D 61v18

Risk management

Objective

Objective of the module: Master risk management to be able to:

- achieve the company's objectives with serenity
- optimize decision-making
- plan the continuity of operational processes

1 Risk

1.1 History

The word risk could come from the Latin word *resecum* “that which cuts, reef” hence the maritime origin “steep rock” or could derive from the ancient Italian *risicare*, which means “to dare.”

Opportunities and threats are two sides of the same coin called risk. When the outcome is favorable we speak of an opportunity, when the outcome is unfavorable we speak of a threat.

About 5,200 years ago in the Euphrates region, a group called Asipu were consultants in risk analysis for making risky or uncertain decisions.

Every decision involves risk. Peter Barge

In Mesopotamia, around 3,900 years ago insurance began as one of the oldest risk management strategies. The risk premium for ship and cargo losses in basic contracts was formalized in the Hamurabi Code.

More than 2,400 years ago Pericles spoke about taking risks and evaluating them before carrying out an action. His compatriot Socrates defines eikos (possible, probable) as “likelihood of truth”.

Blaise Pascal and Pierre de Fermat laid the foundations of probability theory in the 1650s, which opened the door to quantitative risk assessment.

Pierre Simon de Laplace developed a risk analysis in 1792 with his calculations of the probability of death with and without smallpox vaccination.

Risk management is relatively recent. For example, the Basel II agreement on risk management requirements in the banking sector dates from 2004. Some prescriptive (non-certifiable) standards on risk appeared at the beginning of the 21st century (see § 2.2).

The 2008 global financial crisis called into question the contribution of risk management. Some have said that risk management methods have failed to avert this crisis. But the analysis reveals that this failure is mainly due to:

- the lack of a balanced analysis of the high benefits and the risks involved
- poor judgment of the improbability of certain events (poorly quantified level of risk) based on imprudent financial models
- poor monitoring of key parameters
- the divergent understanding of different stakeholders on risk appetite and attitude towards risk
- the collapse of wholesale money markets not anticipated by the credit models used by certain banks

The future cannot be predicted

But the risk that results from uncertainty can be managed. The ability to identify risk, analyze it, evaluate it, and then act accordingly is the basis of risk management.

A difficulty in risk management arises from the fact that the event concerned (the damage) takes place in the future. You have to imagine an event that may never take place.

Zero risk does not exist

For several decades, the majority of companies have become aware that the costs of implementing risk management are insignificant compared to the unfavorable consequences or even the insurance to take out.

The main objective of risk management is to ensure the survival of the company in all circumstances.

Risk management has been considered in the past by some managers as something superfluous. These people believed that the main goal was to avoid risk. Since then, many have understood that risk is inevitable and intrinsic to any activity but must be reduced to an acceptable level.

Risk cannot be eliminated

Risk management has become a necessity, even the ISO 9001 standard (quality management systems – requirements) since the 2015 version has included the risk-based approach (risk-based thinking).

1.2 Scope

The scope of this module applies to risk management in business. This concern:

- the principles (see chapter 4)
- the framework (see chapter 5)
- the process (see chapter 6)
- tools (see chapter 7)

The risk area includes:

- the structure of the company
- the management system
- the department
- the process
- the product
- the service
- the project
- the performance
- reliability
- costs, cf. annex 01
- the calendar
- the methods
- technology
- requirements
- specifications including acceptance criteria
- functionalities
- the tools
- external providers
- the tests

This module does not specifically include accounting risks and extreme risks related to:

- financial crises
- insurance
- natural disasters
- pandemics
- occupational diseases
- environmental protection
- food crises
- terrorist acts
- tax fraud
- counterfeit parts
- corruption

Example of a scope

For a circus, the risks likely to cause problems during a performance include a power outage, a storm, the absence of several actors or technicians (illness or social conflict) or major transport problems for the public.

After identifying, analyzing and evaluating the risks that could disrupt the performance, top management must decide what actions to take to reduce the chances of cancellation.

Risk management is used in many areas:

- insurance
- the bank
- the army
- energy
- aerospace
- projects
- medical devices
- medicine
- the company
- construction
- the markets

1.3 Benefits

Expected benefits of risk management:

- improved stakeholder confidence
- improved overall performance of the company
- improved company reputation
- improved business resilience
- improved appreciation of opportunities and threats
- increased likelihood of achieving objectives
- increase in opportunities to be seized
- creation of value for the company
- reduction in losses
- establishment of an adequate framework for the implementation in a controlled manner of any activity
- establishment of a reliable basis for decision-making
- identification of gaps

- less work to redo
- obtaining a competitive advantage
- optimization of resource use
- protection of company assets
- effective response to changes
- reduction of costs and deadlines
- reduction of operational surprises
- scrupulous compliance with legal requirements
- increased visibility of the responsibilities of each staff member

The biggest risk is not taking any!

Root causes of failures:

- unplanned activities
- priority change
- irregular communication of results
- excessive self-confidence
- poorly defined acceptance criteria
- poorly understood requirements
- lack of resources
- poor estimation of effort
- poor distribution of work
- unplanned product modification
- new methods and technologies misunderstood
- unrealistic goals
- industrialization problems
- design issues
- unforeseen technical problems
- sporadic and inaccurate progress reports
- unidentified risks
- insufficient support from top management
- conflicting or inconsistent specifications

Applying risk management upstream costs 10 times less than managing a crisis

The cost of managing risk over the life of a product is shown in figure 1-1.

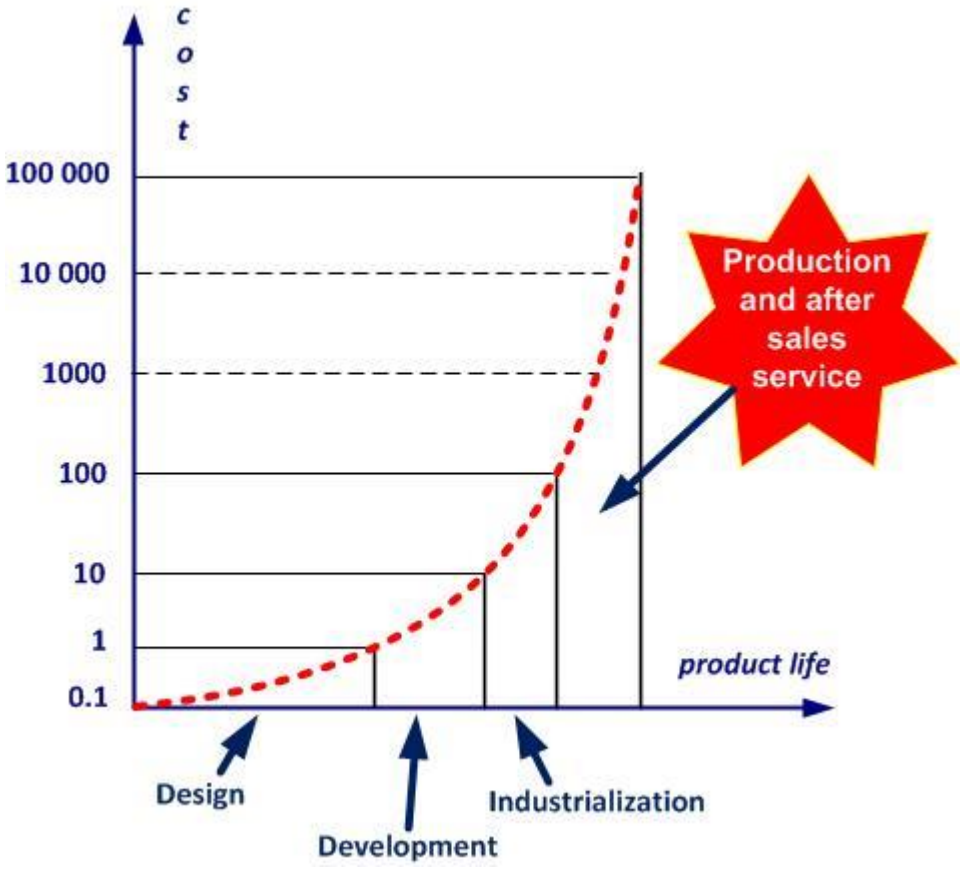


Figure 1-1. The cost and product cycle life

He who excuses himself, accuses himself

Common excuses for failure:

- it was the responsibility of top management
- this was not an explicit requirement in the contract
- how can we have an effective plan in the face of so many potential problems
- give me enough time and everything will be sorted
- in the event of a serious emergency situation, the implication will be completely different
- there was not enough time
- there was no staff available
- there are more important things to do
- I was sure we could cope
- I didn't realize it was so serious
- I didn’t think it was a key process
- I didn't think this would happen
- insurance had to take care of this situation
- the contract was already signed
- you cannot plan for the unexpected

A list of risk management successes and failures can be found in annex 02.

2 Definitions, standards and books

2.1 Definitions

The beginning of wisdom is the definition of terms. Socrates

A risk can have negative impacts (we speak of threats) or positive impacts (we speak of opportunities).

Seizing an opportunity is taking risks, but not seizing an opportunity can expose us to risk.

Often risk is assimilated with hazard or danger and commonly used instead of threat.

There are multiple definitions of the word risk. Some examples:

- combination of the probability of occurrence of harm and the severity of that harm. ISO 51 (1999)
- combination of the probability of an event and its consequences. ISO Guide 73 (2002)
- combination of the probability of the occurrence of a dangerous event and the severity of the injury or harm to health caused to people by this event. ILO-OSH (2001)
- possible danger more or less predictable. Little Robert
- description of a specific event that may or may not occur, as well as its causes and consequences. IRM (2013)
- effect of uncertainty on objectives. ISO Guide 73 (2009)
- effect of uncertainty. ISO 45001 (2018)
- negative effect of uncertainty. Christopher Paris
- mathematical expectation of an event probability function. Daniel Bernoulli
- event whose random occurrence is likely to cause damage to people or property or both at the same time. Serge Braudo
- uncertain possible event whose occurrence does not depend exclusively on the will of the parties, and which could cause damage. Larousse
- uncertainty of outcomes, whether a positive opportunity or a negative threat. OGC - UK (2005)
- the extent of the potential loss. Evan Picoult
- the future impact of an uncontrolled danger. Sean Chamberlin
- the extent of the danger. Georges-Yves Kervern
- the possibility that something will happen that will impact the objectives. AS 4360 (2004)
- the likelihood that something will happen. IFRIMA (1994)
- the risk should be proportional to the probability of occurrence as well as the extent of damage. Blaise Pascal
- probability and magnitude of a loss, disaster or other adverse event. Douglas Hubbard

Our preference:

Risk: *likelihood of occurrence of a threat or an opportunity*

Some definitions of risk management:

- coordinated activities to direct and control an organization with regard to risk. ISO Guide 73 (2009)
- culture, processes and structures in place to effectively manage opportunities and negative impacts. Business Continuity Institute
- be smart to take risks. Douglas Hubbard
- provides a framework for organizations to control and respond to uncertainties. Paul Hopkins
- the act or practice of risk. Edmund Conrow

Our preference:

Risk management: *activities to restrict the possibility that something goes wrong*

Some definitions of the word hazard (or dangerous phenomenon):

- what constitutes a threat, a risk for someone, something. Larousse
- what threatens or compromises the safety or existence of a person or thing. Little Robert
- intrinsic property of a substance, of a system which can lead to damage. Yvan Vérot
- source of potential harm. ISO Guide 73 (2009)
- source or situation likely to cause trauma and pathologies. ISO 45001 (2018)

Our preference:

Hazard: *situation that could lead to an incident*

Identify the hazard is to ask yourself what could go wrong

Some definitions of risk assessment:

- overall process of risk identification, risk analysis and risk evaluation. ISO Guide 73 (2009)
- assessment of undesirable outcomes and assigning probabilities to their chances of occurrence. Vlasta Molak
- qualitative and quantitative risk assessment process and determination of the type of analysis to be carried out. Quebec Office of the French Language

Our preference:

Risk assessment: process of risk identification, analysis and evaluation

Some definitions of risk identification:

- process of finding, recognizing and describing risks. ISO Guide 73 (2009)
- process for reviewing program areas and each critical technical process to identify and document associated risk. Edmund Conrow

Our preference:

Risk identification: *assessment activity to find and describe risks*

Some definitions of risk analysis:

- process of examining each identified risk issue or process to refine the description of the risk, isolate the cause and determine the effects. Edmund Conrow
- process to comprehend the nature of risk and to determine the level of risk. ISO Guide 73 (2009)
- systematic use of information to identify sources and assign risk values. Terje Aven

Our preference:

Risk analysis: *activity to understand the nature of a risk and determine its impact*

Some definitions of risk treatment:

- process of developing, selecting and implementing controls. BS 31100 (2011)
- process to modify risk. ISO Guide 73 (2009)
- process that identifies, evaluates, selects and implements options to set risk at acceptable levels given the constraints and objectives of the program. Edmund Conrow

Our preference:

Risk treatment: *risk modification activities*

Some definitions of the word opportunity:

- positive effect of uncertainty. Christopher Paris
- potential for achieving desired and positive outcomes of an event. Robert Charrette

Our preference:

Opportunity: *uncertain event that may have a favorable impact*

Uncertainty and probability are subjective notions with invented quantities.

Impact: *consequence of an event affecting the objectives*

Likelihood: *possibility that something happens*

Probability can be considered as a measure of uncertainty. If probability can be measured it is therefore linked to something that has happened. Likelihood is a more general notion because it can include an effect that never happened.

To avoid confusing hazard and risk, a few simple examples:

Hazard	Risk
slippery floor	broken leg
electricity	electrocution
tobacco	lung cancer
climb a ladder	break your arm when falling

As shown in figure 2-1, the time of exposure to hazard multiplies the risk:

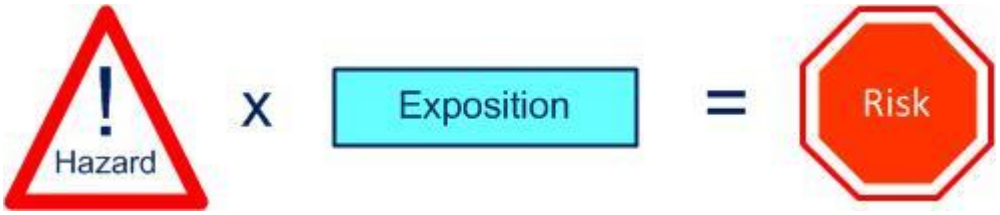


Figure 2-1. Exposure to hazard

Risk (and its level) is a function of impact and likelihood (figure 2-2).

Figure 2-2. The level of risk

The risk is residual when the impact and likelihood are low, cf. figure 2-3. As soon as the impact and likelihood are high, we approach the critical zone (red).

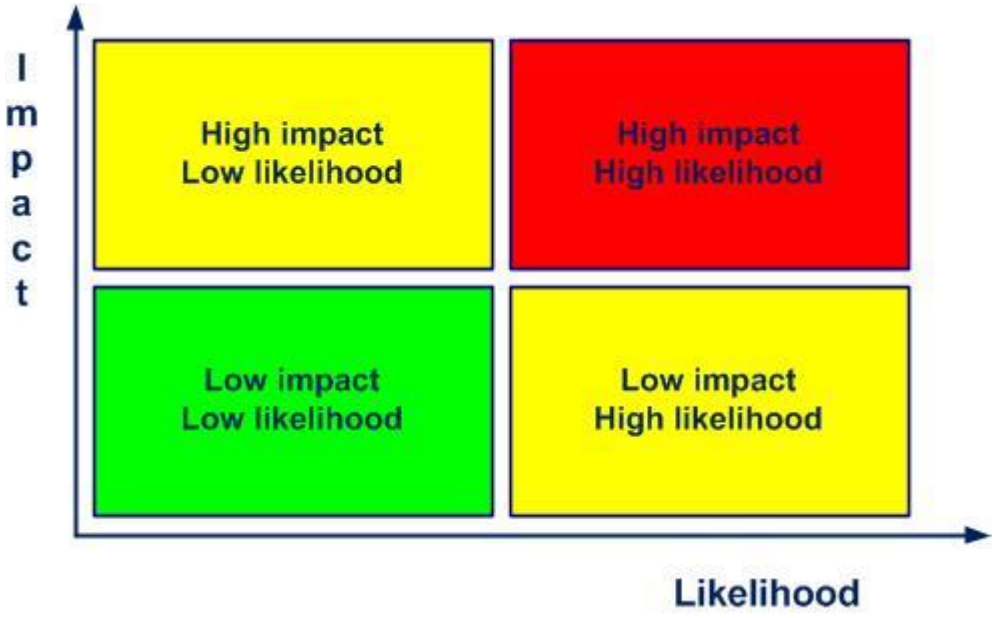


Figure 2-3. The criticality of the risk

More details on risk levels are shown in annex 03.

Some definitions and acronyms:

5 M: *Mother nature, Material, Method, Machine and Manpower (also called Ishikawa diagram and fishbone diagram)*
5 S: *from Japanese Seiri = sort, Seiton = set in order, Seiso = shine, Seiketsu = standardize and Shitsuke = sustain*
5 W: *five times Why?*
8 D: *eight do or eight actions to carry out. The 8 D tool is mainly used in the automotive industry. Allows a team to identify and eradicate the causes of a problem*

A 3: *report in A 3 visual management format on the essentials of problem solving or project progress*
Benchmarking: *comparative analysis technique against one or more competitors*
Brainstorming: *method allowing the development of ideas from the participants in order to find solutions*
Conformity: *fulfillment of a specified requirement*
Control chart: *statistical tool with high and low limits. Allows you to easily detect trends and malfunctions*
Control plan*: document describing the specific measures to carry out the control of a product or process*
Control: *see inspection*
COQ: *cost of obtaining quality*
Corrective action: *action to eliminate the causes of nonconformity or any other undesirable event and to prevent their recurrence*
Criticality*: level of a potential risk*
Curative action: *action to eliminate a detected nonconformity*
Customer satisfaction: *top priority objective of every quality management system related to the satisfaction of customer requirements*
Customer: *anyone who receives a product*
Cycle time: *time between the release of the product from one process and the release of the next product*
Dashboard: *coherent set of indicators to measure performance and facilitate decision support*
Defect: *nonconformity related to a specified use*
DMAIC: *Determine, Measure, Analyze, Improve, Control. Six sigma approach to manage a problem and improve*
Dysfunction: *deviation in the ability of a functional unit to perform a specified function*
Effectiveness: *capacity to perform planned activities with minimum effort*
Efficiency: *financial relationship between achieved results and resources used*
EFQM: *European Foundation for Quality Management. Organization offering a model of excellence ("Sharing effective practices"). EFQM Annual Award*
Fail safe device*: system allowing the prevention of errors by eliminating the human factor, also called Poka-Yoké*
Failure tree analysis (FTA): *tree diagram analysis method (cause - effects) to avoid safety and reliability problems. See also Tree diagram*
Failure: *variation of aptitude of a functional unit to satisfy a specified function*
FIFO: *First In, First Out*
Flowchart: *picture of a process that shows the steps performed and their interactions (see also ISO 22 000, 3.6; also called functional diagram and operational diagram)*
FMEA: *Failure Mode and Effects Analysis*
Functional analysis: *studies of the functions of a product or system in relation to its environment (see also NF X50-151)*
Gemba walk: *walk in the field, where it's happening. Favoring analysis in the field rather than in a meeting room*
Gemba: *from Japanese, = real place, in the field*
IMS: *integrated management system*
Indicator: *value of a parameter, associated with an objective, allowing the objective measure of its effectiveness*
Interested party: *person, group or organization affected by the impacts from a company*
ISO: *international organization for standardization*
Kaizen: *from Japanese, kai = change and zen = good (for the better, better), Kaizen = continual improvement*
Management system: *set of processes allowing objectives to be achieved*
Manager: *someone who gets results through other people*

MCT: *multiple choice test*
Monitoring: *set of planned actions to guarantee the effectiveness of control measures*
Nonconformity (NC): *non-fulfillment of a specified requirement*
Non-quality: *gap between expected and perceived quality*
Organization: *structure that satisfies a need*
Poka-Yoké: *from Japanese Poka – unintentional error, Yoké – avoid. See Fail safe device*
Preventive action: *action to eliminate the potential causes of nonconformity or any other undesirable event and to prevent their appearance*
Problem: *gap that must be reduced to obtain a result*
Process: *activities that transform input into output*
Product (or service): *any result of a process or activity*
QM: *quality manager*
QMS: *quality management system*
QSE: *quality, safety, environment*
Quality management system (QMS): *everything necessary for the quality management of a company*
Quality management: *activities allowing the control of an organization with regard to quality*
Quality objective: *quality-related, measurable goal that must be achieved*
Quality policy: *statement by top management allowing the establishment of quality objectives*
Requirement: *implicit or explicit need or expectation*
Responsibility: *capacity to make a decision alone*
Safety: *aptitude to avoid an undesired event*
Stakeholder*: person, group or company that can affect or be affected by an organization*
Strategy: *total approach to achieve objectives*
Supplier: *entity that provides a product*
SWOT: *Strengths, Weaknesses, Opportunities, Threats. Tool for structuring a risk analysis*
System: *set of interacting processes*
Top management (direction): *group or persons responsible for management at the highest level of the company*
Tree diagram: *graph showing the chain of causes of a problem*
Waste: *anything that adds cost but not value*
WWWWHHW: *Who, What, Where, When, How, How much, Why*

In the terminology of management systems, do not confuse:

- accident and incident
  - an accident is an unexpected serious event
  - an incident is an event that can lead to an accident
- anomaly, defect, dysfunction, failure, nonconformity, reject and waste:
  - an anomaly is a deviation from what is expected
  - a defect is the non-fulfillment of a requirement related to an intended use
  - a dysfunction is a degraded function that can lead to a failure
  - a failure is when a function has become unfit
  - a nonconformity is the non-fulfillment of a requirement in production
  - a reject is a nonconforming product that will be destroyed
  - a waste is when there are added costs but no value
- audit program and plan
  - an audit program is the annual planning of the audits
  - an audit plan is the description of the audit activities
- audit, inspection, auditee and auditor
  - an audit is the process of obtaining audit evidence
  - an inspection is the conformity verification of a process or product
  - an auditee is the one who is audited

    - an auditor is the one who conducts the audit
- control and optimize
    - to control is to meet the objectives
    - to optimize is to search for the best possible results
- customer, external provider and subcontractor
    - a customer receives a product
    - an external provider provides a product on which specific work is done
    - a subcontractor provides a service or product on which specific work is done
- effectiveness and efficiency
    - effectiveness is the level of achievement of planned results
    - efficiency is the ratio between results and resources
- follow-up and review
    - follow-up is the verification of the obtained results of an action
    - review is the analysis of the effectiveness in achieving objectives
- hazard, problem and risk
    - hazard is the state, the situation or the source which can lead to an accident
    - problem is the gap between the actual situation and the desired situation
    - risk is the measure, the consequence of a hazard and it is always a potential problem
- inform and communicate
    - to inform is to give someone meaningful data
    - to communicate is to pass on a message, to listen to the reaction and discuss
- objective and indicator
    - an objective is a sought-after commitment
    - an indicator is the information on the difference between the pre-set objective and the achieved result
- organization and enterprise, society, company
    - organization is the term used by the ISO 9001 standard as the entity between the supplier and the customer
    - an enterprise, society and company are examples of organizations
- prevention and protection, cf. figure 2-4
    - prevention is the means to reduce the likelihood and frequency of occurrence of a risk (checking tire pressure)
    - protection is the means to limit the impact of a risk (fastening your seat belt)
- process, procedure, product, activity and task
    - a process is how we satisfy the customer using people to achieve the objectives
    - a procedure is the description of how we should conform to the rules
    - a product is the result of a process
    - an activity is a set of tasks
    - a task is a sequence of simple operations
- risk and crisis management
    - risk management is like fire prevention
    - crisis management is like putting out a fire

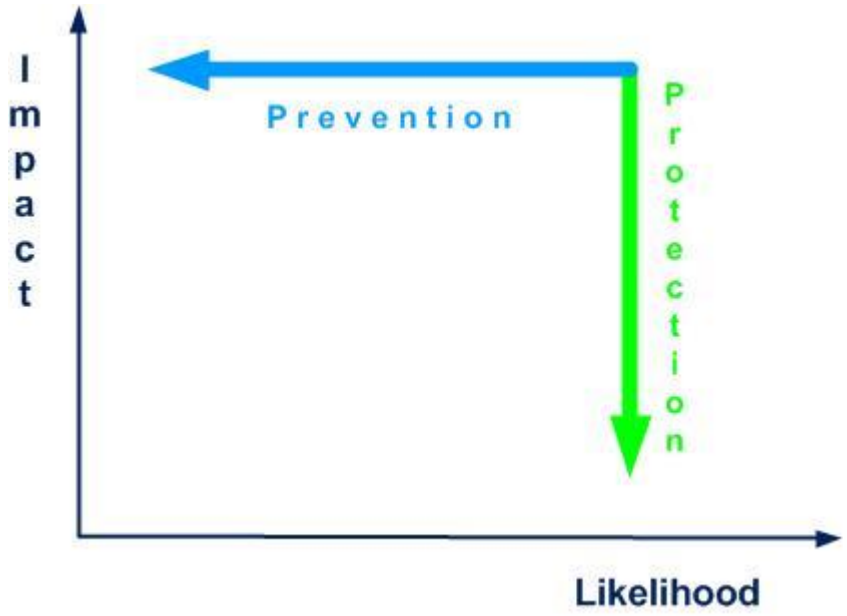


Figure 2-4. Prevention and protection

Remark 1: the most important thing is to determine a common and unequivocal vocabulary for everyone in the company.

Remark 2: between likelihood and probability our preference is for likelihood.

Remark 3: the customer can also be the user, the beneficiary, the trigger, the ordering party or the consumer.

Remark 4: each time you use the expression "opportunity for improvement" instead of nonconformity, malfunction or failure, you will gain a little more trust from your interlocutor (external or internal customer).

For other definitions, comments, explanations and interpretations that you don't find in this module and in annex 06, you can consult:

- ISO Online Browsing Platform (OBP)
- IEC Electropedia

2.2 Standards

Risk-related standards (in chronological order):

- AS 4360 (1995): Risk management
- IRM/Alarm/AIRMIC (2002): A Risk Management Standard (Risk Management Reference Framework)
- FD X50-117 (2003): Project management - Risk management - Project risk management
- COSO (2004): Enterprise Risk Management - Integrated Framework
- XP PR EN 9134 (2005): Aerospace series - Quality systems - Guidelines for risk management concerning the supplier chain
- FD X50-252 (2006): Risk management - Guidelines for risk estimation
- IEC 61025 (2006): Fault tree analysis (FTA)
- ISO Guide 73 (2009): Risk management - Vocabulary

- FD X50-253 (2011): Risk management - Risk management process - Guidelines for communication
- BP Z74-700 (2011): Business Continuity Plan (BCP)
- BS 11200 (2014): Crisis management - Guidance and good practice
- BS 65000 (2014): Guidance on organizational resilience
- FD ISO 31004 (2014): Risk management - Guidelines for the implementation of ISO 31000
- FD X50-259 (2014): Risk management - Business continuity plan (PCA) - Implementation and maintenance approach
- FD X50-260 (2016): Risk management - Guidelines for implementation in ETI/SMEs and other organizations - ETI/SME-PMI
- IEC 61882 (2016): Hazard and operability studies (HAZOP studies) - Application guide
- ISO 22316 (2017): Security and resilience - Organizational resilience - Principles and attributes
- ISO 31000 (2018): Risk management – Guidelines
- NF EN ISO 14971 (2019): Medical devices - Application of risk management to medical devices
- IEC 31010 (2019): Risk management - Risk assessment techniques
- ISO 22301 (2019): Societal security - Business continuity management systems - Requirements
- EFQM (2020): European Foundation for Quality Management
- ISO 22313 (2020): Business continuity management systems – Guidance on the use of ISO 22301
- BS 31100 (2021): Risk management. Code of practice

Two FMEA documents:

- AIAG & VDA FMEA Handbook, AIAG, 2019
- IEC 60812: Analysis of failure modes and their effects (FMEA and FMECA), EIC, 2018

Two French documents related to the processes with explanations, recommendations and examples:

- AC X50-178 (agreement, 2002) Quality management – Process management – Good practices and feedback
- FD X50-176 (documentation booklet, 2017) Management tools – Process management

Risk management – ENA – 2020 bibliography.

None of these standards are obligatory but as Deming said:

There is no need to change. Survival is not obligatory

Risk and the risk-based thinking approach are present in many standards and frameworks. Some of the most common examples:

- ISO 9001 version 2015 (§§ 0.3.3, 6.1)
- ISO 14001 version 2015 (§§ 0.3, 3, 6.1)
- ISO 13485 version 2016 (§§ 0.2, 3, 4.1.2)
- ISO 45001 version 2018 (§§ 3, 6.1, 6.1.2.2, 8.1.2)
- ILO-OSH 2001 version 2002 (§§ 2.3, 3.3, 3.4, 3.5, 3.7, 3.10, 3.11, 3.15, 3.16)

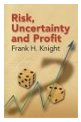
- ISO 26000 version 2010 (§§ 6.1, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.4, 7.8; tables 1 and 2)

A detailed questionnaire (233 questions) on the recommendations of the ISO 31000 version 2018 standard can be found in annex 04.

2.3 Books

When I think of all the books still left for me to read, I am certain of further happiness. Jules Renard

Books for further reading on risk:

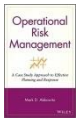
- 

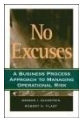
Risk, Uncertainty And Profit, Frank Knight, University of Chicago Press, 1921
- 

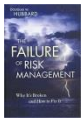
Against the Gods: The Remarkable Story of Risk, Peter Bernstein, John Wiley & Sons, New York, 1998
- 
Business Continuity Management - How to Protect Your Company from Danger, Michael Gallagher, Prentice Hall, 2002
- 

Effective Risk Management: Some Keys to Success, Edmund Conrow, AIAA, 2003
- 

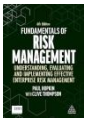
Identifying and managing project risk: Essential Tools for Failure-Proofing Your Project- Tom Kendrick, AMACOM, 2003
- 

The Quality Toolbox, Nancy Tague, ASQC Quality Press, 2005
- 

Operational risk management, Mark Abkowitz, Wiley, 2008
- 

No excuses, A business process approach to managing operational risk, Dennis Dickstein, Wiley, 2009
- 

The Failure of Risk Management: Why It's Broken and How to Fix It, Douglas Hubbard, Wiley, 2009
- 
Management of Risk: Guidance for Practitioners, team, Stationery Office Books, 2010

-  Strategic Risk Management Practice: How to Deal Effectively with Major Corporate Exposures, Torben Andersen, Cambridge University Press, 2010
-  Risk Management, How to Assess, Transfer and Communicate Critical Risks, Antonio Borghesi, Barbara Gaudenzi, Springer, 2013
-  Managing the Unexpected: Sustained Performance in a Complex World, Karl Weick, Kathleen Sutcliffe, Wiley, 2015
-  ISO 31000 - Risk Management - A practical guide for SMEs, ISO, 2015
-  Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, Deputy Assistant Secretary of Defense Systems Engineering, 2017
-  Enterprise Risk Management - Integrating with Strategy and Performance, COSO, AICPA, 2017
-  ISO 31000: 2018 Enterprise Risk Management, Greg Hutchins, Certified Enterprise Risk Manager (R) Academy, 2018
-  Practice Aid: Enterprise Risk Management: Guidance For Practical Implementation and Assessment, 2018, AICPA, Wiley, 2018
-  Enterprise Risk Management in Government: Implementing ISO 31000:2018, James Kline, Quality Plus Engineering, 2019
-  ISO 31000 Risk Management A Complete Guide - 2021 Edition, The Art of Service, 2020
-  A Review of Risk Management According to ISO 31000, 2018, Amir Samimi, Scholars' Press, 2020
-  The Failure of Risk Management: Why It's Broken and How to Fix It 2nd Edition, Douglas W. Hubbard, Wiley, 2020
-  Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Enterprise Risk Management 6th Edition, Kogan Page, 2021

- 

How to be a Chief Risk Officer: A handbook for the modern CRO, Jennifer Geary, Neilsen, 2022

None of these books are mandatory...

3 Process approach

If you cannot describe what you are doing as a process, you do not know what you're doing. Edwards Deming

3.1 Process types

The word process comes from the Latin root procedere = go, development, progress (Pro = forward, cedere = go). Each process transforms inputs into outputs, creating added value and potential nuisances.

A process has three basic elements: inputs, activities and outputs. 

A process can be very complex (launch a rocket) or relatively simple (audit a product). A process is:

- repeatable
- foreseeable
- measurable
- definable
- dependent on its context
- responsible for its external providers

A process is, among other things, determined by its:

- title and its type
- purpose (why?)
- beneficiary (for whom?)
- scope and activities
- initiators
- documents and records
- inputs
- outputs (intentional and unintentional)
- restrains
- people
- material resources
- objectives and indicators
- person in charge (owner) and actors (participants)
- means of inspection (monitoring, measurement)
- mapping
- interaction with other processes
- risks and potential deviations
- opportunities for continual improvement

A process review is carried out periodically by the process owner (cf. annex 05). 

The components of a process are shown in figure 3-1: 

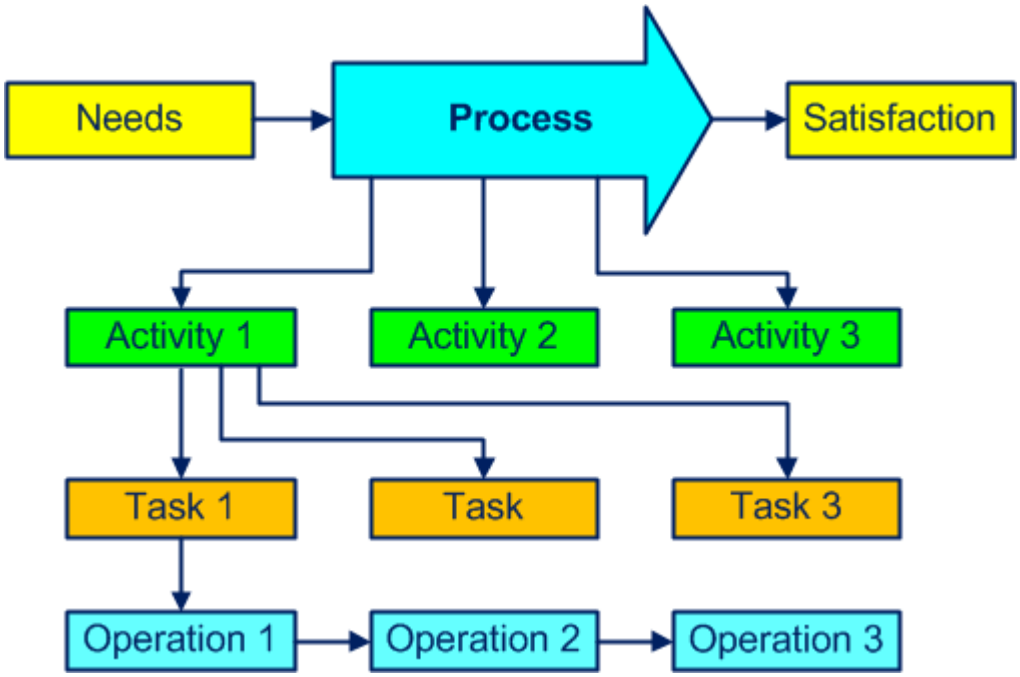


Figure 3-1. Components of a process

Figure 3-2 shows an example that helps answer the questions:

- which materials, which documents, which tooling? (inputs)
- which title, which activities, requirements and constraints? (process)
- which products, which documents? (outputs)
- how, which inspections? (methods)
- what is the level of performance? (indicators)
- who, with what competence? (staff)
- with what, which machines, which equipment? (material resources)

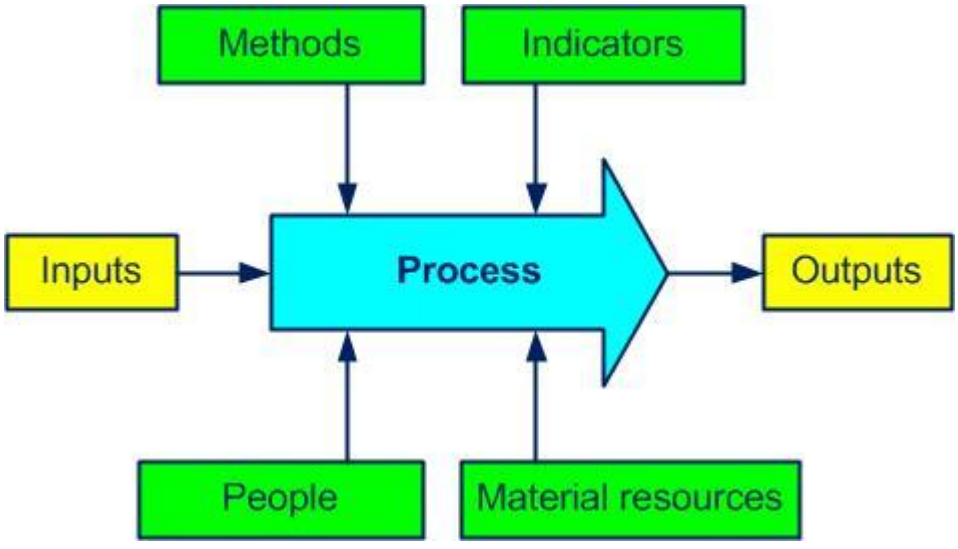


Figure 3-2. Some elements of a process

Often the output of a process is the input of the next process.

You can find some examples of process forms in the document pack D 02.

Any organization (company) can be considered as a macro process, with its purpose, its inputs (customer needs and expectations) and its outputs (products/services to satisfy customer requirements).

Our preference is to identify a process using a verb (buy, produce, sell) instead of a noun (purchases, production, sales) to differentiate the process from the company's department or procedure to maintain and recall the purpose of the process.

The processes are (as we will see in the following paragraphs) of management, realization and support types. Do not attach too much importance to process categorizing (sometimes it is very relative), but ensure that all the company's activities at least fall into one process.

3.1.1 Management processes

Management processes are also known as piloting, decision, key or major processes. They take part in the overall organization and include the development of the policy, deployment of the objectives and all needed checks. They are the glue of all realization and support processes.

The following processes can be part of this family:

- develop strategy
- manage risks, cf. annexes 07 and 08: 
  - plan
  - assess:
    - identify
    - analyze
    - evaluate
  - treat
- develop policy
- establish process ownership
- improve
- audit
- communicate
- plan the MS
- acquire resources
- carry out management review
- measure customer satisfaction
- negotiate contract
- analyze data

3.1.2 Realization processes

The realization (operational) processes are related to the product, increase the added value and contribute directly to customer satisfaction.

They are mainly:

- design and develop new products
- purchase components
- produce products
- sell products
- inspect production

- maintain equipment
- implement traceability (identify and keep history)
- receive, store and deliver
- control nonconformities
- implement preventive and corrective actions

3.1.3 Support processes

The support processes provide the resources necessary for the proper functioning of all other processes. They are not directly related to a contribution of the product's added value but are still essential.

The support processes are often:

- control documentation
- provide information
- acquire and maintain infrastructure
- provide training
- manage inspection means
- manage staff
- keep accountability

3.2 Process mapping

Par excellence process “mapping” is a multidisciplinary work. This is not a formal requirement of the ISO 31000 standard but is always welcome.

The three types of processes and some interactions are shown in figure 3-3 and D 02. 

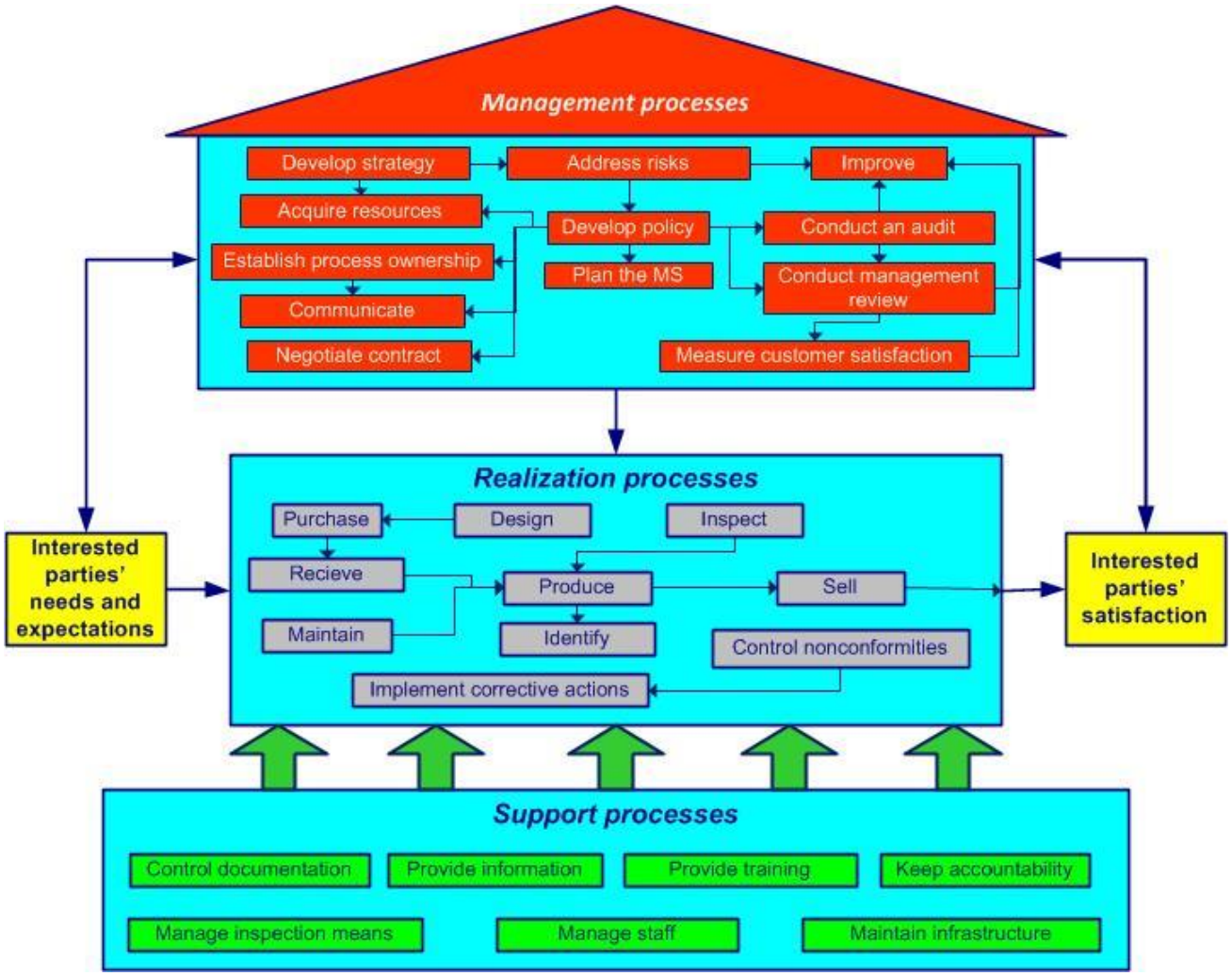


Figure 3-3. Process house

Mapping, among other things, allows you to:

- obtain a global vision of the company
- identify the beneficiaries (customers), flows and interactions
- define (simple) rules for communication between processes

To obtain a clearer picture, you can simplify by using a total of about 15 core processes. A core process can contain several sub-processes: for example, the process "develop the MS" can involve:

- develop strategy
- manage risks
- develop policy
- plan the MS
- deploy objectives
- acquire resources
- establish process ownership
- improve

3.3 Process approach

Simple solutions for now, perfection for later

The fourth principle of quality management is “Process approach” (see ISO 9000, 2.3.4). Some benefits:

- obtain a global vision of the company thanks to the mapping
- identify and manage responsibilities and resources
- achieve effective management of the company based on process indicators
- manage risks that could influence the objectives

Process approach: *management by the processes to better satisfy customers, improve the effectiveness of all processes and increase global efficiency*

When the process approach is integrated during the development, implementation and continual improvement of a management system, it allows one to achieve objectives that are related to customer satisfaction, as is shown in figure 3-4 (cf. ISO 9001, 0.2).

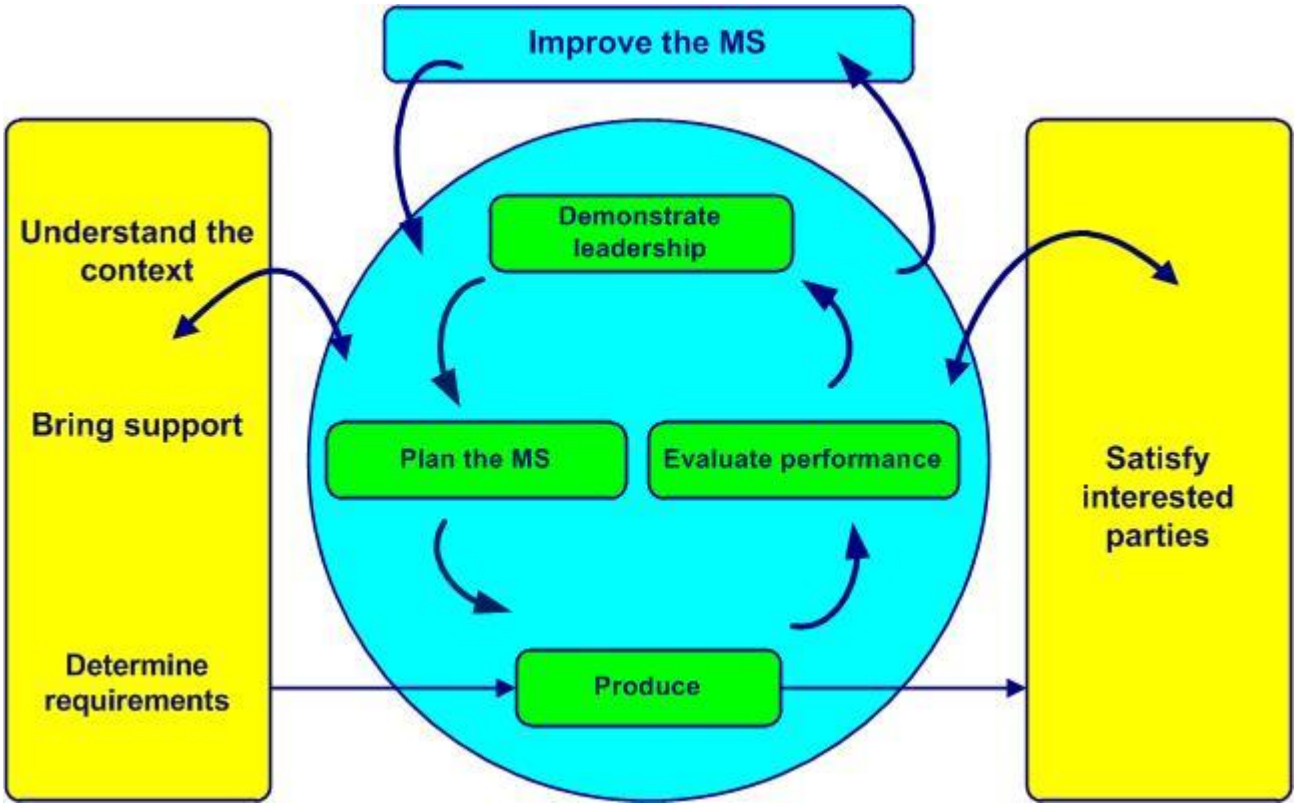


Figure 3-4. Model of an MS-based on the process approach and continual improvement

The process approach (cf. annex 09):

- emphasizes the importance of:
  - understanding and complying with customer requirements
  - prevention so as to react to unwanted elements such as:
    - customer returns
    - waste
  - measuring process performance, effectiveness and efficiency
  - permanently improving objectives based on pertinent measurements
  - process added value
- relies on:
  - methodical identification
  - interactions

    - the sequence and
    - process management, which consists of:
        - determining objectives and their indicators
        - piloting related activities
        - analyzing obtained results
        - permanently undertaking improvements
- allows one to:
    - better view inputs and outputs and their relationship
    - clarify roles and responsibilities
    - judiciously assign necessary resources
    - break down barriers between departments
    - decrease costs, delays and waste
- and ensures in the long run:
    - control
    - monitoring and
    - continual improvement of processes

For a consulting, support or repair business, identifying and defining processes and mapping may not be very useful. More important is to establish and describe for example:

- job descriptions
- staff competence
- the tools to use
- preferred methods for certain recurring cases

The process approach **is not**:

- crisis management ("You will not solve the problems by addressing the effects")
- blaming people (“Poor quality is the result of poor management" - Masaaki Imai)
- prioritizing investments (“Use your brain, not your money" - Taiichi Ohno)

4 Principles

4.1 Value creation

The purpose of risk management is the creation and preservation of value. To achieve the objectives and improve overall performance, the principles listed in paragraphs 4.2 to 4.9 of this module and in clause 4 of the ISO 31000 standard must be scrupulously respected.

As the title of the standard indicates (Risk Management – Guidelines) the ISO 31000 standard does not contain requirements and a company cannot be certified according to this standard. But as we saw in paragraph 1.3 the benefits can be substantial, not to say considerable.

You can check whether you have the presence of mind by answering the questions in the presence of mind test in annex 10. 

True story

In the early 1970s, a project was proposed to Bill Hewlett, one of the founders of HP. It was a small handheld device capable of scientific calculations with ten digits of precision. The prototype was made of wood, with all buttons labeled. Bill Hewlett examined the functions, smiled and slipped the device into his shirt pocket. This would become the HP-35 calculator.

Imposing your will to seize an opportunity can pay off enormously, even when the market is unknown and the technology is not complete.

4.2 Integration

Risk is everyone's business

Integrating risk management into all company processes is a key objective.

All staff should be regularly made aware of the importance of taking risk into account in design, development, industrialization, production and operational support.

4.3 System approach

The system (structured and global) approach to risk management contributes to the achievement of objectives.

This approach is timely and comprehensive. It helps to define priorities and make the right decisions.

4.4 Adaptation to context

Risks cannot be considered outside of the context that gave rise to the risks. Paul Hopkins

Risk management is tailor-made based on the business context, priority objectives and available resources.

It is recommended that the effort to implement risk management be proportionate to the risk level in the company.

True story

A piece of equipment was moved to make room for large new equipment. When planned maintenance was to begin on the first piece of equipment, the maintenance guy was unable to carry out his activities because the equipment was too close to the wall. He suggested creating a door in the wall to allow access to the equipment.

The only problem was that it was an exterior wall!

4.5 Stakeholder participation

The involvement and active participation of stakeholders enable transparent and inclusive risk management.

The knowledge, needs and expectations of stakeholders are better taken into account.

True story

"In a typical business, if you have a meeting, no matter how important, there is always one party that is not represented: the customer. It is therefore very easy within the company to forget the customer." Jeff Bezos.

To remedy this problem of forgetting, he got into the habit of placing an empty chair at each meeting.

 Minute of relaxation. See the "Gold contract" joke.

4.6 Dynamism

Risk management is a journey, not a destination

The internal and external challenges of the business context are constantly changing.

Risk management is dynamic, iterative and responsive to any change.

4.7 Best information

Risk management is based on the best information needed and the communication of the performance obtained.

Information is identified, stored, available, clear and accessible to stakeholders.

4.8 Factors

Human and cultural factors are taken into account at all stages of risk management.

The expectations, specificities and abilities of stakeholders are identified and integrated into activities to better achieve the objectives.

4.9 Improvement

The effectiveness of risk management is continually improved using the training of all staff and the experience of people with strong influence.

Improving risk management takes into account:

- available resources
- stakeholder contribution
- the effectiveness of the existing process
- potential opportunities
- performance monitoring and evaluation

 Minute of relaxation. Cf. the “The quality engineer and the shepherd” joke.