diagnostic information</strong></td>
</tr>
<tr>
<td>Static discharge</td>
<td>— acidic</td>
<td>— examination result</td>
</tr>
<tr>
<td>Voltage</td>
<td>— alkaline</td>
<td>— image artefacts</td>
</tr>
<tr>
<td><strong>Mechanical energy</strong></td>
<td>— oxidants</td>
<td>— image orientation</td>
</tr>
<tr>
<td>Kinetic energy</td>
<td>Flammable, combustible, explosive</td>
<td>— image resolution</td>
</tr>
<tr>
<td>— falling objects</td>
<td>Fumes, vapors</td>
<td>— patient identity / information</td>
</tr>
<tr>
<td>— high pressure fluid injection</td>
<td>Osmotic</td>
<td><strong>Functionality</strong></td>
</tr>
<tr>
<td>— moving parts</td>
<td>Particles (including micro- and nanoparticles)</td>
<td>— alarm</td>
</tr>
<tr>
<td>— vibrating parts</td>
<td>Pyrogenic</td>
<td>— critical performance</td>
</tr>
<tr>
<td><strong>Potential (stored) energy</strong></td>
<td></td>
<td>— measurement</td>
</tr>
</tbody>
</table>
Sequence of Events can be exemplified

<table>
<thead>
<tr>
<th>General category</th>
<th>Events and circumstances</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td>Inadequate specification of:</td>
</tr>
<tr>
<td></td>
<td>— design parameters</td>
</tr>
<tr>
<td></td>
<td>— operating parameters</td>
</tr>
<tr>
<td></td>
<td>— performance requirements</td>
</tr>
<tr>
<td></td>
<td>— in-service requirements (e.g. maintenance, reprocessing)</td>
</tr>
<tr>
<td></td>
<td>— end of life</td>
</tr>
<tr>
<td>Manufacturing processes</td>
<td>Insufficient control of:</td>
</tr>
<tr>
<td></td>
<td>— manufacturing processes</td>
</tr>
<tr>
<td></td>
<td>— changes to manufacturing processes</td>
</tr>
<tr>
<td></td>
<td>— materials</td>
</tr>
<tr>
<td></td>
<td>— materials compatibility information</td>
</tr>
<tr>
<td></td>
<td>— subcontractors</td>
</tr>
<tr>
<td>Transport and storage</td>
<td>Inadequate packaging</td>
</tr>
<tr>
<td></td>
<td>Contamination or deterioration</td>
</tr>
<tr>
<td></td>
<td>Inappropriate environmental conditions</td>
</tr>
</tbody>
</table>
### Table C.3 — Relationship between hazards, foreseeable sequences of events, hazardous situations and the harm that can occur

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Foreseeable sequence of events</th>
<th>Hazardous situation</th>
<th>Harm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electromagnetic energy (high voltage)</td>
<td>(1) Electrode cable unintentionally plugged into power line receptacle</td>
<td>Line voltage appears on electrodes</td>
<td>Serious burns. Heart fibrillation</td>
</tr>
<tr>
<td></td>
<td>(2) Solvent residue converts to gas at body temperature</td>
<td>Development of gas embolism (bubbles in the bloodstream) during dialysis</td>
<td>Infarct. Brain damage</td>
</tr>
<tr>
<td>Chemical (volatile solvent, embolus)</td>
<td>(1) Incomplete removal of volatile solvent used in manufacturing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(2) Solvent residue converts to gas at body temperature</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biological (microbial contamination)</td>
<td>(1) Inadequate instructions provided for decontaminating re-used anaesthesia tubing</td>
<td>Bacteria released into airway of patient during anaesthesia</td>
<td>Bacterial infection</td>
</tr>
<tr>
<td></td>
<td>(2) Contaminated tubing used during anaesthesia</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Functionality (no delivery)</td>
<td>(1) Electrostatically charged patient touches infusion pump</td>
<td>Failure to deliver insulin to patient with elevated blood glucose level, no warning given</td>
<td>Minor organ damage. Decreased consciousness</td>
</tr>
<tr>
<td></td>
<td>(2) Electrostatic discharge (ESD) causes pump and pump alarms to fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Functionality (no output)</td>
<td>(1) Implantable defibrillator battery reaches the end of its useful life</td>
<td>Defibrillator cannot deliver shock when an arrhythmia occurs</td>
<td>Death</td>
</tr>
<tr>
<td></td>
<td>(2) Inappropriately long interval between clinical follow-up visits</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Start

Establish intended use and reasonably foreseeable misuse (5.2)

Identify characteristics related to safety (5.3)

Identify hazards and hazardous situations (5.4)

Estimate the risk(s) for each hazardous situation (5.5)

Is risk control required? (6) No

Yes

Identify appropriate risk control measures (7.1)

Is risk control practicable? (7.1)

No

Benefits outweigh the risk? (7.4)

No

Yes

Do the benefits outweigh the risk? (7.4)

No

Yes

Implement and verify the identified risk control measures (7.2)

Is the residual risk acceptable? (7.3)

No

Are new hazards or hazardous situations introduced or existing risks affected? (7.5)

Yes

The manufacturer may consider modifying the medical device or its intended use (go back to 5.2). Otherwise the risk remains unacceptable.

No
Figure B.1 — Overview of risk management activities as applied to medical devices

The manufacturer may consider implementing additional risk control measures (go back to 7.1) or modifying the medical device or its intended use (go back to 5.2). Otherwise the overall residual risk remains unacceptable.
Generic Software Engineering Risk Management

- ISO 15288: System Lifecycle
- ISO 12207: Software Lifecycle
- ISO 16085: Risk Management
Summary

• ISO 31000 covers the completely generic approach to risk management.
• As a result, there are general principles, but the standard can make few requirements
• Looking at a particular domain the lifecycle (EN 62304) and the incorporated risk management (ISO 14971) can be much more specific around device risk.
• The generic systems and software lifecycles and risk management are more specific than the overarching standard (ISO 31000)