



# The ISO 31 000 standard on risk management

Eric Marsden

<eric.marsden@risk-engineering.org>



Govern well thy appetite, lest Sin

Surprise thee, and her black attendant Death.

— John Milton, Paradise Lost

#### The ISO 31000 standard

- ▷ An international standard that provides **principles** and **guidelines** for **effective risk management** 
  - published in 2009, revised in 2018
- ▷ Generic approach:
  - not specific to any industry or sector
  - can be applied to any type of risk (financial, technological, natural, project)
  - can be applied to any type of organization
- ▷ A brief standard (24 pages)
- Provides foundations for discussing risk management and undertaking a critical review of an organization's risk management process



#### The ISO 31000 standard: scope

- $\triangleright$  Includes:
  - definitions and terms relevant to risk management
  - a set of **principles** that inform effective risk management
  - recommendations for establishing a risk management framework
  - recommendations for establishing a risk management process
- $\,\triangleright\,$  Does not include:
  - detailed instructions/guidance on how to manage specific risks
  - advice relevant to any specific domain
  - any elements related to certification



#### **Related standards**



- ▷ The International Organization for Standardization (ISO) is an international, membership-based NGO
  - based in Geneva, represented in 165 member countries
  - has published over 22 000 international standards
  - Web: www.iso.org
- ▷ ISO Guide 73:2009 on Risk management Vocabulary
  - provides definitions for commonly used terminology in risk management and risk assessment
- ISO 31004:2013 on Risk management Guidance for the implementation of ISO 31000
  - how do I implement ISO 31000 in my organization?
- ▷ ISO 31010:2019 on Risk management Risk assessment techniques
  - guidance on selecting and applying systematic techniques for risk assessment



#### Background to development of ISO 31000 standard

- > The COSO framework on Enterprise Risk Management
  - mostly internal control/auditing: sees risk management primarily as a compliance activity
  - ISO 31000 sees risk management as a **strategic process** for making **risk-adjusted decisions**
- $\,\triangleright\,$  The Australian/New Zealand risk management standard, AS/NZS 4360
- $\,\triangleright\,$  Work started on ISO 31000 in 2005, using AS/NZS 4360 as a first draft
  - consensus-driven process with input from risk management professionals around the world
- $\,\triangleright\,\,$  Standard published in 2009, well received by critics
  - revised version published in 2018 (simplifications)



#### Some controversy in the standard's creation

- ▷ The IEC *Advisory Committee on Safety* removed its support from the ISO working group, arguing that:
  - safety risks are a special case and should be excluded from a general-purpose risk management process
  - any risk to people is unacceptable
- Position of the ISO working group on risk:
  - most human activities lead to some safety risks
  - a uniform process for managing risks is useful

IEC: International Electrotechnical Commission



Source: Purdy (2010). ISO 31000:2009-Setting a new standard for risk management, Risk Analysis 30:6

# New notions in the ISO 31000 standard



# What's new?

- > A new definition of risk
- The notion of *risk appetite*
- The risk management framework
- A management philosophy where risk management is an inseparable aspect of managing change and other forms of decision-making

#### The classical definition of risk

Risk: a combination of the probability and scope of the consequences.

- ISO risk management vocabulary, 2002

More precisely, after Kaplan and Garrick, we ask:

- ▷ What can go wrong?
- ▷ How likely is it to go wrong?
- ▷ If it does go wrong, what are the consequences?



Further reading: Kaplan & Garrick (1984), On the quantitative definition of risk, Risk Analysis 1:1

#### The classical definition of risk: example

Scenario	Annual probability	Consequences		
Fire on tank F	$0.45 \cdot 10^{-4}$	3 killed, 20 M€ loss		
Fire on tank F	$1.2 \cdot 10^{-4}$	1 injured, 20 M€ loss		
Small leak on pipe D	$3 \cdot 10^{-3}$	1 M€ equivalent of environmental damage		
Large leak on pipe D	$1 \cdot 10^{-3}$	20 M€ equivalent of environmental damage		

Risk on this installation is the set of all the lines in this table.



#### Classical definition and financial risks

```
Risk = set of triples \langle \text{scenario}_i, p_i, \text{consequence}_i \rangle
```

For financial risks (where consequences can be all uncontroversially be expressed in monetary units), can be converted into an **expected loss**.

Risk is then the mathematical expectation of the total loss.

$$\mathbb{E}(loss) = \sum_{i} p_i \times \text{consequence}_i$$

This definition also works when some consequences are positive



#### Classical definition and safety risks

Acceptable

Place each scenario in your organization's risk matrix, according to its probability and level of consequences.

Examine whether the sum of possible outcomes is acceptable.



Frequency

For safety risks, all consequences are negative



Risk: the *effect* of uncertainty on an organization's ability to meet its objectives



Risk: the *effect* of uncertainty on an organization's ability to meet its objectives

An effect is a **deviation** from what was expected, which can be positive or negative.

Safety risks are generally negative (losses, deaths, pollution). Financial risks may be positive. This definition is relevant for safety, financial risks, strategic risks, project risks.



Risk: the *effect* of *uncertainty* on an organization's ability to meet its objectives

**Lack of information** or knowledge concerning an event, its consequences or its likelihood



Risk: the *effect* of uncertainty on an organization's ability to meet its objectives

Makes the role of objectives explicit: an activity is only undertaken to reach some goal. Objectives can be financial, health and safety, environmental goals. They can apply at a strategic level, or per project, per product, per site.

This definition leads to more transparency in discussions with stakeholders because objectives (possibly competing) are made explicit.





The organization establishes its objectives: at time  $t_1$  it wants to be at position *O*.





The organization establishes its objectives: at time  $t_1$  it wants to be at position *O*.

It establishes an **action plan** to move from its current position to position *O*.





The presence of uncertainty means that **unexpected perturbations** can cause deviations from the plan defined at  $t_0$ . If unchecked, these would mean that the organization does not achieve its objective of reaching position *O*.

This is *risk*, the effect of uncertainty on the possibility of reaching your objectives.

**RÍSK** ENGINEERING



The risk management activity consists of trying to anticipate and looking out for deviations from the plan, and implementing **corrective actions** so that the organization's objectives are reached despite the unexpected perturbations.



# Risk appetite

#### Concept of "risk appetite"

- ▷ **Risk appetite**: the amount and type of risk that an organization is prepared to pursue, retain or take in pursuit of its objectives
- Represents a balance between the potential benefits of innovation (and risk) and the threats that change inevitably brings
- Helps to guide people within the organization on the level of risk permitted and encourage consistency of approach across an organization
- ▷ Generally expressed (for a company) by a broad statement of approach, which is written by the board



#### Expressing an organization's risk appetite: example

**C** The Organization operates within a low overall risk range. The Organization's lowest risk appetite relates to safety and compliance objectives, including employee health and safety, with a marginally higher risk appetite towards its strategic, reporting, and operations objectives. This means that reducing to reasonably practicable levels the risks originating from various medical systems, products, equipment, and our work environment, and meeting our legal obligations will take priority over other business objectives.

- Risk appetite statement used by a health-care organization



Source: Understanding and Communicating Risk Appetite, COSO, 2012

#### Expressing an organization's risk appetite: example

	Willingness to accept risk					
	Low		Medium		High	
	1	2	3	4	5	
Earnings volatility						
Capital requirements						
Reputation						
Credit ratings						
Regulatory standing						

Appetite may vary across risk categories



Source: Understanding and articulating risk appetite, KPMG, 2008

#### Components of the standard

The standard comprises three main elements:

- ▷ the risk management process
  - how are risks identified, analyzed and treated?

#### ▷ the **risk management framework**

- the overall structure and operation of risk management across the organization
- similar to the plan/do/check/act (PDCA) cycle
- ▷ a set of **principles** which guide risk management activities











**Risk identification**: what could prevent us from achieving our objectives?

**Risk analysis**: understanding the sources & causes of the identified risks; studying probabilities and consequences given the existing controls, to identify the level of residual risk.

**Risk evaluation**: comparing risk analysis results with risk criteria to determine whether the current level of risk is tolerable.

**Risk treatment**: changing the magnitude and likelihood of consequences, both positive and negative, to achieve a net increase in benefit.









Define the scope for the risk management process, define organization's objectives, establish the risk evaluation criteria.

Includes:

- external context: regulatory environment, market conditions, external stakeholder expectations
- internal context: organization's governance, culture, standards and rules, capabilities, existing contracts, worker expectations, information systems, etc.





#### Monitoring and review

Measure risk management performance against indicators, which are periodically reviewed for appropriateness.

Check for deviations from the risk management plan.

Check whether the risk management framework, policy and plan are still appropriate, given organizations' external and internal context.

Report on risk, progress with the risk management plan and how well the risk management policy is being followed.

Review the effectiveness of the risk management framework.





#### **Communication and consultation**

Early on: helps understand stakeholders' interests and concerns, to check that the risk management process is focusing on the right elements.

Later on: helps explain the rationale for decisions and for particular risk treatment options.



#### The risk management framework

- Determines how risk management is integrated with the organization's management system
- ▷ Should include:
  - risk architecture: roles and responsibilities of individuals and committees that support the risk management process (who "owns" different risks?)
  - **strategy**: objectives of the risk management activity in the organization
  - protocols: how the strategy will be implemented and risks managed (procedures, indicators, risk reporting and escalation procedures)





#### Sample risk architecture & responsibility allocation







Principles should influence the design & implementation of organization's risk management framework and process

#### Risk management...

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



Principles guide the creation of the framework





The framework defines the risk management process







Feedback on the performance of the process is used for monitoring and reviews



#### A non-certifiable standard

- Many ISO standards are certifiable: your organization can obtain (purchase!) a certificate from an accredited conformity assessment body stating that its activities on a specific perimeter conform to the standard
  - example: many large organizations certify their quality management system to the ISO 9001 standard
- The 31000 standard provides guidance rather than requirements, so is "not intended for the purposes of certification"





#### Relationship with other standards





#### **Reading the standard**

You can purchase the ISO standard in PDF format from the ISO Store for a "mere" 90€ (price in 2022).

Or you can consult the publication of the Bureau of Indian Standards

- ▷ identical to ISO 31 000:2009 Risk management Principles and guidelines
- made available to interested readers on the web "to promote the timely dissemination of this information in an accurate manner to the public"

 $\rightarrow \texttt{https://web.archive.org/web/20140822235145/https://law.resource.org/pub/in/bis/S07/is.iso.31000.2009.pdf$ 







#### Importance of effective risk management



Source: PricewaterhouseCoopers analysis, based on Bloomberg data, 2007

Importance of effective risk management for safety risks is evident.

For financial risks, evidence shows that the financial markets value good risk management, and better ratings of risk management performance lead to lower capital costs for firms.



Source: PriceWaterhouseCoopers report Seizing opportunity: linking risk and performance, 2009

▷ Flower on slide 8: motiqua via flic.kr/p/6mB7up, CC-BY licence

#### Credits

- Venus flytrap (slide 15): Aurore D via flic.kr/p/5qdqE7, CC BY-NC-ND licence
- b Thanks to Alex Dali (G31000 Risk Institute) for useful suggestions on the slides (Oct. 2022)



Further reading

- ▷ A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000, Airmic/Alarm/IRM, 2010, from theirm.org/media/886062/ISO3100\_doc.pdf
- La norme ISO 31000 en 10 questions, G. Motet, available (in French) from foncsi.org/fr/publications/cahiers-securite-industrielle/-10-questions-norme-ISO31000/

For more free content on risk engineering, visit risk-engineering.org



#### Feedback welcome!



This presentation is distributed under the terms of the Creative Commons Attribution - Share Alike licence

@LearnRiskEng

fb.me/RiskEngineering



Was some of the content unclear? Which parts were most useful to you? Your comments to feedback@risk-engineering.org (email) or @LearnRiskEng (Twitter) will help us to improve these materials Thanks!



For more free content on risk engineering, visit risk-engineering.org