D 26v19

Business continuity

Goal of the module: Readiness for the implementation, certification, maintenance and improvement of your business continuity management system (ISO 22301) in order to:
- **ensure the protection of the company against major crises**
- **reduce the likelihood of disruptive events occurring**
- **increase confidence in the resilience of the company**

1 Business continuity

1.1 History

<p style="text-align:center">**Any decision involves a risk. Peter Barge**</p>

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 was consultant in risk analysis for making risky or uncertain decisions.

In Mesopotamia, around 3900 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 2400 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 start of the 21st century.

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.

<p style="text-align:center">**No-risk situations do not exist**</p>

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

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 an essential necessity, even the ISO 9001 standard (quality management systems – requirements) since the 2015 version has included the risk approach.

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.

Business continuity management is also relatively recent. One of the first standards concerning the business continuity management system (BCMS) dates from 2003: BSI PAS 56, Guide to Business Continuity Management, (see paragraph 2.2).

The first edition of the ISO 22301 standard ("Societal security – Business continuity management systems – Requirements") dates from 2012.

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

Some differences between risk management and business continuity management are shown in Table 1-1:

Table 1-1. Differences

	Risk management	**Business continuity management**
Purpose	Risk reduction	Survival (resilience) of the company
Activity	Daily incident	Major disruption
Scope	A department	The company
Method	Risk analysis	Impact analysis
Subjects concerned	Likelihood and impact	Direct and long term impact

True story

A fire breaks out in a computer center. The damage is enormous because the situation will be restored after more than a month.

The center had signed a backup contract with an external service provider.

But the contract did not include a fire guarantee and had not been properly tested.

According to an Eagle Rock Alliance survey, 40% of companies surveyed believe that 72 hours of interruption of their IT system is a critical time before the risk of bankruptcy.

The main objective of business continuity management is to ensure the survival of the business in all circumstances.

1.2 Implementation

Preparing for the worst is a realistic and pragmatic view of the world

The establishment and implementation of the ISO 22301 business continuity management system is shown in figure 1-1.
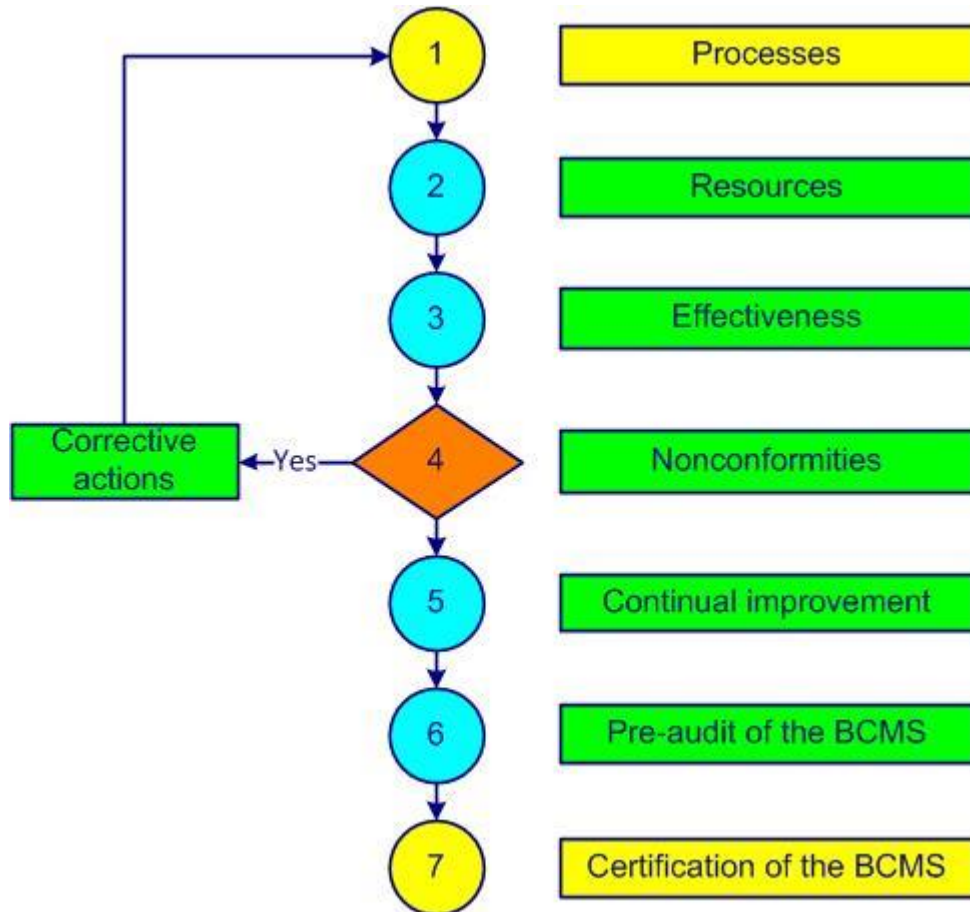

Figure 1-1. Implementation of the BCMS

Step 1 consists of explaining the importance of having a BCMS, identifying and defining the **processes**, interactions, owners, responsibilities and drafts of certain documents. With the participation of as many people as possible, the first versions of business continuity plans are drawn up.

In **step 2**, the **resources** necessary to achieve the business continuity policy and objectives are set. A plan of tasks, responsibilities and deadlines is established. Training for internal auditors is taken into account.

Step 3 allows you to define and implement methods to measure the **effectiveness** and efficiency of each process and business continuity plans. Internal audits make it possible to assess the degree of implementation of the BCMS.

Nonconformities of all kinds are listed in **step 4**. An outline of the various deviations is established. Corrective actions are implemented and documented.

An initial assessment of the tools and the scope of the **continual improvement** process is made in **step 5**. Risks are determined, actions are planned and opportunities for improvement are found. Internal and external communication is established and formalized.

To perform the BCMS **pre-audit** (**step 6**) the BCMS documentation is verified and approved by the appropriate people. A management review makes it possible to assess compliance with applicable requirements. The business continuity policy and objectives are finalized. A business continuity manager from another company or a consultant will be able to provide valuable comments, suggestions and recommendations.

When the system is correctly implemented and respected, **certification of the BCMS** by an external body becomes a formality (**step 7**).

An example of an ISO 22301 Certification project plan with 26 steps is presented in annex 01.

A relevant method for assessing the level of performance of your business continuity management system is the RADAR logic of the EFQM (European Foundation for Quality Management) excellence model with its 9 criteria and its overall score out of 1000 points.

The PDCA cycle, or Deming cycle (figure 1-2) applies to the control of any process. PDCA cycles (Plan, Do, Check, Act) are a universal basis for continual improvement.
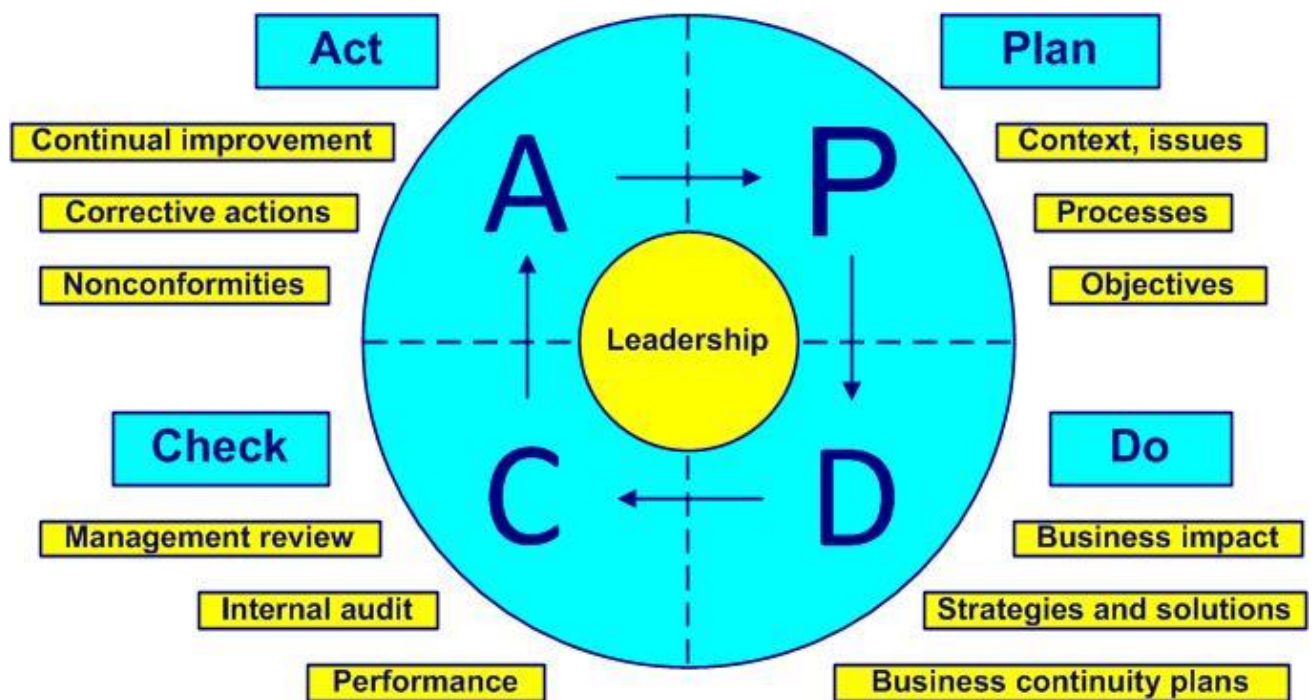

Figure 1-2. The Deming cycle

- Plan, define the context, issues and processes, demonstrate leadership, establish business continuity policy and objectives, address risks (clauses 4, 5, 6 and 7)
- Do, demonstrate leadership, analyze the business impact, provide support, establish strategies and solutions, carry out business continuity plans and test them (clauses 5, 7 and 8)
- Check, demonstrate leadership, evaluate, inspect, conduct audits and management reviews (clauses 5 and 9)

- Act, adapt, demonstrate leadership, address nonconformities, react with corrective actions and find new improvements (new PDCA), (clauses 5 and 10)

To deepen your knowledge of the Deming cycle and its 14 points of management theory you can consult the book "Out of the crisis" W. Edwards Deming, published for the first time in 1982, cf. paragraph 2.3.

1.3 Benefits

Preparing for war in peacetime

Often the decision to implement a BCMS and BCPs is taken after having suffered a crisis or a situation very close to a financial catastrophe.

Incidents, accidents, crises, disasters and catastrophes don't just happen to others!

Each disruption is specific and often causes unexpected and different damage. Preparing for these events of natural origin (earthquake, flood, fire) or human origin (terrorism, cyber attack, loss of qualified personnel) can only benefit us.

One response to a partial or total disruption, potential or actual, is to have a business continuity plan and a designated crisis team. Then you will be able to reduce certain risks, mitigate impacts and recover priority activities during and after a disruption.

Expected benefits of business continuity management:

- prevent crisis situations
- strengthen your resilience by assessing and reducing the consequences of a crisis
- maintain vital business operations during a disruption
- put in place civil protection tools and equipment
- raise awareness and train staff on the behavior to adopt in the event of a crisis
- protect the company's assets
- reduce insurance costs (renegotiation of the contract)
- protect and improve the reputation of the company
- strengthen stakeholder confidence
- consolidate competitive advantage
- meet legal and regulatory requirements
- anticipate disruptive incidents and reduce the risk of disaster
- have effective processes to guarantee business continuity
- establish a reliable basis for decision-making in times of crisis
- analyze and understand the main threats and areas of vulnerability
- increase the likelihood of achieving objectives
- increase the opportunities to be seized
- reduce losses

True story

Amazon, a global leader in e-commerce, implemented ISO 22301 to improve customer confidence in the company's ability to maintain its services in the event of a major incident.

ISO 22301 certification has allowed Amazon to demonstrate its commitment to the continuity of its services and to reassure its customers.

Amazon saw an increase in customer trust, demonstrating the importance of business continuity for e-commerce customers.

He who apologizes accuses himself

Common excuses for failure:

- it was the responsibility of top management
- this was not an explicit requirement in the contract
- how to 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 Business continuity 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.

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

- combination of the probability of occurrence of damage and its severity. 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. MRI (2013)
- effect of uncertainty on the achievement of objectives. ISO Guide 73 (2009)
- effect of uncertainty on objectives. ISO 22301 (2019)
- 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 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 extent of the potential loss. Evan Picoult
- 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 opportunity*

Identifying hazard means asking yourself what could go wrong

Often risk is equated with danger and commonly used instead of threat.

Uncertainty and probability are subjective notions with fictitious quantities.

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.

Some definitions and abbreviations:

Activity: *set of tasks to obtain a deliverable*
BCP: business continuity plan
Benchmarking*: comparative analysis method in connection with one or more competitors*
Business impact analysis (BIA): *analysis of the impact of a disruption on the business*
Brainstorming*: method allowing the development of ideas from the participants in order to find solutions*
Brainstorming*: method allowing the development of ideas from the participants in order to find solutions*
Business continuity management system (BCMS): *set of processes enabling business continuity objectives to be achieved*
Business continuity management: *method aimed at ensuring that in the event of a crisis, critical functions remain operational or become operational again as quickly as possible (see also resilience)*
Business continuity manager: leader to the resilience journey
Business continuity: *the ability of a company to continue delivering products and providing services during and after a disruption*
Disruption: *incident which results in deviation from the delivery of products and the provision of services*
Fail safe device*: system allowing the prevention of errors by eliminating the human factor*
FMEA*: Failure Mode and Effects Analysis*
Hazard*: situation that could lead to an incident*
Impact*: consequence of an event affecting the objectives*
Kaizen*: from Japanese kai - change, zen - better. Continual improvement step by step to create more value and less waste. Approach based on common sense and staff awareness*
Likelihood: *possibility that something happens*
Monitoring*: pack of planned actions to guarantee the effectiveness of the critical control points*
MTPD: *maximum tolerable period of disruption*
Non-quality: *gap between expected quality and perceived quality*
Opportunity: *uncertain event that could have a favorable impact*
Requirement: *explicit or implicit need or expectation*
Resilience*: the ability to resolve a crisis and continue to function as before*
Responsibility*: capacity to make a decision alone*
Risk analysis: *methodical analysis of the existence of a hazard to understand its nature and to facilitate the adoption of control measures*
Risk assessment: *risk identification, analysis and evaluation process*
Risk criteria: *indices to assess the importance of the risk*
Risk estimation: *activities to assign values to the likelihood and impact of risk*
Risk evaluation: *risk assessment activities to determine whether the risk is acceptable*
Risk factor (peril, danger): *element likely to cause a risk*
Risk identification: *risk assessment activity to find and describe risks*
Risk level: *criticality of the risk according to the impact and likelihood*
Risk management plan*: risk management planning including approach, steps, methods, resources*

Risk management system: *set of processes allowing the achievement of the risk objectives*
Management system (MS): *set of processes allowing objectives to be achieved*
Risk management: *activities to restrict the possibility that something goes wrong*
Risk measurement: *set of possibilities with quantified probabilities and losses*
Risk owner: *person with responsibility and authority to manage risk*
Risk prevention: *activities based on decreasing risk likelihood of occurrence*
Risk protection: *activities based on reducing risk impacts*
Risk register*: folder containing information relating to identified risks*
Risk severity*: measuring the impact of the risk*
Risk threshold*: acceptance (below) or non-tolerance (above) limit*
Risk treatment: *risk reduction activities*
Security*: ability to avoid an unwanted event*
Strategy*: total approach to achieve objectives*
SWOT: *Strengths, Weaknesses, Opportunities, Threats. Tool for structuring a risk analysis*
System: *set of interacting processes*
Threat *uncertain event that could have a negative impact on the objectives*
Uncertainty*: existence of more than one possibility*
Waste*: anything that adds cost but no value*

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, 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
    - control is meeting the objectives
    - optimize is searching 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, the source which can lead to an accident
    - the problem is the gap between the actual situation and the desired situation

- o risk is the measure, the consequence of a hazard and it is always a potential problem
- inform and communicate
    - o to inform is to give someone meaningful data
    - o to communicate is to pass on a message, to listen to the reaction and discuss
- mapping and organization chart
    - o mapping is the graphical presentation of processes and their interactions in a company
    - o the organizational chart is the graphic presentation of the departments and their links in a company
- objective and indicator
    - o an objective is a sought after commitment
    - o an indicator is the information on the difference between the pre-set objective and the achieved result
- organization and enterprise, society, company
    - o organization is the term used by the ISO 9001 standard as the entity between the supplier and the customer
    - o an enterprise, society and company are examples of organizations
- prevention and protection, cf. figure 2-1
    - o prevention is the means to reduce the likelihood and frequency of occurrence of a risk (check tire pressure)
    - o protection is the means to limit the impact of a risk (fasten your seat belt)
- probability, uncertainty and likelihood
    - o the probability expresses the quantitative analysis of the uncertainty
    - o uncertainty is the inaccuracy of predicting
    - o the likelihood expresses the qualitative analysis of the uncertainty
- process, procedure, product, activity and task
    - o a process is how we satisfy the customer using people to achieve the objectives
    - o a procedure is the description of how we should conform to the rules
    - o a product is the result of a process
    - o an activity is a set of tasks
    - o a task is a sequence of simple operations
- safety and security
    - o safety is prevention against malicious risks
    - o security is prevention against risks of unintentional origin
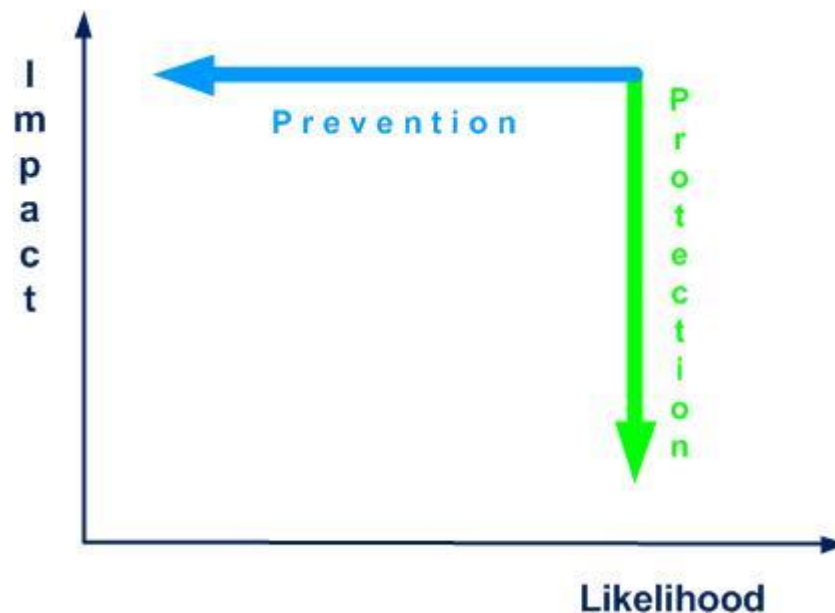
Figure 2-1 Prevention and protection

Remark 1: between stakeholders and interested parties our preference is for stakeholders

Remark 2: between impact, gravity, consequence and severity our preference is for impact

Remark 3: between likelihood and probability our preference is for likelihood (of occurrence)

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 cannot find in this module and annex 06, you can consult:

- ISO Online Browsing Platform (OBP)
- IEC Electropedia

The icons used in the module:

- explanation, example, detail, rule
- process
- procedure (documented)
- record
- joke
- game
- trap to avoid

2.2 Standards

There can be no improvements where there are no standards. Masaaki Imai

Standards and specifications related to risks and business continuity (in chronological order):

- AS 4360 (1995), Risk management
- ANAO Better Practice Guide (2000), Business Continuity Management—Keeping the wheels in motion
- BSI PAS 56 (2003), Guide to Business Continuity Management
- HB 221 (2004), Business Continuity Management
- NFPA 1600 (2004), Standard on Disaster/Emergency Management and Business Continuity Programs
- BS 25999-1 (2006), Business Continuity Management – Part 1: Code of Practice
- FD X50-252 (2006), *Management du risque - Lignes directrices pour l'estimation des risques* (Risk management - Guidelines for risk estimation)
- BS 25999 – 2 (2007), Business continuity management – Specification
- ISO/PAS 22399 (2007), Societal security - Guideline for incident preparedness and operational continuity management
- SI 24001 (2007) Organizational resilience management system (ORMS) – Requirements and guidance for use
- ISO Guide 73 (2009), Risk management - Vocabulary
- ANSI/ASIS SPC1 (2009), Organisational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use
- SS 540 (2008), Singapore Standard for Business Continuity Management (BCM)
- ANSI/ASIS/BSI BCM.01 (2010), Business Continuity Management Systems: Requirements with Guidance for Use
- BP Z74-700 (2011), Repository of best practises - Business Continuiy Plan (BCP)
- ISO/IEC 27031 (2011), Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity
- ISO 22398 (2013), Societal security, Guidelines for exercises
- FD X50-259 (2014), Risk management - Business continuity plan - Implementation and maintenance procedure
- BS 11200 (2014), Crisis management - Guidance and good practice
- FD X50-259 (2014), Risk management - Business continuity plan - Implementation and maintenance procedure
- BS 65000 (2014), Guidance on organizational resilience
- ISO 22316 (2017), Security and resilience - Organizational resilience - Principles and attributes
- ISO 31000 (2018), Risk management - Guidelines
- ISO 19011 (2018), Guidelines for auditing management systems
- ISO/TS 22330 (2018), Security and resilience - Business continuity management systems - Guidelines for people aspects of business continuity
- ISO/TS 22331 (2018), Security and resilience - Business continuity management systems - Guidelines for business continuity strategy
- ISO 22320 (2018), Security and resilience, Emergency management, Guidelines for incident management
- ISO 22301 (2019), Security and resilience - Business continuity management systems - Requirements
- IEC 31010 (2019), Risk management - Risk assessment techniques
- ISO 22313 (2020), Security and resilience - Business continuity management systems - Guidance on the use of ISO 22301
- AS/NZS 5050(Int) (2020), Managing disruption-related risk
- BS 31100 (2021), Risk management. Code of practice

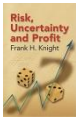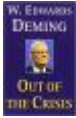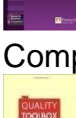- ISO 22300 (2021), Security and resilience - [Vocabulary](#)
- ISO/TS 22317 (2021), Security and resilience - Business continuity management systems - [Guidelines for business impact analysis](#)
- ISO/TS 22318 (2021), Security and resilience - Business continuity management systems - [Guidelines for supply chain continuity management](#)
- ISO 22322 (2022) Security and resilience, Emergency management, [Guidelines for public warning](#)
- ISO/IEC 27001 (2022), Information security, cybersecurity and privacy protection - Information security management systems - [Requirements](#)
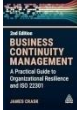
None of these standards are obligatory but as Deming said:

<p align="center">**There is no need to change. Survival is not mandatory**</p>

2.3 Books

To go further, some books, classified in chronological order:

- Frank Knight, [Risk, Uncertainty And Profit](#), University of Chicago Press, 1921

- Edwards Deming, [Out of the crisis](#), MIT Press, 1982

- Peter Bernstein, [Against the Gods](#): The Remarkable Story of Risk, John Wiley & Sons, New York, 1998

- Michael Gallagher, [Business Continuity Management](#) - How to Protect Your Company from Danger, Prentice Hall, 2002

- Nancy Tague, [The Quality Toolbox](#), ASQC Quality Press, 2005

- Douglas Hubbard, [The Failure of Risk Management](#): Why It's Broken and How to Fix It, Wiley, 2009

- team, [Business Continuity For Dummies](#), For dummies, 2012

- Susan Snedaker, [Business Continuity and Disaster Recovery Planning](#) for IT Professionals, Syngress, 2013

- team, [ISO 22301 A Complete Guide](#) - 2021 Edition, The Art of Service, 2020

- Alan Carder, [ISO 22301:2019 and business continuity management](#) - Understand how to plan, implement and enhance a business continuity management system (BCMS), IT GP, 2021

- PECB, [ISO 22301:2019 Auditing Guide](#): A simple and practical guide to auditing a Business Continuity Management System (BCMS), PECB, 2021

- Kris Hermans, [Mastering ISO 22301:2019](#): A Comprehensive Guide to the Business Continuity Management System (BCMS), Independently published, 2023

- Arman Suman, [ISO 22301 Foundation](#) - Study Guide, Kindle, 2023

- James Crask, [Business Continuity Management](#): A Practical Guide to Organization Resilience and ISO 22301, KoganPage, 2024

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

3 Process approach

3.1 Types of processes

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

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 suppliers

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

- title and type
- purpose (why?)
- beneficiary (for whom?)
- scope and activities
- initiators
- documented information
- inputs
- outputs (intentional and not intentional)
- restraints
- 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 conducted periodically by the process owner (cf. annex 03).

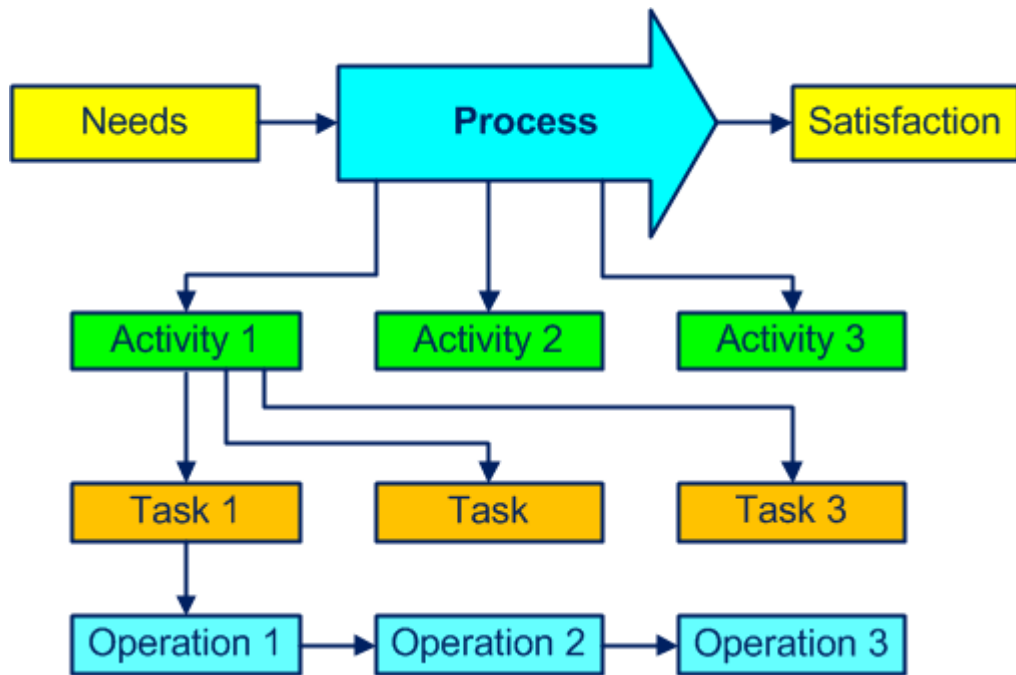The components of a process are shown in figure 3-1:

Figure 3-1. Components of a process

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

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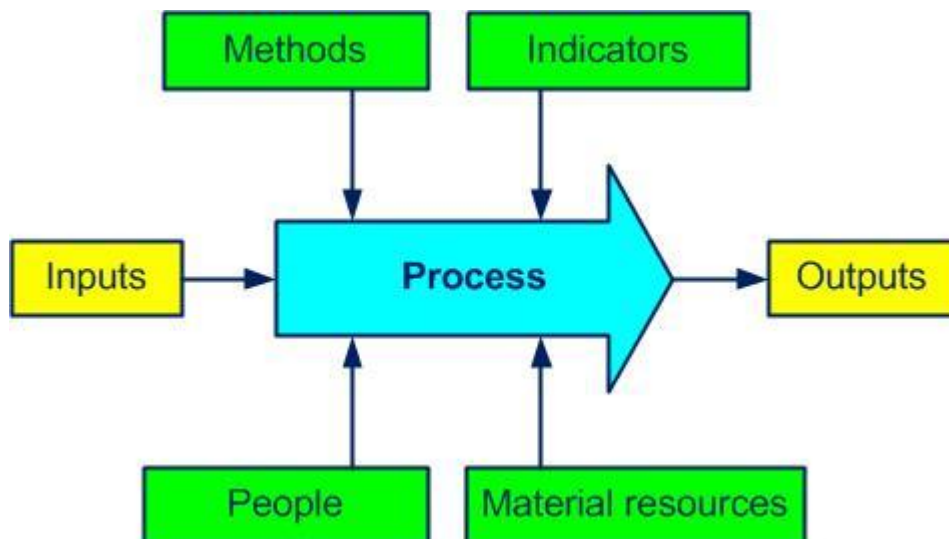- with what, which machines, which equipment? (material resources)

Figure 3-2. Elements of a process

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

You can find some examples of process sheets 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 meet 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 documented information to maintain and recall the purpose of the process.

The processes are (as we shall see in the following paragraphs) of management, realization and support types. Do not attach too much importance to process categorizing (sometimes it's 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 elaboration of the policy, deployment of the objectives and all needed checks. They are the glue of all the realization and support processes.

The following processes can be part of this family (* mandatory, cf. annex 04):

- develop strategy
- address risks
- assess risks * (paragraph 8.2.3)
- control operational risks
- develop emergency plans
- investigate an incident
- meet requirements
- develop policy
- establish process ownership
- improve
- conduct an audit * (paragraph 9.2.2)
- communicate
- plan the MS
- acquire and manage resources
- evaluate performance
- conduct management review
- 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 (* mandatory):

- meet legal and regulatory requirements * (paragraph 4.2.2)
- design and develop
- purchase components
- sell products

- produce
- maintain equipment
- inspect production
- analyze business impact * (paragraph 8.2.1)
- anticipate emergencies
- recover activities * (paragraph 8.4.5)
- apply traceability (identify and keep history)
- receive, store and deliver
- control nonconformities
- implement 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 Mapping

Par excellence process "mapping" is a multidisciplinary work. This is not a formal requirement of the ISO 22301 standard but is always welcome.

The three types of processes and some interactions are shown in figure 3-3.
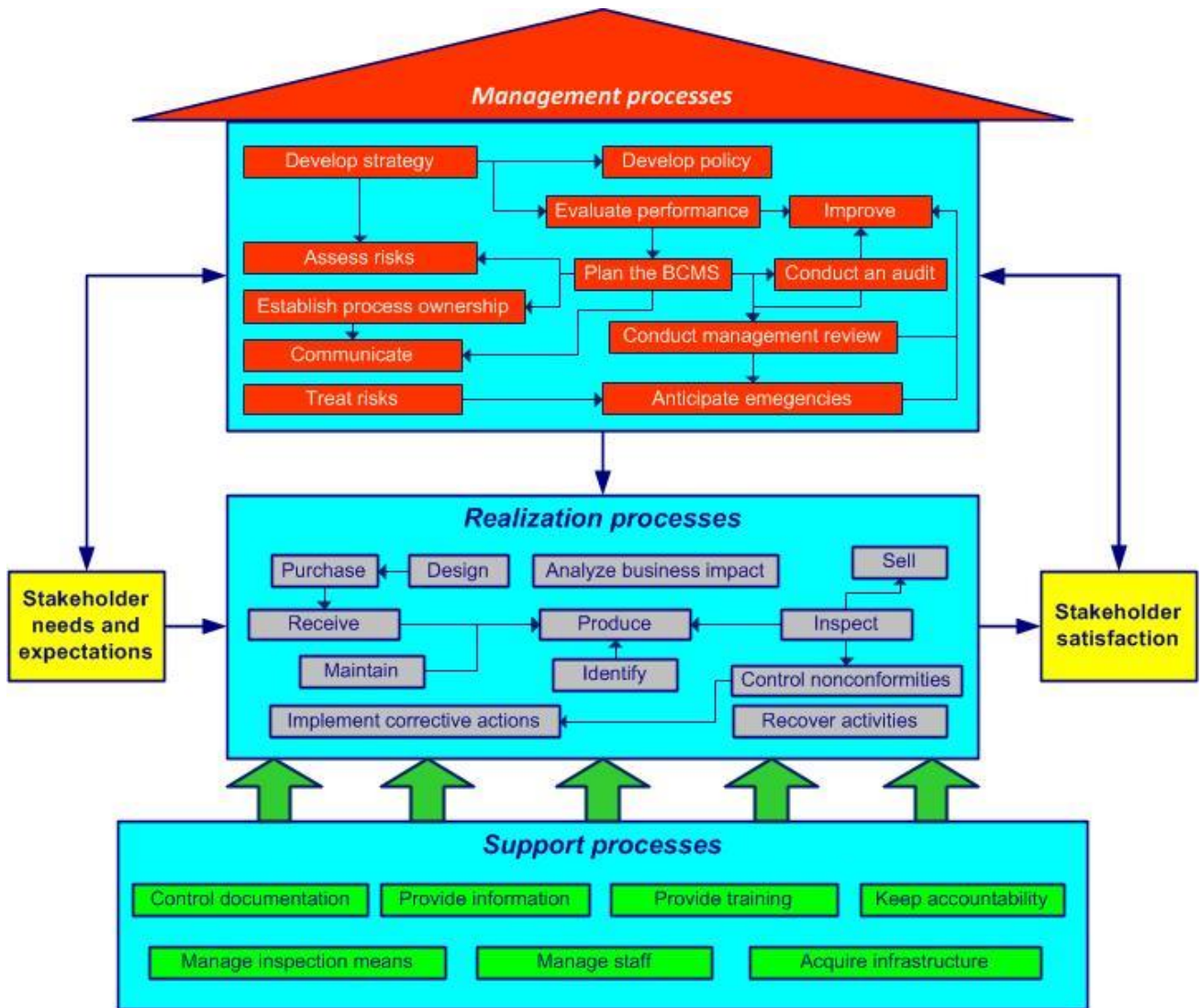
Figure 3-3. The process house

Mapping, among other things, allows you to:

- obtain a global vision of the company
- identify the beneficiaries (customers), flows and interactions
- define rules (simple) 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
- address risks
- meet requirements
- develop policy
- plan the MS
- deploy objectives
- acquire resources
- establish process ownership
- improve

A list of Specific processes is shown in annex 04.

3.3 Process approach

Simple solutions for now, perfection for later

The fourth principle of quality management is "Process approach", cf. ISO 9000, 2.3.4. Some benefits:

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

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

The integrated process approach during the development, implementation and continual improvement of a management system makes it possible to achieve the objectives linked to the protection of the company against crises, as shown in figure 3- 4.
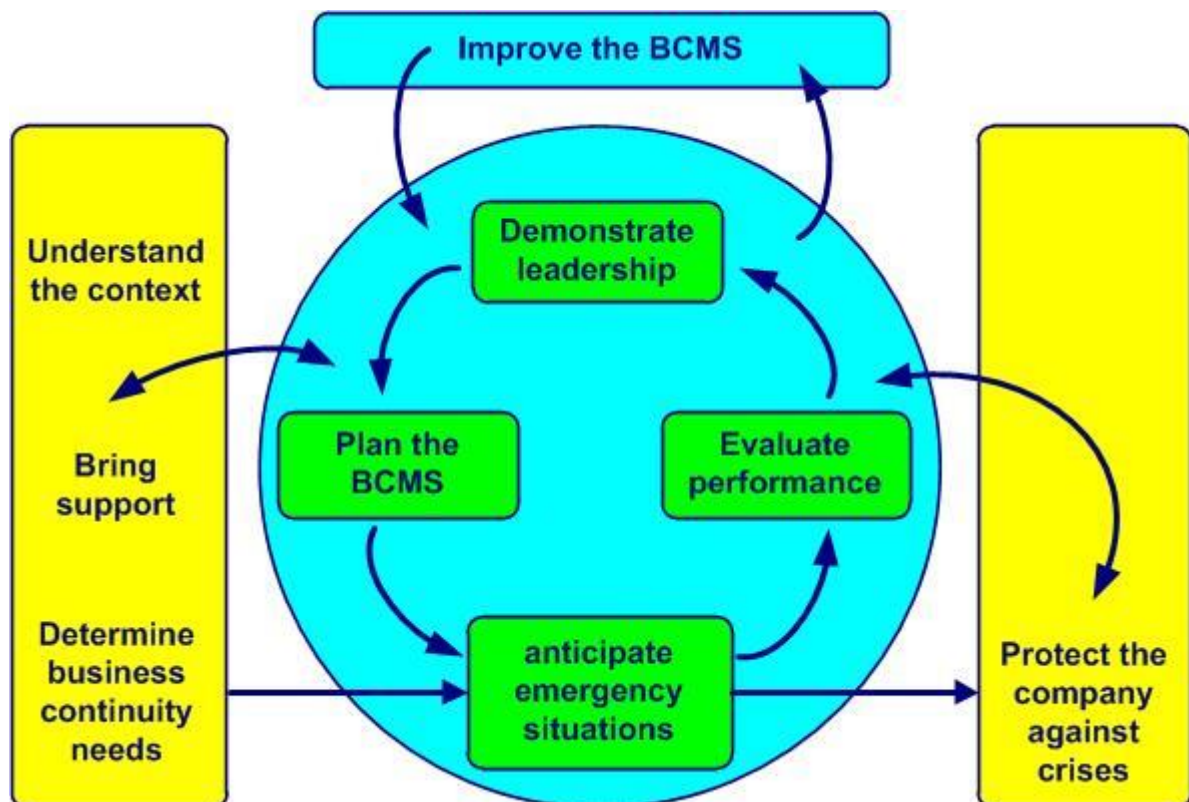

Figure 3-4. Model of a BCMS based on process approach and continual improvement

The Process approach (cf. annex 05):

- emphasizes the importance of:
  - understanding and complying with business continuity requirements
  - prevention so as to react to unwanted elements such as:
    - incidents
    - crises
    - catastrophes

- o measuring process performance
- o permanently improving objectives based on pertinent measurements
- o process added value
- relies on:
  - o methical identification
  - o interactions
  - o the sequence and
  - o process management, which consists of:
    - ▪ determining objectives and their indicators
    - ▪ piloting related activities
    - ▪ analyzing obtained results
    - ▪ permanently undertaking improvements
- allows one to:
  - o better view inputs and outputs and their relationship
  - o clarify roles and responsibilities
  - o judiciously assign necessary resources
  - o break down barriers between departments
  - o decrease costs, delays and waste
- and ensures in the long run:
  - o control
  - o monitoring and
  - o continual improvement of processes

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 Context

4.1 Context of the company *(requirement 1)*

The two most important things in a company do not appear in its balance sheet: its reputation and its people. Henry Ford

To successfully implement a quality management system, we must understand and evaluate everything that can influence the reason for being and business performance. You should think carefully about a few key activities:

- develop a thorough diagnosis of the unique context in which your company exists, taking into account:
    - external issues such as the environment like:
        - social
        - regulatory
        - economic
        - technology
    - internal issues like:
        - specific aspects of the corporate culture:
            - vision
            - rationale, purpose and mission
            - core values
        - staff
        - products and services
        - infrastructure
- monitor and review regularly any information relating to external and internal issues
- analyze the factors that may influence the achievement of business objectives

The SWOT and PESTEL analyses can be useful for relevant analysis of business context (cf. annex 07).

A list of external and internal issues is carried out by a multidisciplinary team. Each issue is identified by its level of influence and control. Priority is given to issues with great influence and poor control.

Good practices

- *the diagnosis of the context includes the main external and internal issues*
- *essential values such as corporate culture are taken into account*
- *the results of the context analysis are widely communicated*
- *SWOT analysis helps identify the main threats and opportunities*

Bad practices

- *issues in the business context such as the regulatory environment are not taken into account*
- *in some cases corporate culture is not taken into account*
- *the threats and weaknesses identified in the SWOT analysis remain without action*

4.2 Needs and expectations of stakeholders *(requirements 2 to 6)*

There is only one valid definition of a business purpose: to create a customer. Peter Drucker

To understand the needs and expectations of interested parties, we must begin by determining those who may be affected by the business continuity management system, such as:

- employees
- customers
- external providers
- owners
- shareholders
- bankers
- distributors
- competitors
- citizens
- neighbors
- social and political organizations

Every stakeholder is determined by its level of influence and control. Priority is given to stakeholders with great influence and poor control. A List of stakeholders is created by a multidisciplinary team, cf. annex 08.

True story

The customer is king but we can still fight against rudeness. Example of the Nice restaurant La petite Syrah and coffee prices:

"A coffee"............................7 €
"A coffee, please"............4,25 €
"Hello, a coffee, please"....1,40 €

Anticipating the reasonable and relevant needs and expectations of stakeholders involves:

- meeting legal and statutory requirements
- preparing to address threats
- finding improvement opportunities

The Identify legal requirements process of business continuity allows you to take into account the mandatory requirements and comply with them.

Requirements may concern:

- incident response (emergency management)
- business continuity (business continuity plan, exercise program)
- risk management
- hazard management (chemical materials)

When an applicable requirement is accepted, it becomes an internal requirement of the BCMS.

Good practices

- *the list of stakeholders is updated*
- *stakeholder needs and expectations are established through on-site meetings, surveys, round tables and meetings (monthly or frequent)*
- *the application of legal and regulatory requirements is a preventive approach and not a constraint*

Bad practices

- *regulatory and legal requirements are not taken into account*
- *stakeholder expectations are not determined*
- *the list of stakeholders does not contain their field of activity*

4.3 Scope of the BCMS *(requirements 7 to 15)*

In many areas, the winner is the one who is best informed. André Muller

The scope (or in other words the perimeter) of this module applies to the business continuity management system (or in other words to crisis risk management) in the company and concerns:

- the localization
- products and services
- activities and processes
- the resources

The Scope of the BCMS is available to stakeholders, cf. annex 09.

When a requirement cannot be applied, a justification is included in the document.

The scope of a company BCMS is established taking into account:

- its reason for being
- its products and services
- its context (internal and external issues)
- stakeholder requirements
- the complexity of its structure

Questions that require answers:

- what is the most vulnerable company activity?
- what is the maximum tolerable level of disturbance?

- what are the applicable regulatory obligations?
- what are the priority risks?
- what crisis can surprise us?
- is the crisis team prepared?
- how to protect staff and work tools?
- what is the plan to maintain part of the activity?
- how to restore normal activity as quickly as possible?

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

- financial crises
- insurance
- 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), 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.

Business continuity concerns many areas and risks:

- the staff
- the reputation of the company
- products and projects
- insurance
- supply disruption
- lack of skills
- terrorist threats
- natural disasters

To properly determine the scope of the BCMS, the specificities of the company context are taken into account, such as:

- the issues (cf. paragraph 4.1)
- products and services
- corporate culture
- the environment:
    - o   social
    - o   financial
    - o   technological
    - o   economical
- stakeholder requirements (cf. paragraph 4.2)
- outsourced processes

Good practices

- *he scope is relevant and available on simple request*

- *non-applicable requirements are justified in writing*

Bad practices

- *certain workshops are outside the scope of the BCMS without justification*
- *the scope is obsolete (the new subsidiary is not included)*

4.4 Business continuity management system *(requirement 16)*

Prevention is better than cure

The requirements of the ISO 22301 standard concern:

- the context of the company
- business continuity policy and objectives
- response to disruptions
- evaluation of the performance of the BCMS
- continual improvement of the BCMS

For that:

- the business continuity management system is:
  - established
  - documented (a simple and sufficient documentary system is put in place)
  - implemented and
  - continually improved
- the business continuity policy, objectives, resources and work environment are determined
- threats are identified and actions to reduce them are established (cf. paragraph 6.1)
- the essential processes necessary for the BCMS are mastered:
  - the corresponding resources assured
  - the input and output elements determined
  - the necessary information available
  - named owners (responsibilities and authorities defined)
  - the sequences and interactions determined
  - each process is measured and monitored (established criteria), objectives are established and performance indicators analyzed
  - process performance is evaluated
  - the necessary changes are introduced to achieve the expected results
  - actions to achieve continual process improvement are established
- the bare minimum necessary ("as much as necessary") of process documents are maintained and retained ( )

Pitfalls to avoid:

- going overboard on quality:
  - an unnecessary operation is carried out without adding value – it is waste, cf. D 12 quality tools

- having all procedures written by the business continuity manager:

o safety is everybody's business, "the staff is conscious of the relevance and importance of each to the contribution to objectives", which is even more true for department heads and process owners

- forgetting to take into account the specificities related to the corporate culture:
  o innovation, luxury, secrecy, authoritarian management (Apple)
  o strong culture related to ecology, action and struggle, while cultivating secrecy (Greenpeace)
  o fun and quirky corporate culture (Michel & Augustin)
  o liberated company, the man is good, love your customer, shared dream (Favi, cf. T 50)

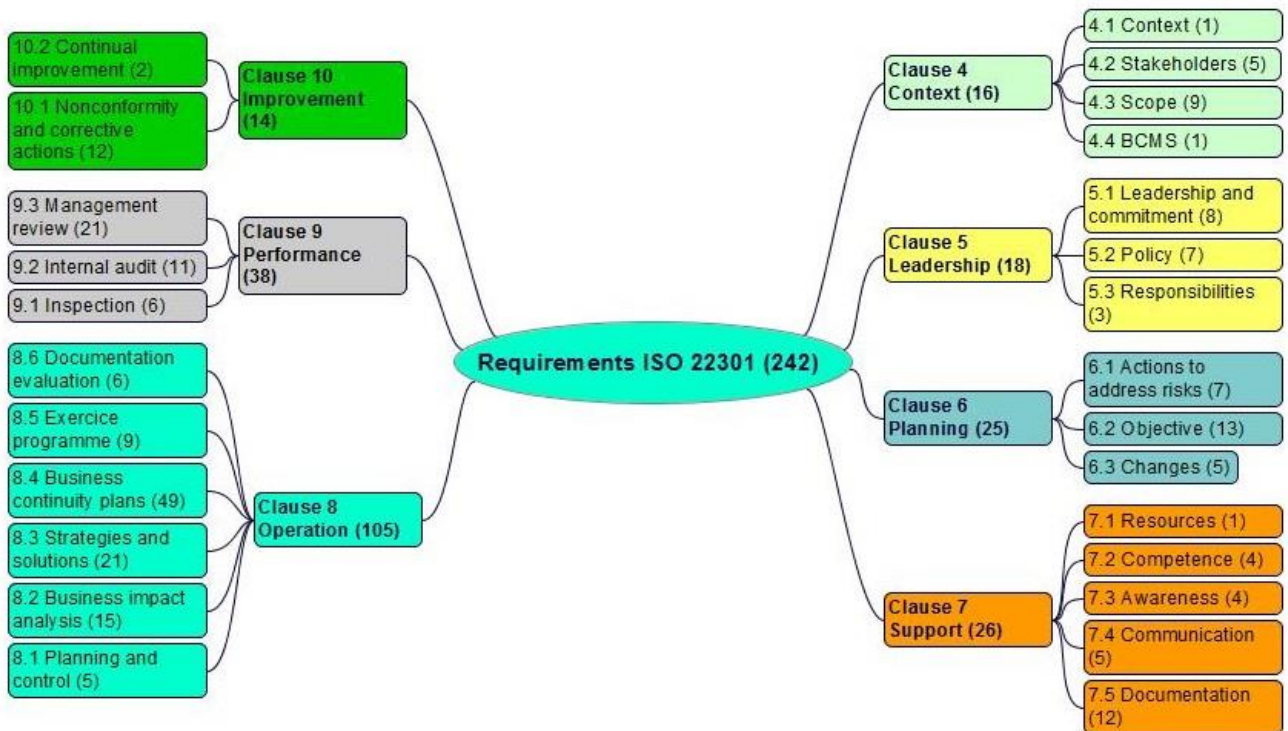The requirements of the ISO 22301 standard are shown in 4-1:

Figure 4-1. The requirements of ISO 22301

An effective BCMS is mainly oriented towards:

- the potential consequences
- the capacity of critical activities
- team simulation exercises
- flexible responses

Do not hesitate to look for answers in ISO 22313 ("Guidance on the use of ISO 22301") when you cannot find them in this module, cf. paragraph 2.2.

Good practices

- *the process map contains enough arrows to clearly show who the customer is (internal or external)*
- *many arrows (multiple customers) are used for processes (no customer is forgotten)*
- *during the process review the added value of the process is clearly revealed*

- *process performance analysis is an example of proof of continual improvement of BCMS effectiveness*
- *top management regularly monitors objectives and action plans*
- *top management commitments relating to continual improvement are widely communicated*
- *the purpose of each process is clearly defined*

<div style="background:orange; text-align:center">**Bad practices**</div>

- *some process output elements are not correctly defined (customers not taken into account)*
- *process efficiency criteria not established*
- *non-formalized process owner*
- *outsourced processes not determined*
- *very real activities are not identified in any process*
- *control of outsourced services not described*
- *sequences and interactions of certain processes are not determined*
- *criteria and methods to ensure the performance of processes are undefined*
- *monitoring of the performance of certain processes not established*
- *BCMS resources do not enable business continuity objectives to be achieved*
- *the BCMS is not updated (new processes not identified)*