Risk Management and ISO/IEC 23894

Peter Deussen

ISO JTC1 IEC
INFORMATION TECHNOLOGY STANDARDS

SC 42 – Artificial Intelligence

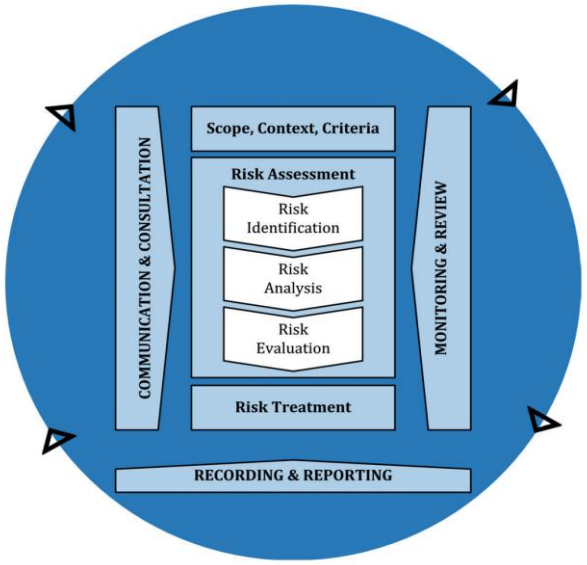
Dr Peter Deussen

- National Standards Officer Germany, Microsoft
- Co-chair of the German Mirror for ISO/IEC JTC 1/SC 42 and CN-CNLC/JTC 21
- Editorships
  - ISO/IEC 23894; Information technology – Artificial intelligence – Guidance on risk management
  - ISO/IEC 42005; Information technology – Artificial intelligence – AI system impact assessment
- Liaison representation
  - From ISO/IEC JTC 1/SC 42 towards ISO/IEC JTC 1/SC 27 (Enhanced liaison)
  - From CN-CNLC/JTC 21 towards ISO/IEC JTC 1/SC 42
- Convenorship
  - ISO/IEC JTC 1/SC 42/AHG 4 – Liaison with SC 42

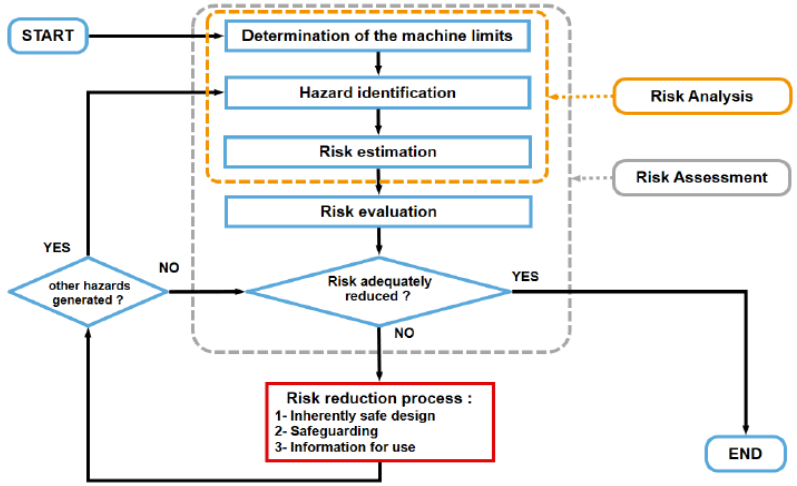
Risk definitions - Spectrum

GRID DIMENSIONS	D1	D2
What is at risk? Negative effects only vs. negative and positive effects	*ISO 21505:2017* Uncertain event or set of events with a potential positive or negative impact	*Guide 51:1999* combination of the probability of occurrence of harm and the severity of that harm
Risk to whom? Organization vs. external effects	*ISO 31000:2018* Effect of uncertainty to objectives	*ISO/TR 2801:2007* combination of the probability of the occurrence of a hazard in a particular situation and the consequences or extent of harm to the individual to be expected from the hazard
Focus on outcomes vs. mechanics	*Directives/Manage System Standards* Effect of uncertainty	*ISO 16311-2:2014* combination of the probability or frequency of occurrence of an event and the magnitude of its consequences

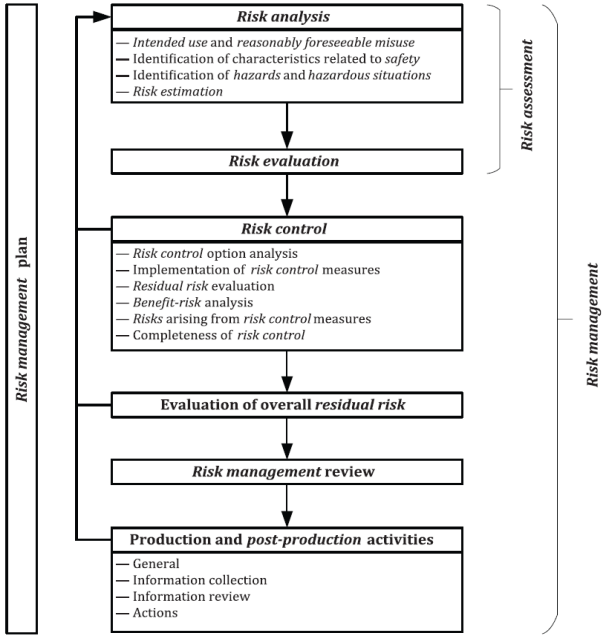
Risk management – some examples



ISO 31000, ISO/IEC 23984



ISO 12100:2010 Safety of machinery — General principles for design — Risk assessment and risk reduction



ISO 14971 2019 (En) Medical devices — Application of risk management to medical devices

Conjecture: While RM approaches differ in scope/focus, RM processes are comparable

Artificial Intelligence Risks

AI Risks Are related to

Fairness / non-discrimination

Security

Safety

Privacy

Robustness

Transparency / explainability

Environmental impact

Accountability

Maintainability

Availability and quality of data

AI expertise

Caused by

- Level of automation
- Lack of transparency and explainability
- Complexity of environment
- System life cycle issues
- System hardware issues
- Technology readiness
- Machine learning issues

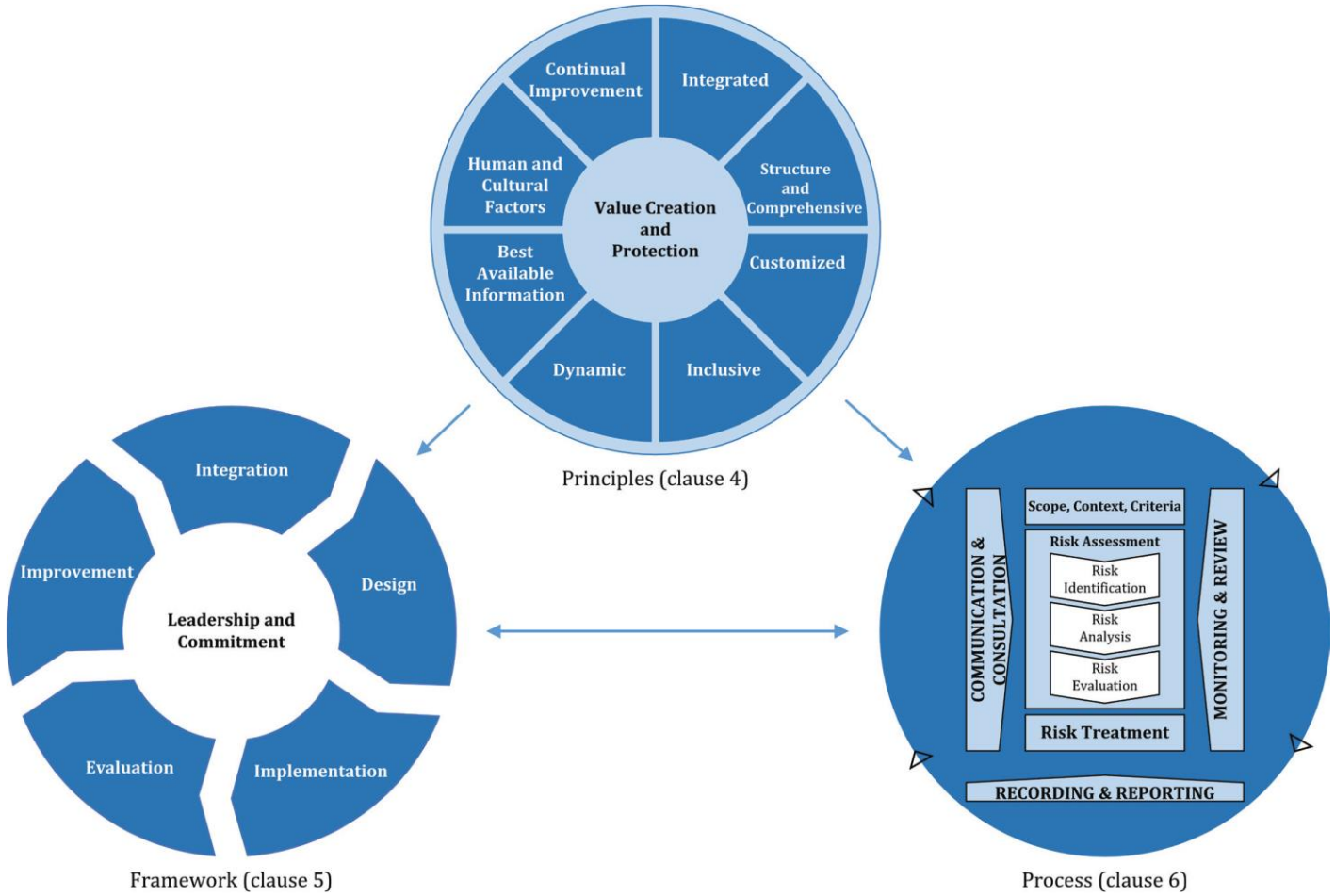
Risk Management

Overview

Risk management as described in ISO 31000:2018:

- Well accepted in industry
- Approach comprises of
  - Principles to follow
  - Management framework
  - Processes

ISO/IEC 23894 follows this approach and adopts AI specific considerations



[Source: ISO/IEC 31000:2018, © ISO]

ISO/IEC 23894

Artificial Intelligence Risk Management

Information technology — Artificial intelligence — Guidance on risk management

Scope

This document provides guidance on how organizations that develop, produce, deploy or use products, systems and services that utilize artificial intelligence (AI) can manage risk specifically related to AI. The guidance also aims to assist organizations to integrate risk management into their AI-related activities and functions. It moreover describes processes for the effective implementation and integration of AI risk management.

The application of these guidance can be customized to any organization and its context.

- **Current state**: FDIS ballot in progress, publication expected for early 2023
- Please note: Guidance only!
  - No requirements
  - No basis for certification
- Relates to risks to the organization
  - Impact to individuals, society, environment considered as part of organizational risk management

Principles of risk management

ISO 31000
Principles

- Integrated
- Structured and comprehensive
- Customized
- Inclusive
- Dynamic
- Best available information
- Human and cultural factors
- Continual improvement

ISO/IEC 23894
AI specific Interpretation

- Extended need to understand stakeholder needs and expectations
- Nature of AI systems
- Implications to the organization itself
- Consideration of societal concerns

Risk management framework

ISO 31000
Framework components

- Leadership and commitment
- Integration
- Design
- Implementation of risk management
- Evaluation of risk management
- Improvement of risk management

ISO/IEC 23894
AI specific Interpretation

- Communicate responsible use / development of AI systems
- Understand the context of the organization
  - Social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors
  - key drivers and trends
  - stakeholder relationships, perceptions, values, needs and expectations
  - contractual relationships and commitments;
  - complexity of networks and dependencies
  - Internal factors, e.g., culture and values, organizational strucures, capabilities, data
- Define roles and responsibilities, allocate resource
- Determine needed information for continual improvement

Risk Management Process

1. Define scope, Context, Risk Criteria

Scope	Context	Risk Criteria
• Objectives and expected outcomes • time, location, specific inclusions and exclusions • tools and techniques • resources and responsibilities • relationships with other projects, processes and activities.	• Societal, legal and contractual environment of the organization • Stakeholder identificaiton, their needs and expectectation	• the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible) • how consequences and likelihood will be defined and measured • time-related factors • consistency in the use of measurements • how the level of risk is to be determined • how combinations and sequences of multiple risks will be taken into account • the organization’s capacity

Risk Management Process

2. Risk Assessment

Risk identification	Risk analysis	Risk evaluation

• Identification of assets and their value:
  • Assets of and their value to the organization
  • Assets of and their value to individuals
  • Assets of and their value to society
• Identification of risk sources
• Identification of potential outcomes
• Identification of controls
• Identification of consequences
	• Assessment of consequences:
	  • criticality of the impact
	  • tangible and intangible impacts
	  • criteria used to establish the overall impact
	• Assessment of likelihood
		• Compare the results of the risk analysis with the established risk criteria to determine where additional action is required

Risk Management Process

3. Risk Treatment

Treatment options

- avoiding the risk by deciding not to start or continue with the activity
- taking or increasing the risk in order to pursue an opportunity
- removing the risk source
- changing the likelihood
- changing the consequences
- sharing the risk (for instance, through contracts or buying insurance)
- retaining the risk by informed decision

Risk Management Process

Additional steps

Communication and consultation

- Involvement and information of stakeholders
- Communication of policies and commitments

Monitoring and review

- Determining the effectiveness of the risk management processes
- Improvements

Recording and reporting

- Information to be recorded
- Reporting requirements

THANKS !

QUESTIONS ?

REMARKS ?

Contact

Peter Deussen

National Standards Officer Germany

Corporate Standards Group

Microsoft Deutschland GmbH

Mobile: +49 151 4406 3650

E-Mail: peter.deussen@microsoft.com