D 26v19

**Business continuity**

|  |  |
| --- | --- |
| **Goal**  [**1 Business continuity**](#SM1)  **1.1 History**  **1.2 Implementation**  **1.3 Benefits**  [**2 Definitions, standards and books**](#SM2)  **2.1 Definitions**  **2.2 Standards**  **2.3 Books**  [**3 Process approach**](#SM3)  **3.1 Types of processes**  **3.2 Mapping**  **3.3 Process approach**  [**4 Context**](#SM4)  **4.1 Context of the company**  **4.2 Stakeholders**  **4.3 Scope**  **4.4 BCMS**  [**5 Leadership**](#SM5)  **5.1 Leadership and commitment**  **5.2 Policy**  **5.3 Roles and responsibilities**  [**6 Planning**](#SM6)  **6.1 Risks**  **6.2 Objectives**  **6.3 Changes** | [**7 Support**](#SM7)  **7.1 Resources**  **7.2 Competence**  **7.3 Awareness**  **7.4 Communication**  **7.5 Documentation**  [**8 Operation**](#SM8)  **8.1 Planning and control**  **8.2 Business impact**  **8.3 Strategies**  **8.4 Business continuity plans**  **8.5 Exercise program**  **8.6 Evaluation**  [**9 Performance**](#SM9)  **9.1 Inspection**  **9.2 Internal audit**  **9.3 Management review**  [**10 Improvement**](#SM10)  **10.1 Nonconformity**  **10.2 Continual improvement**  **Annexes** |
|  |  |

**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**

Any decision involves a risk. Peter Barge

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.

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 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.

No-risk situations do not exist

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 a 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.*

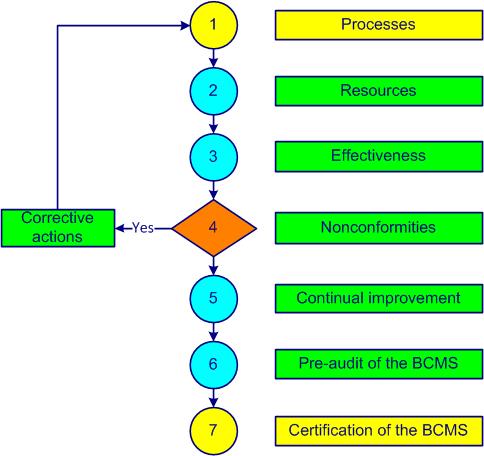
According to an Eagle Rock Alliance survey, 40% of companies surveyed believe that 72 hours of interruption of their IT system is a critical time before the risk of bankruptcy.

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.

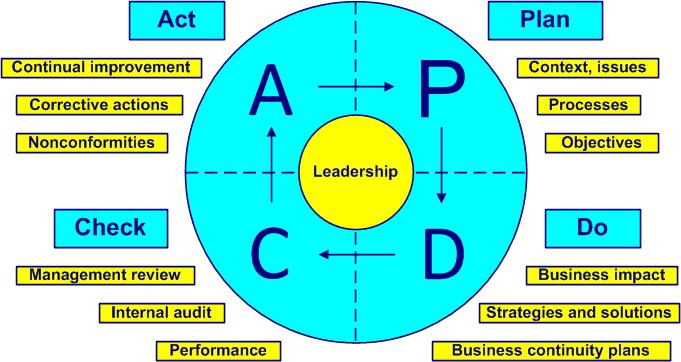
To perform the BCMS **pre-audit** (**step 6**) the BCMS documentation is verified and approved by the appropriate people. A management review makes it possible to assess compliance with applicable requirements. The business continuity policy and objectives are finalized. A business continuity manager 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*](https://efqm.org/) (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” by 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 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 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 hazards 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*

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: *ability of a company to continue delivering products and providing services during and after a disruption*

Conformity: *fulfillment of a specified requirement*

Corrective action*: action to eliminate the causes of nonconformity or any other undesirable event and to prevent their recurrence*

Customer*: anyone who receives a product*

Disruption: *incident which results in deviation from the delivery of products and the provision of services*

Effectiveness: *capacity to realize planned activities with minimum effort*

Efficiency*: financial relationship between achieved results and used resources*

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*

Management system (MS): *set of processes allowing objectives to be achieved*

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*: 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*

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*

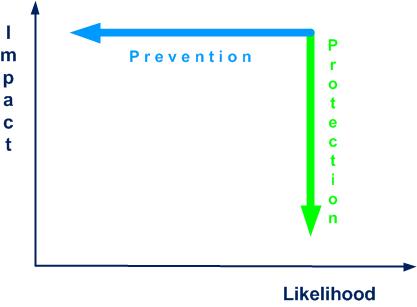
Threat: *uncertain event that could have a negative impact on the objectives*

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
  + 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
* mapping and organization chart
  + mapping is the graphical presentation of processes and their interactions in a company
  + the organizational chart is the graphic presentation of the departments and their links in a company
* 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 2-1
  + prevention is the means to reduce the likelihood and frequency of occurrence of a risk (check tire pressure)
  + protection is the means to limit the impact of a risk (fasten your seat belt)
* probability, uncertainty and likelihood
  + the probability expresses the quantitative analysis of the uncertainty
  + uncertainty is the inaccuracy of predicting
  + the likelihood expresses the qualitative analysis of the uncertainty
* 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
* safety and security
  + safety is prevention against malicious risks
  + 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*

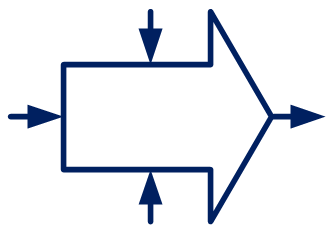
*Remark 3: between likelihood and probability our preference is for likelihood (of occurrence)*

*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*](https://www.iso.org/obp/ui#home))
* IEC [*Electropedia*](http://www.electropedia.org/)

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):

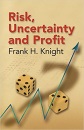
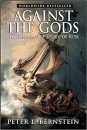
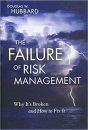
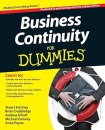
* AS 4360 (1995), [Risk Management](https://infostore.saiglobal.com/preview/as/as4000/4300/4360-1995(%2ba2).pdf?sku=381545)
* ANAO Better Practice Guide (2000), [Business Continuity Management](https://www.anao.gov.au/sites/default/files/anao_report_2002-2003_53.pdf)—Keeping the wheels in motion
* BSI PAS 56 (2003), [Guide to Business Continuity Management](https://global.ihs.com/doc_detail.cfm?document_name=BS%20PAS%2056&item_s_key=00410326)
* HB 221 (2004), [Business Continuity Management](https://infostore.saiglobal.com/en-au/standards/hb-221-2004-131103_saig_as_as_277729/)
* NFPA 1600 (2004), [Standard on Disaster/Emergency Management and Business Continuity Programs](https://emacintl.com/docs/nfpa1600.pdf)
* BS 25999-1 (2006), Business Continuity Management – Part 1: [Code of Practice](https://fr.wikipedia.org/wiki/BS_25999_Management_de_la_Continuit%C3%A9_d%27Activit%C3%A9)
* FD X50-252 (2006), [*Management du risque*](https://www.boutique.afnor.org/norme/fd-x50-252/management-du-risque-lignes-directrices-pour-l-estimation-des-risques/article/694541/fa136845) *- Lignes directrices pour l'estimation des risques* (Risk Management - Guidelines for Risk Estimation)
* BS 25999 – 2 (2007), Business Continuity Management – [Specification](https://fr.wikipedia.org/wiki/BS_25999_Management_de_la_Continuit%C3%A9_d%27Activit%C3%A9)
* ISO/PAS 22399 (2007), Societal Security - [Guideline for Incident Peparedness and Operational Continuity Management](https://www.iso.org/standard/50295.html)
* SI 24001 (2007) Organizational Resilience Management System (ORMS) – [Requirements and Guidance for Use](https://www.sii.org.il/en/24001)
* ISO Guide 73 (2009), Risk Management - [Vocabulary](https://www.boutique.afnor.org/en-gb/standard/fd-iso-guide-73/risk-management-vocabulary/fa156519/34732)
* ANSI/ASIS SPC1 (2009), [Organisational Resilience](https://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf): Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use
* SS 540 (2008), [Singapore Standard for Business Continuity Management](https://www.singaporestandardseshop.sg/Product/SSPdtDetail/235b31c7-7d39-4282-9205-6e4a5a3f7805) (BCM)
* ANSI/ASIS/BSI BCM.01 (2010), [Business Continuity Management Systems](https://webstore.ansi.org/standards/bsi/asisbsibcm012010-2404831): Requirements with Guidance for Use
* BP Z74-700 (2011), Repository of Best Practises - [Business Continuiy Plan](https://www.boutique.afnor.org/en-gb/standard/bp-z74700/business-continuiy-plan-bcp/fa172269/1137) (BCP)
* ISO/IEC 27031 (2011), Information Technology - Security Techniques - [Guidelines for Information and Communication Technology Readiness for Business Continuity](https://www.iso.org/standard/44374.html)
* ISO 22398 (2013), Societal Security, [Guidelines for Exercises](https://www.iso.org/standard/50294.html)
* FD X50-259 (2014), Risk Management - [Business Continuity Plan](https://www.boutique.afnor.org/en-gb/standard/fd-x50259/risk-management-business-continuity-plan-implementation-and-maintenance-pro/fa175949/42762) - Implementation and Maintenance Procedure
* BS 11200 (2014), [Crisis Management](https://shop.bsigroup.com/ProductDetail/?pid=000000000030274343) - Guidance and Good Practice
* BS 65000 (2014), [Guidance on Organizational Resilience](https://shop.bsigroup.com/ProductDetail/?pid=000000000030258792)
* ISO 22316 (2017), [Security and Resilience](https://www.iso.org/standard/50053.html) - Organizational Resilience - Principles and Attributes
* ISO 31000 (2018), Risk Management - [Guidelines](https://www.iso.org/standard/65694.html)
* ISO 19011 (2018), [Guidelines for Auditing Management Systems](https://www.iso.org/standard/70017.html)
* ISO/TS 22330 (2018), Security and Resilience - Business Continuity Management Systems - [Guidelines for People Aspects of Business Continuity](https://www.iso.org/standard/50067.html)
* ISO/TS 22331 (2018), Security and Resilience - Business Continuity Management Systems - [Guidelines for Business Continuity Strategy](https://www.iso.org/standard/50068.html)
* ISO 22320 (2018), Security and resilience, [Emergency management](https://www.iso.org/standard/67851.html), Guidelines for Incident Management
* ISO 22301 (2019), Security and Resilience - Business Continuity Management Systems - [Requirements](https://www.iso.org/standard/75106.html)
* IEC 31010 (2019), Risk Management - [Risk Assessment Techniques](https://www.iso.org/standard/72140.html)
* ISO 22313 (2020), Security and Resilience - Business Continuity Management Systems - [Guidance on the use of ISO 22301](https://www.iso.org/standard/75107.html)
* AS/NZS 5050(Int) (2020), [Managing Disruption-Related Risk](https://www.standards.govt.nz/shop/asnzs-5050int2020/)
* BS 31100 (2021), [Risk Management. Code of Practice](https://shop.bsigroup.com/products/risk-management-code-of-practice-and-guidance-for-the-implementation-of-bs-iso-31000-2018/tracked-changes)
* ISO 22300 (2021), Security and Resilience - [Vocabulary](https://www.iso.org/standard/77008.html)
* ISO/TS 22317 (2021), Security and Resilience - Business Continuity Management Systems - [Guidelines for Business Impact Analysis](https://www.iso.org/standard/79000.html)
* ISO/TS 22318 (2021), Security and Resilience - Business Continuity Management Systems - [Guidelines for Supply Chain Continuity Management](https://www.iso.org/standard/79001.html)
* ISO 22322 (2022) Security and Resilience, Emergency Management, [Guidelines for Public Warning](https://www.iso.org/standard/84558.html)
* ISO/IEC 27001 (2022), Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - [Requirements](https://www.iso.org/standard/27001)

None of these standards are obligatory but as Deming said:

**There is no need to change. Survival is not mandatory**

**2.3 Books**

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

*  Frank Knight, [*Risk, Uncertainty And Profit*](https://www.amazon.fr/Risk-Uncertainty-Profit-Frank-Knight/dp/0486447758/ref=tmm_pap_title_0?_encoding=UTF8&qid=&sr=), University of Chicago Press, 1921
* [](http://www.amazon.com/Out-Crisis-W-Edwards-Deming/dp/0262541157) Edwards Deming, [*Out of the Crisis*](http://www.amazon.com/Out-Crisis-W-Edwards-Deming/dp/0262541157), MIT Press, 1982
*  Peter Bernstein, [*Against the Gods*](https://www.amazon.fr/Against-Gods-Remarkable-Story-Risk/dp/0471295639/ref=asc_df_0471295639/?tag=googshopfr-21&linkCode=df0&hvadid=229316545170&hvpos=2o1&hvnetw=g&hvrand=13513608854921118670&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9055414&hvtargid=pla-449980713491&psc=1): *The Remarkable Story of Risk*, John Wiley & Sons, New York, 1998
*  Michael Gallagher, [*Business Continuity Management*](https://www.amazon.fr/Business-Continuity-Management-Protect-Company/dp/0273663518/ref=sr_1_1?s=english-books&ie=UTF8&qid=1506592924&sr=1-1&keywords=Business+Continuity+Management%3A+How+To+Protect+Your+Company+From+Danger) - *How to Protect Your Company from Danger*, Prentice Hall, 2002
* [](http://www.amazon.com/Quality-Toolbox-Nancy-R-Tague/dp/0873896394) Nancy Tague, [*The Quality Toolbox*](http://www.amazon.com/Quality-Toolbox-Nancy-R-Tague/dp/0873896394), ASQC Quality Press, 2005
*  Douglas Hubbard, [*The Failure of Risk Management*](https://www.amazon.fr/Failure-Risk-Management-x2032-Broken/dp/0470387955/ref=tmm_hrd_title_0?_encoding=UTF8&qid=1503762479&sr=1-3): *Why It's Broken and How to Fix It*, Wiley, 2009
*  team, [*Business Continuity For Dummies*](https://www.amazon.com/Business-Continuity-Dummies-Cabinet-Office/dp/1118326830/ref=pd_sim_d_sccl_1_1/134-8230961-2176041?pd_rd_w=YFVbz&content-id=amzn1.sym.807772be-f817-4c8d-8a9d-04ee37f7ad33&pf_rd_p=807772be-f817-4c8d-8a9d-04ee37f7ad33&pf_rd_r=QZ34ZM53FR9Q4GQY9PMP&pd_rd_wg=VUhkQ&pd_rd_r=5cb45717-1d4e-464c-a693-7c4187c211b7&pd_rd_i=1118326830&psc=1), *For Dummies*, 2012
*  Susan Snedaker, [*Business Continuity and Disaster Recovery Planning*](https://www.amazon.com/Business-Continuity-Disaster-Recovery-Professionals/dp/0124105262/ref=pd_bxgy_img_d_sccl_1/134-8230961-2176041?pd_rd_w=cqXN1&content-id=amzn1.sym.2b132e63-5dcd-4ba1-be9f-9e044543d59f&pf_rd_p=2b132e63-5dcd-4ba1-be9f-9e044543d59f&pf_rd_r=T3GXR5TPZVW66ZED5DVX&pd_rd_wg=cqulq&pd_rd_r=3a4d9d3c-53a6-4c14-abbb-f24c220eb44b&pd_rd_i=0124105262&psc=1) *for IT Professionals*, Syngress,2013
*  team, [*ISO 22301 A Complete Guide*](https://www.amazon.fr/ISO-22301-Complete-Guide-2021/dp/1867426285/ref=sr_1_6?__mk_fr_FR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&crid=2J3QF0DWE98NF&keywords=iso+22301&qid=1707407781&s=books&sprefix=iso+22301%2Cstripbooks%2C281&sr=1-6&ufe=app_do%3Aamzn1.fos.49fccda8-a887-4188-817b-b9a64bb30e43) *- 2021 Edition*, The Art of Service, 2020
*  Alan Carder, [*ISO 22301:2019 and business continuity management*](https://www.amazon.com/ISO-22301-continuity-management-Understand/dp/1787782999) - *Understand how to plan, implement and enhance a business continuity management system (BCMS)*, IT GP, 2021
*  PECB, [*ISO 22301:2019 Auditing Guide*](https://www.amazon.com/ISO-22301-practical-Continuity-Management-ebook/dp/B09GPNSP2Y/ref=monarch_sidesheet#detailBullets_feature_div)*: A simple and practical guide to auditing a Business Continuity Management System* (BCMS), PECB, 2021
*  Kris Hermans, [*Mastering ISO 22301:2019*](https://www.amazon.com/Mastering-ISO-22301-Comprehensive-Continuity/dp/B0C7F59QY7/ref=sr_1_18?crid=3FGTHEPI46W1M&dib=eyJ2IjoiMSJ9.4noDUmCedeJ5CgbRM7O21pN22Mym-eTDLV5OrL0RkAx-6f2wbHNO7zy44_wJ61CyvgDOdhgzhJf-4HivkjjNWQ.VtUGU78CIOZSCyG1YGP_WVQHv6dC65CuggNbgGC8b4s&dib_tag=se&keywords=iso+22301&qid=1712327790&s=books&sprefix=iso+22301%2Cstripbooks-intl-ship%2C366&sr=1-18#detailBullets_feature_div)*: A Comprehensive Guide to the Business Continuity Management System (BCMS)*, Independently published, 2023
*  Arman Suman, [*ISO 22301 Foundation*](https://www.amazon.com/ISO-22301-Foundation-Study-Guide-ebook/dp/B0C4H94GKW/ref=sr_1_14?crid=3FGTHEPI46W1M&dib=eyJ2IjoiMSJ9.3TdjgYl6ID_2q7hgT6frQVffsLlPZRz96_gRIwMNPUCGa25jUSB94N0g6M-laM0TwNNd2cFrcDCGnJt4WygUus3_7lytN03kMIPub7LEPxZCwFJ5WtbKui-iM7tSHo9luP852D2aBcrO0RKwyDVZq5n8gn1BEuaH6a0yj6cmKKT9k4lypkKl7uTfeQZOOA3SOQd54EH9qAm5jKcX1Di3bFOGcirC52OEHiuOnpc5oTs.khYiUpYfEzb48oRLzVHiucAQiNl3pD9CyTaI6LvE0Bk&dib_tag=se&keywords=iso+22301&qid=1712328184&s=books&sprefix=iso+22301%2Cstripbooks-intl-ship%2C366&sr=1-14) *- Study Guide*, Kindle, 2023
*  James Crask, [*Business Continuity Management*](https://www.amazon.com/Business-Continuity-Management-Organization-Resilience/dp/1398614874/ref=sr_1_12?crid=3FGTHEPI46W1M&dib=eyJ2IjoiMSJ9.3TdjgYl6ID_2q7hgT6frQVffsLlPZRz96_gRIwMNPUDEDpfy9uO2zWaOKl7pyFqSoYwCWKewNFG6tC6pZOfeN83_7lytN03kMIPub7LEPxZCwFJ5WtbKui-iM7tSHo9luP852D2aBcrO0RKwyDVZq5n8gn1BEuaH6a0yj6cmKKT9k4lypkKl7uTfeQZOOA3SOQd54EH9qAm5jKcX1Di3bCXfd4vRk2VDkeQlzHX1PoY.04xdHvN83VG7RhZkAC8IV_AGjosTyNgRke-TR-lOioM&dib_tag=se&keywords=iso+22301&qid=1712327294&s=books&sprefix=iso+22301%2Cstripbooks-intl-ship%2C366&sr=1-12)*: 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:

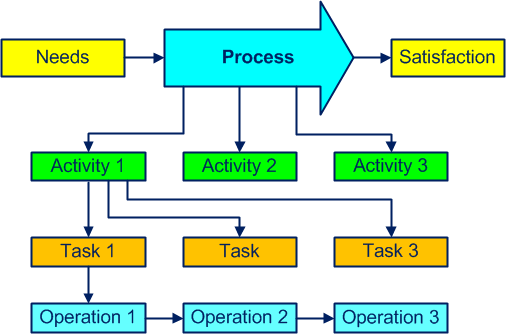
* repeatable
* foreseeable
* measurable
* definable
* dependent on its context
* responsible for its suppliers

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

* title and type
* purpose (why?)
* beneficiary (for whom?)
* scope and activities
* initiators
* documentation
* 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). G:\19 07\ISO\ISO 14001\Pr à l'ISO 14001\enregistrement.gif

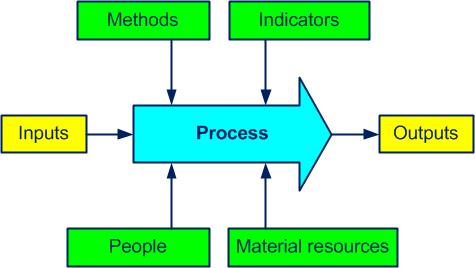
The components of a process are shown in figure 3-1: 

****

*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*](https://www.pqbweb.eu/document-d-02-processes-for-your-operational-management-system-set-of-documents.php).

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 procedure 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.

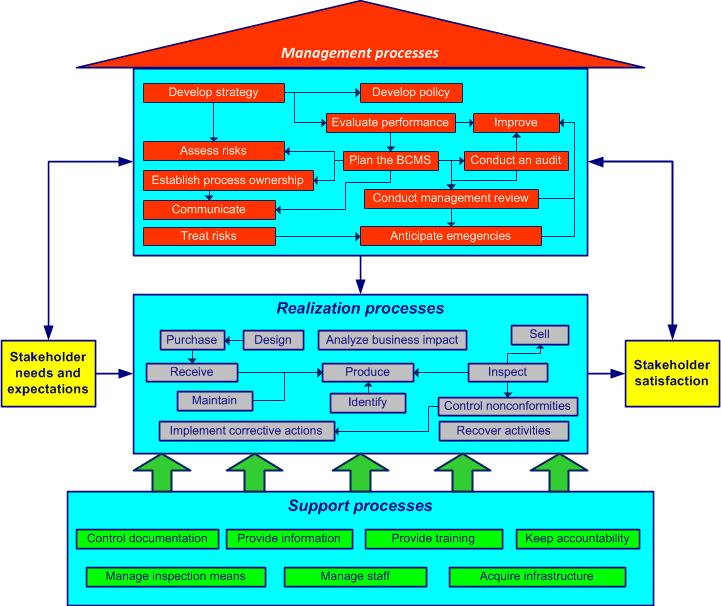


Figure 3-3. The process house

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.

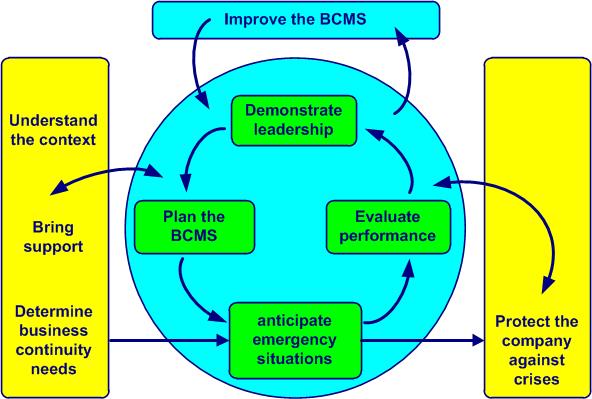


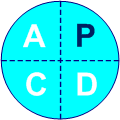
Figure 3-4. Model of a BCMS based on process approach and continual improvement

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
  + measuring process performance
  + 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

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*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#4.1)*, see also the* [*quiz*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php)*)*

**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 business continuity 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). G:\19 07\ISO\ISO 14001\Pr à l'ISO 14001\enregistrement.gif

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 Stakeholders** *(requirements* [*2 to 6*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#4.2)*)*

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

To understand the needs and expectations of stakeholders, 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** *(requirements* [*7 to 15*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#4.3)*)*

**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 the BCMS of a company 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 can we protect staff and work tools?
* what is the plan to maintain part of the activity?
* how can we 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) 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.*

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:
  + social
  + financial
  + technological
  + economical
* stakeholder requirements (cf. paragraph 4.2)
* outsourced processes

***Good practices***

* *the 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*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#4.4)*)*

**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

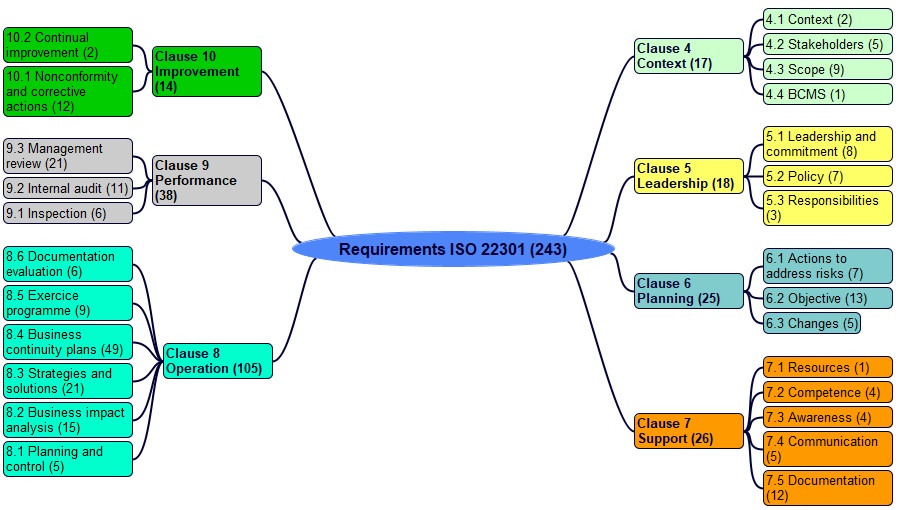
For that:

* 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
  + owners named (responsibilities and authorities defined)
  + the sequences and interactions determined
  + each process measured and monitored (established criteria), objectives established and performance indicators analyzed
  + process performance evaluated
  + the necessary changes introduced to achieve the expected results
  + actions to achieve continual process improvement 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*](https://www.pqbweb.eu/document-d-12-quality-tools-for-your-operational-management-system-set-of-documents.php) quality tools
* having all procedures written by the business continuity manager: 
  + 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: 
  + innovation, luxury, secrecy, authoritarian management (Apple)
  + strong culture related to ecology, action and struggle, while cultivating secrecy (Greenpeace)
  + fun and quirky corporate culture (Michel & Augustin)
  + liberated company, the man is good, love your customer, shared dream (Favi, cf. [*T 50*](https://www.pqbweb.eu/training-t-50-e-learning-happiness-in-the-liberated-company-special-price!.php))

The requirements of the ISO 22301 standard are shown in figure 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

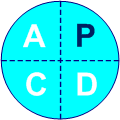
Do not hesitate to look for answers in ISO 22313 (“Guidance on the Use of ISO 22301”) when you cannot find them in this module, cf. paragraph 2.2.

***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*

***Bad practices***

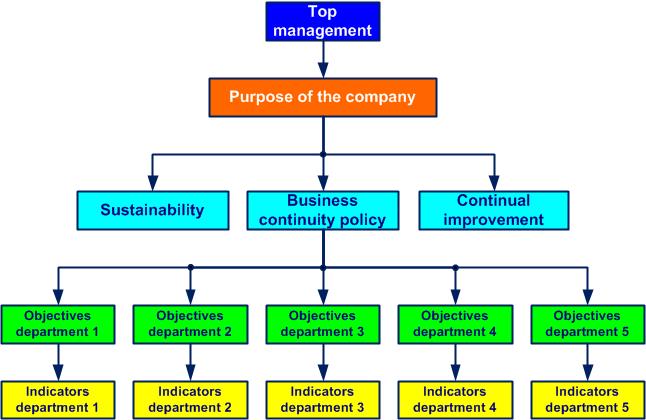
* *some process output elements are not correctly defined (customers not taken into account)*
* *process efficiency criteria not established*
* *non-formalized process owner*
* *outsourced processes not determined*
* *very real activities are not identified in any process*
* *control of outsourced services 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)*

**5 Leadership **

**5.1 Leadership and commitment** *(requirements* [*17 to 24*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#5.1)*)*

**When you sweep the stairs, you start at the top. Romanian proverb**

Top management demonstrates leadership (fully assuming its responsibility for the performance of the BCMS) by defining the purpose (the reason to exist) of the company and ensuring the sustainability, business continuity policy and continual improvement of the business continuity management system (cf. figure 5-1). Business continuity objectives are deployed in each department and indicators are implemented to measure process performance.



*Figure 5-1. Deployment of objectives*

**Tell me and I’ll remember for an hour; show me and I’ll remember for a day; but let me do it and I’ll remember forever. Chinese Proverb**

**Leadership**: *ability to inspire and lead a team to achieve set goals*

Top management at its highest level commits to:

* define and promote the business continuity policy, which follows from the purpose, strategic direction and context of the company
* communicate the importance of:
  + integrating within internal processes the requirements of:
    - the BCMS
    - customers
    - other stakeholders
    - regulations
  + having a performing business continuity management system (BCMS)
  + meeting the requirements of the business continuity management system
* ensure the availability of manpower and technical resources to achieve the objectives
* do everything so that the established objectives are met (lead by example on the field)
* involve staff to achieve expected results
* fully support the process approach and continual improvement
* define, communicate and support the responsibilities and authorities at all levels

***True story***

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

*To address this concern, it became customary to place an empty chair at every meeting.*

***Good practices***

* *top management assumes its responsibility by communicating the importance of having an efficient BCMS to sustain the company*
* *the director’s statement of commitment is displayed in a few key locations*

***Bad practices***

* *top management commitment does not contain objectives*
* *communication on BCMS requirements is not ensured in the workshop*
* *some indicators are difficult to interpret*
* *certain indicators are not consistent with the objectives*

**5.2 Policy** *(requirements* [*25 to 31*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#5.2)*)*

**The worst policy is the lack of policy**

The business continuity policy is written and signed by the director. It:

* is adapted to the purpose, culture and context of the company
* provides the framework for defining and reviewing business continuity objectives
* is adequate to the nature and extent of risks in the company
* includes a commitment to:
  + meet statutory and other requirements
  + continual improvement of performance
* is communicated, understood and applied at all levels
* is reviewed in the context of continual improvement (cf. management review, paragraph 9.3)
* is available to stakeholders

Business continuity policy: *statement by top management allowing the establishment of business continuity objectives*

The proof of top management's commitment to a high-performance BCMS is the availability of the Business continuity policy in the form of a document posted in a few key places, cf annex 10. 

The business continuity policy is, among other things, an advantage for calls for tenders and a step ahead of your competitors.

***Good practices***

* *the business continuity policy takes into account all the specificities linked to the corporate culture*
* *the business continuity policy includes the commitment to continual improvement*

***Bad practices***

* *the business continuity policy is not updated*
* *the business continuity policy is not dated*
* *the business continuity policy is not signed by the director*
* *in the business continuity policy, there is a lack of possibilities to increase stakeholder satisfaction*
* *the business continuity policy is not posted outside the director’s office*

**5.3 Roles, responsibilities and authorities** *(requirements* [*32 to 34*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#5.3)*)*

**Responsibility cannot be shared. Robert Heinlein**

The business continuity manager is appointed by top management. Their responsibilities and authorities are communicated to all staff.

Top management defines the responsibilities and authorities for the implementation and improvement of the business continuity management system. Information on these different roles is freely available internally.

The person in charge of that job is appointed to:

* ensure that the BCMS is established, implemented and maintained in accordance with the requirements of the ISO 22301 standard
* involve staff so that business continuity objectives are met
* report regularly on the performance of the BCMS to top management
* promote the requirements of the business continuity plan
* realize the exercise and test program
* channel proposed improvements
* monitor change control

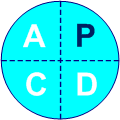
 Minute of relaxation. Cf. joke “[Is Hell exothermic or endothermic?](http://www.pqbweb.eu/admin/pages.php?act=see&id=31#hell)”.

***Good practices***

* *the job description of all positions (including executives) is accessible on the Intranet network*
* *the animation, coordination and training missions of the BCMS are explicitly defined*

***Bad practices***

* *the roles and missions of managers are not well known or understood in the workshop*
* *the job description of the business continuity manager is not updated*
* *the responsibilities and authorities of the business continuity manager are not recorded*

**6 Planning** 

**6.1 Risks** *(requirements* [*35 to 41*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#6.1)*)*

**The greatest risk of all is to take none at all!**

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

Often a risk is assimilated to a hazard and commonly used instead of threat.

To calmly plan its business continuity management system, top management takes into account:

* the list of external and internal issues (cf. paragraph 4.1)
* stakeholder requirements (cf. paragraph 4.2)
* the scope of the business continuity management system (cf. paragraph 4.3)
* the processes necessary for the business continuity management system (cf. paragraph 4.4)
* roles, responsibilities and authorities within the company (cf. paragraph 5.3)
* opportunities for improvement (cf. paragraph 10.2)

Any threat that could disrupt the normal activities of the company is:

* determined
* analyzed
* evaluated and
* appropriate actions are taken to prevent or reduce adverse effects

The risk approach allows us to prepare the action to be taken if an output element of the process does not meet a requirement. In other words, be prepared in case something doesn't work (well).

Any opportunity that can increase desirable effects on the business continuity management system is supported with continual improvement actions.

The nature of actions is proportional to the potential impact of threats and opportunities. Some examples of risks are listed in annex 11. 

**Actions speak louder than words. English proverb**

An example of ranking the risks of a process by level is shown in annex 12 (Risk level). With the impact and likelihood of occurrence indices, each risk is classified in a table. According to predefined acceptance criteria, the level of risk can be acceptable, unacceptable minor or unacceptable major. Our goal is not zero risk (that does not exist) but to create conditions for working with an acceptable level of risk. 

Planning actions to reduce negative impacts and increase beneficial impacts often includes implementing:

* business continuity objectives and indicators
* input elements:
  + support (cf. clause 7)
  + of realization (cf. clause 8)
  + performance evaluation (cf. clause 9)
  + improvement (cf. clause 10)
* a method for evaluating the effectiveness of actions (periodic reviews)

An appropriate methodology is chosen to:

* anticipate and assess risks:
  + estimate the consequences
  + plan the frequency
* classify the risks:
  + in acceptable or not acceptable
  + which can be controlled (transform them into acceptable)
* ensure consistency between risk assessment and the objectives of the business continuity policy

The list of risks is confidential data, but displaying risk control in front of your customers can be beneficial.

The risk-based approach (see ISO 31000 and training [*T 51v18*](https://www.pqbweb.eu/training-t-51v18-e-learning-risk-management-iso-31000-version-2018-optimize-decision-making.php) “Risk Management”) is a process with a few distinct activities:  

* assess the risk:
  + identify (list)
  + analyze (impact)
  + evaluate (type and level)
* treat (options)
* monitor and review (effectiveness)

The “Manage risks” process is shown in annex 04. An example of a “Risk Management” procedure is shown in annex 13.  

Actions to address risk can be summarized in a few options:

* avoid risk (refuse the risk-bearing activity)
* accept risk to gain opportunity
* eliminate the source of the risk
* modify the probability of occurrence of the risk
* react to the consequences of the risk
* share the risk with other stakeholders
* maintain the residual risk (acceptable level)

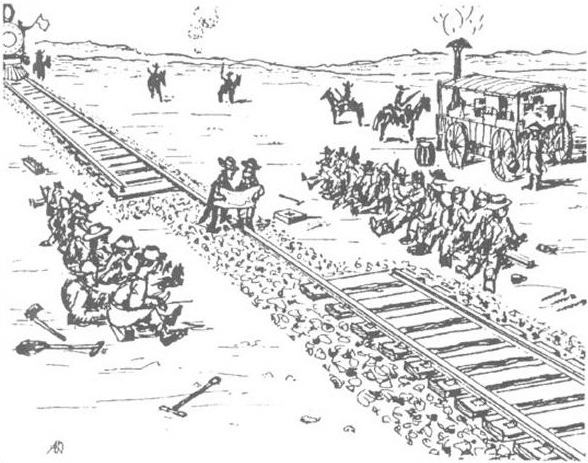
A Risk support, in Excel format, is shown in annex 14. 

A Risk treatment plan, in Excel format, is shown in annex 15. 

The actions include, among other things:

* roles and responsibilities at all levels involved
* essential resources (including training needs) and means used
* anticipation of future changes to a process
* description of the actions to be implemented
* the completion time
* monitoring of actions
* evaluation of results

 Example of an unidentified risk:



***Good practices***

* *the list of external and internal issues is exhaustive*
* *planning of actions to deal with risks takes into account the scope of the BCMS*
* *the list of risks taken into account is exhaustive*
* *actions to reduce certain risks are integrated into key processes*
* *the action plan includes a column used for monitoring the effectiveness of actions*
* *the action plan takes into account the results of internal audits*

***Bad practices***

* *certain stakeholder requirements are not taken into account when planning actions to address risks*
* *risk analysis does not take into account strategic issues*
* *no action planning to reduce negative impacts*
* *no opportunity to increase desirable effects*
* *threats and opportunities are not determined for certain processes*

**6.2 Objectives** *(requirements* [*42 to 54*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#6.2)*)*

**He who has no goals will not achieve them. Sun Tzu**

Business continuity objectives derive directly from the business continuity policy (cf. paragraph 5.2). The objectives are shown to all staff through indicators displayed on one or more dashboards. The business continuity manager (or team leader) monitors the level of indicators daily.

Business continuity objectives change over time. Business continuity objectives are SMART:

* Specific (and understandable)
* Measurable (when it is possible)
* Achievable (and comply with the applicable requirements)
* Realistic (adequate with the business continuity policy)
* Time-bound (planned in time, short and long term)

Planning to achieve the business continuity objectives includes:

* what will be done (what)
* the necessary resources (whom, with what)
* a deadline (until when)
* evaluation of the effectiveness of actions (level obtained)

Some examples of objectives:

* update the business impact analysis
* carry out business continuity plan exercises
* reduce nonconformities
* staff competence
* staff awareness
* improvement of the BCMS

Some examples of indicators:

* rate of completion of business impact analyses
* number of risks identified
* number of nonconformities identified and corrected
* exercises completed on time
* % of staff made aware
* % of staff trained
* improvement opportunities implemented

***Good practices***

* *the available resources and associated objectives are in line with the business continuity policy*
* *the dashboard with all the indicators helps raise staff awareness*

***Bad practices***

* *no objectives communicated*
* *some objectives are not measurable*
* *the objectives are not broken down into indicators*
* *non-existent dashboard*
* *no planned action to achieve business continuity objectives*
* *certain objectives are not monitored regularly*
* *planning does not include any criteria to evaluate the effectiveness of actions*

**6.3 Changes** *(requirements* [*55 to 59*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#6.3)*)*

**The only person who likes change is a wet baby**

BCMS change planning allows you to seize opportunities for improvement, cf. paragraph 10.2.

Before introducing a change, you need to consider:

* its necessity
* its objective
* its beneficial impact
* the integrity of the BCMS
* the risk of potential nuisance
* availability of personnel and technical resources
* responsibilities and authorities for its application

***True story***

*In 1982, the GM plant in Fremont, California, was closed (5000 layoffs) partly because of the struggles between unions, the combative conservative management and workers who were not at all docile.*

*In 1984, Toyota created a partnership with GM and reopened the plant under the name of Nummi. The contract stipulated that the same amount of cars would be produced with half of the former staff.*

*Japanese officials put in place the "Toyota spirit", the Lean approach, trust, respect, responsibility, freedom to think, act and solve problems, simplification, war on waste, work in small teams, versatility and quality first.*

*The cost of production decreased significantly, absenteeism fell from 20 to 2%, and the quality of cars rivaled those produced in Japan.*

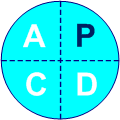
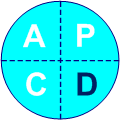
*When change is well-prepared and well-managed, it can work wonders! Since 2010, the plant has become a Tesla factory (electric cars).*

***Good practices***

* *changes are planned and validated before any application*
* *no change has a negative impact*

***Bad practices***

* *certain changes are applied without planning or analysis of the risk of potential nuisances*
* *the person responsible for a change is not known to the people concerned*
* *change applied without clearly established objective*

**7 Support**  ****

**7.1 Resources** *(requirement* [*60*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#7.1)*)*

**But in the long run - and I emphasize this - no matter how good or successful you are or how clever or crafty, your business and its future are in the hands of the people you hire. Akio Morita**

Top management identifies, plans and provides the necessary resources to:

* establish, implement, maintain and continually improve the business continuity management system
* protect personnel
* confirm its commitment to the effective operation of the BCMS

Top management takes into account the limits of available internal resources and resorts to external providers when essential.

Resources include:

* personnel and time for participation in the BCMS
* infrastructure
* technology:
  + processes
  + IT
* field exercises
* financial resources

Top management periodically reviews the adequacy of resources.

Top management contributes to increasing the competence of the personnel required for the smooth running of the BCMS and priority activities.

***(Almost) true story***

*The story of the three stonecutters conveys a great deal. When asked about their work:*

*- the first replied that he is cutting stones for a living*

*- the second that he tries to be the best stonemason in the country*

*- while the third answered that he is building a cathedral*

*Hence the three main types of relationship to work:*

*- livelihood*

*- career*

*- vocation*

 Minute of relaxation. Cf. joke “[Gold contract](http://www.pqbweb.eu/page.php?id=31#gold)”

Top management provides and maintains the infrastructure required for the BCMS to operate smoothly. Examples of infrastructure:

* equipment
* associated services:
  + computer systems
  + software

***True story***

*A piece of equipment was moved to make room for some new, bulky equipment. When scheduled maintenance was to begin on the first piece of equipment, the maintenance guy was unable to perform his activities, as the equipment was too close to the wall. He suggested creating a door in the wall to allow access to the equipment.*

*The only concern was that it was an outside wall!*

***Good practices***

* *the necessary resources are planned and secured to achieve the objectives*
* *the list of equipment, machines and infrastructure is updated regularly*
* *the presentation of the company on the website is very clear and updated*

***Bad practices***

* *financial resources are not released on time*
* *staff expectations are not identified*
* *the business continuity manager has neither deputy nor replacement*

**7.2 Competence** *(requirements* [*61 to 64*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#7.2)*)*

**If you are planning for a year, sow rice; if you are planning for a decade, plant trees; if you are planning for a lifetime, educate people. Chinese proverb**

Staff and people working under the company's control:

* have the appropriate competence (knowledge and know-how) to carry out activities that have an impact on the performance of threats and opportunities of the BCMS
* know how to use common sense and pragmatism
* are trained according to identified needs (training program)
* carry out learning actions when necessary to acquire new skills. A posteriori, the effectiveness of these actions is evaluated

The competence of staff with responsibilities for improving business continuity mainly concern those involved in:

* identifying external and internal issues, cf. paragraph 4.1
* gathering relevant information on crisis management, cf. paragraph 4.1
* analysis of legal and regulatory requirements, cf. paragraph 4.2
* risk management, cf. paragraph 6.1
* change management following BCP revision, cf. paragraph 6.3
* communication management, cf. paragraph 7.4
* computer backup control, cf. paragraph 8.1
* anticipating emergency situations, cf. paragraph 8.1
* establishing a business continuity strategy, cf. paragraph 8.3
* selecting technical backup solutions, cf. paragraph 8.3
* recovering critical activities (including the IT system), cf. paragraph 8.4.5
* assessment of the BCMS performance (internal audits), cf. paragraph 9.2
* seizing opportunities for improvement, cf. paragraph 10.2

Appropriate training in incident response and business resumption includes:

* incident assessment
* personnel evacuation
* alternative workplaces
* internal and external communication
* simulation exercises

Further details can be found in ISO/TS 22330 ("Guidelines for People Aspects of Business Continuity"), cf. paragraph 2.2.

Competence-related documents are kept, cf. annex 16. 

***Good practices***

* *the annual training program is updated at least twice a year*
* *the training file of each employee is protected (access restrictions)*
* *each training is evaluated at the end of the session and two to three months later*
* *an analysis of the effectiveness of training is carried out at the end of the year*
* *the skills matrix is updated regularly*

***Bad practices***

* *missing skills are not listed*
* *some departments do not determine their training needs*
* *evaluation of the effectiveness of training is not carried out*
* *certain training courses were not evaluated either at the end of the session or later*
* *the annual training program is not updated (training planned but not provided)*

**7.3 Awareness** *(requirements* [*65 to 68*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#7.3)*)*

**Staff are part of the problem, but also part of the solution**

The entire staff is made aware of the:

* importance of understanding and respecting:
  + the business continuity policy
  + objectives in each department
  + BCMS requirements
  + legal and regulatory requirements
* knowledge of one's own role and the tools to use
* positive effects coming from each person’s performance
* contribution of each person to improving the performance of the BCMS
* difference between notions like:
  + incident and accident
  + disaster and disruption
  + crisis and crisis management
  + emergency scenario and simulation
  + business continuity plan and business impact analysis

***Good practices***

* *everyone contributes to continual improvement without any constraints*
* *all staff are made aware of the business continuity policy and objectives*

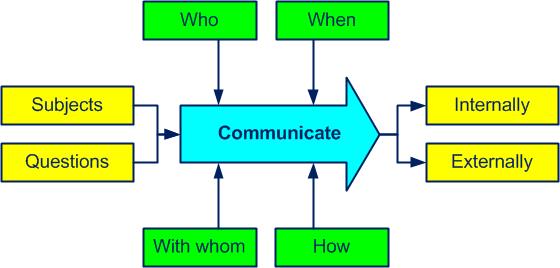
***Bad practices***

* *no formalized document for raising awareness among new hires or staff of external providers*
* *new hires do not receive formal information on emergency preparedness*

**7.4 Communication** *(requirements* [*69 to 73*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#7.4)*)*

**Good news walks, bad news runs. Swedish proverb**

The “Communicate” process is shown in figure 7-1. 



*Figure 7-1. The communicate process*

Top management plans and implements appropriate information communication arrangements with stakeholders (with whom) at appropriate times (when). The business continuity manager takes over in the field. The appropriate tool for this activity is the Communication plan, cf. annex 16. 

Try doing this simply because:

**Too much communication kills communication**

The staff is:

* involved (participation)
* consulted
* made aware
* represented
* informed

The following activities are defined:

* who is responsible for communication
* communication methods (how) on the BCP and its improvement:
  + orientation handbook
  + reports
  + meetings
  + newsletters
  + posters
  + explanatory notes
  + Intranet, Internet
  + dashboards
  + instructions:
    - evacuation
    - wearing personal protective equipment
    - access to specific areas
* processing of requests for information, feedback (including complaints) from stakeholders
* communicate externally relevant, non-confidential and mandatory information

External communication builds stakeholder confidence in your ability to maintain normal business during a disruption.

Effective communication is above all:

* explaining
* informing
* making aware
* empowering

***True story***

*The Manhattan military project (the creation of the atomic bomb) was moving too slowly. Secrecy was the rule for security reasons and the nature of the project was hidden from all staff.*

*To move up a gear, the head project leader, Robert Oppenheimer, decided to inform all team members of the nature of the project, its extreme urgency and its critical importance to the end of the war. Unsuspected energy freed itself, and work advanced in leaps and bounds.*

*Informing staff about the mission, giving meaning to their work and trusting them is a guarantee of success for any project.*

 Minute of relaxation. Cf. joke “[Lack of communication](http://www.pqbweb.eu/page.php?id=31#lack)”

***Good practices***

* *the methods and means of internal and external communication are carefully described in the process sheet*
* *communication is transparent and systematic*
* *for important issues, staff and stakeholders are consulted and involved upstream*

***Bad practices***

* *complaints are not taken into account*
* *lack of communication plan*
* *the follow-up of actions following complaints are not transmitted to the stakeholder*

**7.5 Documentation** *(requirements* [*74 to 85*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#7.5)*)*

**7.5.1 General**

**The right document, in the right place, at the right time**

A document can be in any form and any medium but meets the requirements of the ISO 22301 standard.

For an effective business continuity management system, everyone uses, according to their own judgment, only simplified and strictly necessary documentation. To believe that you must at all costs document your competence and skills to conserve and transmit them is a conception of the past.

The term procedure can be replaced by documented information to maintain. procédure

A procedure should be short, simple and relevant. Especially in cases where its absence could lead to deviations from policy or objectives.

Examples of procedures (\* mandatory, cf. annex 13): procédure 

* legal requirements
* risk management
* document control
* backup
* response to disruptions
* IT business continuity (paragraph 8.4.1) \*
* warning and communication (paragraph 8.4.3) \*
* business continuity plan (paragraph 8.4.4) \*
* exercise and test
* internal audit
* corrective actions

The term record can be replaced by documented information to retain. 

Each record is unique and normally cannot be modified except for error correction. Any record provides evidence of a task, operation, activity, process or requirement. Records are the essential database for analyzing process efficiency and contributing to the continual improvement of the business continuity management system.

Examples of records (\* mandatory, cf. annex 16): 

* context of the company
* list of legal requirements \* (paragraph 4.2.2)
* scope \* (paragraph 4.3.1)
* responsibilities and authorities
* business continuity objectives \* (paragraph 6.2.1)
* plan to achieve objectives
* competence \* (paragraph 7.2)
* training program
* communication plan
* list of documents of external origin
* operational control
* change management plan
* outsourced processes
* impact analysis
* risk treatment
* strategies and solutions
* crisis team \* (paragraph 8.4.2)
* communication on disruption \* (paragraph 8.4.3)
* disruption \* (paragraph 8.4.3.1)
* business continuity plans \* (paragraph 8.4.4)
* exercise program
* incident scenarios
* exercise results
* review of business continuity capabilities
* performance evaluation \* (paragraph 9.1)
* internal audit \* (paragraph 9.2.2)
* management review \* (paragraph 9.3.3.2)
* nonconformities and corrective actions \* (paragraph 10.1.3)
* improvement report

The Business continuity policy is communicated and available to all staff, paragraph 5.2, cf. annex 10. 

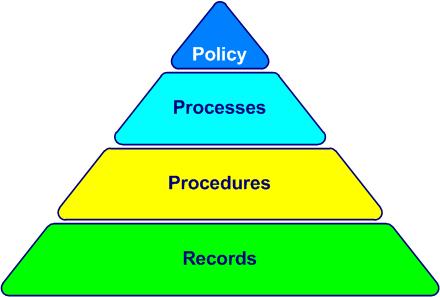
The documents are related to:

* the size, type and field of activity of the company
* the complexity of processes and their interactions
* products and services
* the competence of the staff

**7.5.2 Creating and updating**

**Spoken words fly away, written one stay. Latin proverb**

BCMS documentation (cf. figure 7-2) includes policy, process documents, procedures and records. Documents of external origin (from service providers, suppliers, customers, standards) are part of the documentation as records.



*Figure 7-2. The documentation pyramid*

Each internal document is codified and approved (validated). Outdated (obsolete) documents are identified and their use prohibited.

The ISO 10013 (2021): "Quality management systems - Guidance for documented information" provides recommendations in relation to the documentation of a BCMS.

Answers to all 242 requirements (in the text “shall”) of clauses 4 to 10 of the ISO 22301 standard are included in the documentation, cf. paragraph 4.4.

Each procedure is identified, among other things, by: 

* title
* author (authors)
* coding (reference number)
* format
* creation date
* review
* approval (suitability and adequacy)

**7.5.3 Document control**

Document control includes:

* the availability:
  + at the right time
  + in the right place
* suitability for use
* protection
* confidentiality
* distribution
* storage and preservation
* change management
* retention time
* elimination
* management of documents of external origin

A review of the documentary system is conducted periodically by the business continuity manager with the heads of departments. Each head of department is responsible for controlling the activities falling within his field, including the management of his documents.

***True story***

*At a third party, audit the auditor asked to see the version history of three procedures and some instructions.*

*The procedures all had more than three versions and the instructions (in our case, audit reports) had on average two or three versions (actions and one or two follow-ups).*

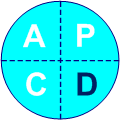
*The auditor was comforted because he was afraid he would come across “inactive” documents.*

***Good practices***

* *document control clearly shows the author and approver of the initial document and subsequent versions*
* *change management (line in the middle of the old text, red color) allows you to quickly see the history*
* *the hierarchy of documents is logical and clear (policy, processes, procedures, records)*
* *the master list of documents also contains the retention period*
* *the procedures fulfill their role of controlling situations where their absence could lead to deviations from legal requirements*
* *documents of external origin (standards, applicable regulations, customer documents, external providers and machines) are codified like internal documents and in a specific column the storage location is notified*
* *the review of all BCMS documentation, carried out twice a year, is very well organized, the actions are finalized within the set deadlines*
* *records show compliance with legal and regulatory requirements, ISO 22301 and the company's business continuity policy*
* *the list of dates for implementing changes is accessible to everyone internally*

***Bad practices***

* *the scope of the BCMS is not mentioned in any document*
* *some process sheets are incomplete*
* *very real activities are not identified in any document*
* *some documents are not codified*
* *documents are not approved before their distribution*
* *there are documents that are incomprehensible to staff*
* *documents are not where they are needed*
* *instructions are not updated (before the latest version)*
* *the protection of documents on the network is not defined*
* *documents of external origin are not controlled (codified)*
* *the retention period and disposal methods for documents are not determined*
* *no document prohibits the use of dangerous equipment (non-compliance with legal requirements)*
* *documents not kept until the date of their elimination*
* *business continuity meeting without recorded minutes*

**8 Operation **

**8.1 Planning and control** *(requirements* [*86 to 90*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#8.1)*)*

**Minimizing uncertainty is important, and planning is never optional. Tom Kendrick**

Preparing for crisis management is a prerequisite for mastering BCP. The activities concerned are planned, organized and coordinated by the business continuity manager.

The essential processes necessary for the business continuity management system are established, planned, implemented and controlled (cf. paragraph 4.4). These processes help the company meet stakeholder requirements, including legal and other requirements (cf. paragraph 4.2). Actions to address threats and opportunities are put in place (cf. paragraph 6.1).

Planning and above all controlling the processes means: 

* protect personnel, equipment and data
* determine the applicable requirements
* establish the criteria for:
  + acceptance
  + operation
  + shutdown sequence
  + recovery
* provide the necessary resources
* establish preventive actions
* respect the criteria in order to avoid a deviation from:
  + the business continuity policy
  + business continuity objectives
  + legal and regulatory requirements
* maintain and record documents (“to a sufficient extent”) proving that processes have been carried out as intended 

Examples of documents:

* business continuity plan
* exercise program
* BCMS maintenance plan
* emergency plan

Process changes are made in accordance with paragraph 6.3. If risks are detected during the upstream analysis then actions are planned to limit any negative consequences.

Backing up the computer system is almost always a prerequisite and concerns:

* part of the system following everyday incidents, on-site
* the entire system following a major disaster, remote site
* the entire system following a cyber-attack, on-site

Backup is described in a documented procedure, cf. annex 13. 

 Questions that require answers:

* what to do if:
  + we cannot access the site (transport cut)?
  + there is no more power (electricity, water, gas)?
  + a supplier no longer responds?
* was this disaster not predictable?
* have preventive actions been implemented?
* which activity should be dealt with first?
* who must stay working?
* is the computer backup effective?
* what is the situation of the products to be shipped?
* how can we restart as quickly as possible?

***Good practices***

* *acceptance and operating criteria are established, displayed and respected*
* *documents of process results are saved*
* *change management is controlled*
* *actions following changes are effective*
* *the list of external partners also includes the history of evaluations*

***Bad practices***

* *process acceptance criteria are not clearly defined*
* *documents relating to processes are not kept*
* *temporary and permanent changes to processes are not controlled*
* *the consequences of changes are not analyzed*
* *corrective actions are not requested from faulty external providers*

**8.2 Business impact** *(requirements* [*91 to 105*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#8.2)*)*

**Identify critical activities in order to determine priority activities**

**8.2.1 General**

The Analyze business impact process makes it possible to identify the vital and critical activities of the company, the recovery priority (activities, sequence), the consequences on the activity and to assess the risks during a disruption, cf. annex 04.  

The results of the analysis are the basis on which business continuity strategies and solutions are determined.

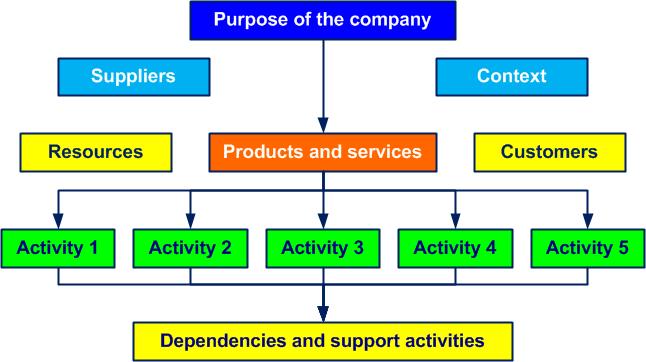
This process is not fixed in time and is reviewed following significant changes in the structure of the company and its context.

**8.2.2 Business impact analysis**

**If you don’t invest in risk management, it doesn’t matter what business you’re in, it’s a risky business. Gary Cohn**

The Analyze business impact process allows you to understand the purpose of the company and determine activities by priority in order to recover the situation to what it was before a disruption. 

The purpose of the company and its key activities (essential, priority, critical) are shown in figure 8-1.



*Figure 8-1. The purpose of the company*

Essential activities of the “Analyze business impact” process: 

* understand business continuity requirements
* define the types of disruption (interruption, shutdown, loss, destruction, flooding, deterioration)
* identify critical activities related to products, services and resources
* establish the emergency location
* list essential contacts (internal and external)
* determine the resources necessary for the recovery of priority activities, cf. paragraph 8.3.4
* define the impact criteria linked to the business context
* analyze the negative impacts, including the worst case, initially and in the following days
* identify the maximum tolerable period of disruption (MTPD)
* take into account:
  + unavoidable obligations (payroll, declarations)
  + stakeholder requirements and dependencies
* establish the sequence and duration of recovery activities
* keep priority activities updated
* verify significant impacts in the field such as:
  + financial losses (penalties)
  + damaged image (reputation)
  + stoppage of sales (breach of contract, disputes)
* obtain validation of the analysis by top management

The unacceptable duration of a disruption can be measured between a few minutes and a few weeks.

The business impact analysis is reviewed annually or following significant internal or external changes.

Do not hesitate to use the technical specification ISO/TS 22317 (“Guidelines for business impact analysis) and the ISO 27031 standard (“Guidelines for Information and Communication Technology Readiness for Business Continuity") when you do not find an answer on the business impact analysis in this module, cf. paragraph 2.2.

**8.2.3 Risk assessment**

**What we anticipate seldom occurs: but what we least expect generally happens. Benjamin Disraeli**

The “Assess risk” process concerns the risks of disruption to business activities, cf. annex 04. The risks of the management system are examined in paragraph 6.1.  

The objective of risk assessment is to evaluate risks in order to take appropriate measures to address those risks.

The main activities of the process are:

* identify the risks of disruption of:
  + critical activities
  + resources
* analyze risks. Take into account:
  + the causes and sources of risk
  + the likelihood of occurrence
  + the likelihood factors
  + positive and negative consequences
* assess risks. Take into account:
  + the need for treatment
  + the resources required for priority activities
  + replacement requiring a significant delay
  + the obligation to communicate
* classify risks
* address risks (reduction measures by priority)

The threats are diverse:

* fire
* flood
* power outage
* loss of competent personnel
* computer virus

The causes of vulnerability are also diverse:

* unpreparedness against fires and floods
* no backup power
* no replacements for critical positions
* poor information security

 Questions that require answers:

* what could happen?
* how likely is this to happen?
* what are the threats by priority?
* what are the critical vulnerabilities?
* what could be the impacts?
* what are the possible failures:
  + staff?
  + processes?
  + the computer system?
  + suppliers?
* what are the internal and external dependencies?
* what is the MTPD for each critical activity?
* what are the prevention and protection measures (reducing the likelihood and impact)?

For this, the following are taken into account:

* the context of the company
* stakeholder requirements
* resource vulnerability
* the business impact analysis

Measures for dealing with business continuity risks are:

* preventive actions:
  + create a dike
  + ensure a non-flooding storage location
  + anticipate an emergency power supply (current generator)
  + make a computer backup to a remote location
* corrective actions:
  + move stocks in case of imminent threat
  + set up teleworking
  + use automatic cellar pumps

The Business impact is validated by top management, cf. annex 16. 

More details on risk management can be found in the [*T 51v18*](https://www.pqbweb.eu/training-t-51v18-e-learning-risk-management-iso-31000-version-2018-optimize-decision-making.php) training based on the ISO 31000 standard.

***Good practices***

* *the business impact analysis is carried out after each significant change*
* *the assessment of disruption risks includes the main critical activities*
* *the list of unacceptable durations is updated*

***Bad practices***

* *resources for priority activities are not identified*
* *dependencies of priority activities are not determined*
* *risks are not subject to treatment measures*

**8.3 Strategies** *(requirements* [*106 to 126*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#8.3)*)*

**However beautiful the strategy, you should occasionally look at the results. Winston Churchill**

**8.3.1 General**

The results of the business impact analysis and those of the assessment of the risk of disruption make it possible to:

* select business continuity strategies
* find solutions to strengthen the weak points of critical activities

A strategy is based on:

* the MTPD
* the cost of the solution
* the negative impact if nothing is planned

The strategies are valid before, during and after a disruption and include several business continuity solutions.

Sometimes it is better to decide on the strategy after analyzing possible technical solutions.

The strategies and solutions make it possible to:

* reduce risks
* protect priority activities
* stabilize, continue, resume and recover priority activities
* mitigate and manage impacts

More details can be found in ISO 22330 (“Guidelines for People Aspects of Business Continuity”) and in ISO/TS 22331 (“Guidelines for Business Continuity Strategy"), cf. paragraph 2.2.

**8.3.2 Identification of strategies and solutions**

Identifying business continuity strategies (and solutions) means considering how much this will:

* help restore critical activities within agreed time frames and at a required capacity level, cf. paragraph 8.2.2
* protect critical activities by:
  + reducing risk
  + finding workarounds (manual processes)
  + transferring activities internally or externally
  + choosing to live with risk
* reduce the likelihood of disruptions occurring
* reduce the period of disruption taking into account the urgency of the activity
* limit impacts on products and services
* ensure the availability of adequate resources
* strengthen emergency resources
* support dependency management
* enable the rapid resumption of priority activities with an acceptable level of recovery

The strategy for mitigating the impacts of a disruption may include taking out insurance, but this will not cover all costs or non-material risks (reputation, market loss).

To manage reputation during a disruption, it is recommended to develop an effective alert and communication capacity (cf. paragraph 8.4.3).

**8.3.3 Selection of strategies and solutions**

To select business continuity strategies and solutions, you must choose simulation scenarios. In this way you will understand how much it will:

* help restore critical activities within the agreed deadlines and at a required capacity level according to the business impact analysis, cf. paragraph 8.2.2
* allow you to decide what risk to accept or not accept
* positively influence the cost/benefit ratio

A solution may be:

* strategic (major crisis, media management)
* tactical (BCP, emergency services)
* operational (damage, recovery)

Business continuity solutions to stabilize, continue, resume or recover a priority activity can be prohibitively expensive. One possible response is to accept the risk (especially for extremely unlikely threats), reassess the risk and remove, for example, certain products or services from the scope of the BCMS.

 Questions that require answers:

* what are the priority activities?
* reduce a risk or accept it?
* what is the maximum tolerable period of disruption (MTPD) for each critical activity?
* what is the acceptable level of recovery?
* which rescue providers are chosen?

**8.3.4 Resource requirements**

The resources in order to apply the selected business continuity solutions are mainly:

* crisis staff and team (authority for preparation, response and recovery)
* financing (before, during and after a disruption)
* protection of information and data
* infrastructure (emergency premises and offices, teleworking)
* equipment
* consumables
* the computer system
* logistics (stabilize, continue, resume or recover an activity)
* the partners
* suppliers (supply chain)
* transport (to an alternative site)
* communication in times of crisis

 Questions that require answers:

* what is the protection regarding staff?
* what is the allocated budget?
* what are the essential means?
* what are the actions to reduce the impacts?
* what is the contract with the recovery provider?
* what are the teleworking conditions?
* what means of communication are available in times of crisis?
* how prepared are the emergency premises?
* what is the level of performance of IT recovery?
* how can we justify the means of production with minimum recovery?
* what is the protection of transport means?
* what is the level of preparation of suppliers?

You can find more details on IT system business continuity in ISO 27031 (“Guidelines for Information and Communication Technology Readiness for Business Continuity”).

**8.3.5 Implementation of solutions**

The possible responses to an event are often multiple and compatible.

The selected business continuity solutions are feasible, applied and maintained before and during the occurrence of a disruption.

A realistic solution is often a compromise between cost and time (speed of recovery).

The necessary resources (alternative premises, personnel, equipment) are available at all times.

***Good practices***

* *each strategy includes several solutions*
* *the selected solutions protect critical activities*
* *adequate resources are available before the disruption*
* *the solutions selected have non-prohibitive costs*

***Bad practices***

* *selected strategies have only one solution*
* *the selected solutions do not take into account certain critical activities*
* *resources are not planned for critical activities*
* *the cost of certain solutions is not realistic (too high)*

**8.4 Business continuity plans** *(requirements* [*127 to 175*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#8.4)*)*

**The BCP is the last chance solution. Matthew Bennasar**

**8.4.1 General**

Using the results of the selected strategies and solutions, business continuity plans and procedures are established and aim to:

* control the response to a disruption
* warn and communicate with stakeholders
* apply solutions to restore critical activities within predefined deadlines

Examples of procedures and business continuity plans (BCPs) are shown in annexes 13 and 16.  enregistrement

The ultimate person in charge of the BCP is the director. He obtains the active participation of the business continuity manager and department heads. The latter contribute during the preparation of the BCP (determination of priority activities, awareness-raising and communication), the establishment of the crisis team and the implementation of the exercise program.

Plans and procedures allow:

* anticipate the main threats
* identify immediate measures to take during a disruption
* contribute to timely decision-making
* adapt to unforeseen risks
* focus on the anticipated impacts of disruptions
* minimize the impacts of the selected continuity solutions
* clearly identify roles
* assign responsibilities and authorities

**8.4.2 Response structure**

**Business continuity cannot be improvised**

An effective response structure is able to:

* identify events likely to cause disruptions
* provide an effective response to these disruptions

Crisis team members, roles during and after the disruption, responsibilities, authorities and hierarchy are established and documented, Responsibility and authority, cf. annex 16. 

Timely communication mechanisms (information and decisions) are determined, Communication plan, cf. annex 16. 

The response structure is specific for each company and takes into account:

* the existing structure
* the nature of the activities
* corporate culture
* the distinct threats identified
* selected business continuity solutions

Crisis teams are capable of:

* assess the nature of the disruption as well as its impact
* measure the impact against predefined thresholds
* determine whether a formal response is justified
* launch an appropriate response to a disruption (limit the damage)
* activate plans
* mobilize intervention teams
* guarantee the availability of required resources
* plan all necessary actions
* establish priorities for actions (the first always being staff safety)
* monitor the disruption, its evolution and the effectiveness of the response
* activate selected solutions
* communicate with stakeholders (staff, families concerned, authorities, customers, media)

Each team has:

* competent members
* documented procedures and plans, cf. annex 16 

**8.4.3 Warning and communication**

As seen in paragraph 7.4, effective control involves knowing how to communicate:

* what
* who
* when
* with whom
* how
* check the correct reception

Top management ensures that:

* information on public warnings and alerts (such as the national risk system) is managed correctly
* communications equipment and facilities during a disruption are available (satellite phones, two-way radios)
* stakeholders will be alerted in time to an imminent disruption
* communication with emergency services and other organizations is well-established
* the response to the media about a disruption will be timely, detailed and complete
* vital information about the Disruption, actions performed and decisions taken are recorded, cf. annex 16 

More details can be found in ISO 22322 (“Guidelines for Public Warnings”), cf. paragraph 2.2.

The Warning and Communication procedure is part of the exercise program, cf. paragraph 8.5 and annex 13.  

**8.4.4 Business continuity plans**

**An untested BCP is only marginally more useful than no BCP at all. Matthew Bennasar**

The Business continuity plan (BCP) is a preventive action that makes it possible to reduce the impacts of a disruption (incident, crisis, disaster, feared event) and restore the normal situation. Some examples are given in annex 16. The BCP does not replace the tools for managing everyday problems and incidents. 

Business Continuity Plan (BCP): *planned measures to ensure the recovery of essential activities following a disruption*

A BCP is always “homemade” by a multidisciplinary team and takes into account the corporate culture. A BCP includes the information and recommendations necessary to address any disruption based on the results of:

* the business impact analysis, cf. paragraph 8.2
* selected strategies and solutions, cf. paragraph 8.3

The purpose of the BCP is to ensure the resilience of the company. The objectives of the BCP are:

* reduce the impacts of the disruption
* guarantee priority activities during the disruption
* control the recovery to the normal situation

The Crisis team is solely responsible for the application of the BCP and the decisions to be taken during a major disruption (disaster, emergency), cf. annex 16. 

A BCP, in the form of a procedure or document, includes:  

* critical activities
* the desired goal
* the scope
* the objectives set
* the risks identified
* the roles of the crisis team
* predefined initiation criteria (assigned authority)
* the meeting place of the crisis team
* protection of personnel
* communication and coordination internally and externally
* monitoring the impacts of the disruption
* BCP dependencies
* the necessary resources
* actions to recover critical activities
* delivery of products and services at the agreed capacity level
* managing the consequences of the disruption
* report management (information on the disruption, actions taken, decisions taken)

The analysis of the consequences takes into account:

* the health and safety of staff
* preventing the loss of certain critical activities
* the impact on the environment

The BCP is updated annually. Unless following a change such as:

* structural (acquisition, move, division, reorganization)
* internal (new executives, new suppliers)

An effective BCP is:

* simple and flexible
* communicated and understood by all staff, cf. paragraph 7.4
* known and reviewed by the crisis team, cf. paragraph 7.5
* available when a disruption occurs, cf. paragraph 8.4
* tested (simulation exercises), audited and reviewed, cf. paragraphs 8.5, 9.2 and 9.3
* updated regularly, cf. paragraph 8.6
* understands lessons learned from past exercises and disruptions, cf. paragraphs 8.5, 9.3 and 10.2

The Business continuity plan is validated by top management, cf. annex 16. 

 Questions that require answers:

* who is the audience for the BCP?
* how can we communicate the BCP?
* what means of communication should we use?
* when were the objectives of the BCP reviewed?
* what is the cost/benefit ratio of the selected solution?
* how do we know that the level of risk is acceptable?
* how effective are the BCP exercises?
* how does the BCP reduce the impacts of the disruption?
* what is the authority of the crisis team?

**8.4.5 Recovery**

The Recover activities process is determined in order to restore and resume all business activities after the temporary measures adopted during and after a disruption, cf. annex 04.  

Resumption of business may involve returning to restored premises or moving to new premises.

During the restoration of activities, the following actions can be taken:

* manage communication during and after the disruption
* determine recovery activities:
  + designate the person in charge of recovery
  + validate the business impact analysis
  + choose risk treatment actions
  + define actions to protect priority activities
  + undertake preventive actions to reduce the risk of disruption
  + reduce and validate the MTPD
  + prepare and apply IT recovery
  + define the resources necessary for recovery of:
* additional staff
* finances (purchases, insurance policies)
* transport and logistics
* emergency providers
* select recovery options
* establish the sequence of recovery activities (restore damaged facilities)
* define emergency means
* raise staff awareness of their responsibility and role
* train the crisis team
* carry out a complete audit after recovery

***Good practices***

* *the response structure is updated*
* *business continuity plans are available in a known location*
* *the responsibilities and authorities of the crisis teams are established*
* *the communication procedure is clear and transparent*
* *the BCPs are updated and realistic*
* *resources for BCPs are properly planned*
* *the process of restoring activities includes how to obtain funding*

***Bad practices***

* *communication with stakeholders before and during a disruption is insufficient*
* *BCPs are not available*
* *the hierarchy of authorities of the crisis teams is not defined*
* *the communication procedure is incomprehensible to staff*
* *resources for BCPs are not available*
* *the restore activities process does not include IT recovery*

**8.5 Exercise program** (*requirements* [*176 to 184*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#8.5)*)*

**The results from a simulation are only as good as the inputs. Edmund Conrow**

The Exercise program is annual and validated by top management. It allows the application of selected business continuity strategies and solutions to be discussed in detail and simulated in the field, cf. annex 16. 

The program contributes to the achievement of strategic objectives and includes:

* business continuity plans
* the objectives to be achieved
* the calendar
* the scope
* the personnel concerned
* the capacities
* resources (budget and time required)
* stakeholders likely to participate in recovery activities
* confidentiality and information security provisions

The exercise and test program:

* is consistent with business continuity objectives, cf. paragraph 6.2.
* is based on the selected simulation scenarios, cf. paragraph 8.3
* is realistic and carefully planned to reduce the risk of incidents resulting directly from the exercise

The exercises and tests allow you to:

* verify and validate the usefulness and effectiveness of business continuity strategies and solutions
* ensure that the BCPs are achievable
* assess capacities and resources to manage a crisis and restore priority activities
* check dependencies on stakeholders
* write improvement reports following lessons learned
* develop the skills of crisis team members
* raise staff awareness of the principles of business continuity
* meet legal and regulatory requirements

The program is:

* updated following significant changes in the business or context
* reviewed annually to include opportunities for improvement proposed following the exercises

The Exercise results are used to improve the BCMS, cf. paragraph 10.2 and annex 16. 

You can find more details on the exercises in:

* ISO 22320 (“Guidelines for Incident Management”), cf. paragraph 2.2
* ISO 22398 (“Guidelines for Exercise”), cf. paragraph 2.2

***Good practices***

* *the program is respected*
* *the program objectives are consistent with the business continuity strategy*
* *the effectiveness of BCPs is verified in the field*
* *opportunities for improvement following the exercises are put in place*

***Bad practices***

* *the program is not updated*
* *the program is with missing objectives*
* *the BCPs are verified only from a documentary point of view*
* *no improvement proposals are documented following the exercises*

**8.6 Evaluation** *(requirements* [*185 to 190*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#8.6)*)*

**Only use documentation that makes sense and adds value**

An evaluation of adequacy and effectiveness is carried out periodically on:

* the business impact analysis
* risk assessment
* selected business continuity strategies and solutions
* business continuity plans and procedures

The evaluation is based on the results of the exercises and tests, the incidents that occurred and the changes made. Carrying out the evaluation can take the form of:

* internal or external audit
* self-assessment
* analysis
* exercise
* testing
* post-incident report

The results of the evaluation make it possible to update the business continuity policy and objectives.

The evaluation checks whether:

* all activities relating to products, services, processes and resources are identified and included in business continuity solutions
* the competence of the people concerned is sufficient
* the response to a disruption includes the control of its:
  + management
  + command
  + coordination
* business continuity solutions are updated
* the exercise program is respected
* the training and awareness program is respected
* the BCPs are communicated to the personnel concerned
* staff understand their responsibility during a disruption
* stakeholder requirements are understood and can be met
* dependencies of priority activities are appropriate and adequate
* legal and regulatory requirements are applied
* best practices in the sector are known and used
* change management is respected
* the company can demonstrate a high level of resilience
* all documentation is updated

Examples of effectiveness measures:

* the backup data is completely up-to-date
* accommodation and equipment required for resuming activities are available
* the required skills are in place to:
  + react quickly to a disruption
  + manage an incident
  + resume priority activities

The results of the Business continuity capacity review are retained, cf. annex 16. 

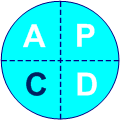
 Minute of relaxation. Cf. joke “[Every Wednesday?](https://www.pqbweb.eu/page-some-jokes-to-distract-yourself-from-training.php#Every)”

***Good practices***

* *evaluations are periodic and the results are kept*
* *the evaluation verifies compliance with the awareness program*
* *legal and regulatory requirements are applied*
* *all BCPs are updated*

***Bad practices***

* *the evaluation of certain parts of the BCMS is not carried out*
* *assessment results are not kept*
* *the training program is not evaluated*
* *the verification of all BCPs is not complete*

**9 Performance **

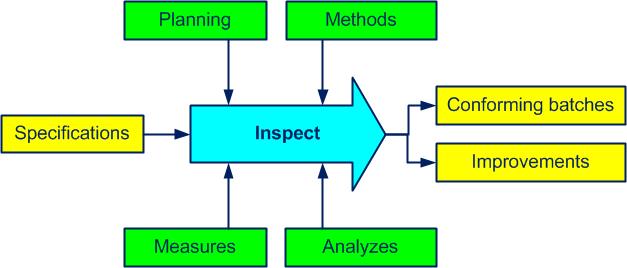
**9.1 Inspection, measure and analysis** *(requirements* [*191 to 196*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#9.1)*)*

**If you can’t measure it, you can’t manage it. Peter Drucker**

The necessary measurements and monitoring (who, what, how, when) or in other words the inspection is carried out:

* in reception (raw materials, semi-finished products)
* in production (critical process points, semi-finished products) and
* at the end (finished products)

The “Inspect” process (see figure 9-1) provides the information necessary for analyses and evaluations which lead to continual improvement actions, cf. annex 04. 



*Figure 9-1. The inspect process*

Inspection: *actions of measures, trials and surveys of a process, product, service or material to establish whether requirements are met*

The inspection and analysis methods are appropriate to the specificities of the company, are easily reproducible and ensure the validation of the results.

Inspection, analysis and evaluation activities are kept in the Performance evaluation document, cf. annex 16. 

Performance: *measurable and expected results of the management system*

The data from the evaluation of the performance of the business continuity management system are presented in the management review (see paragraph 9.3).

***True story***

*After a signal from a group manager, a financial analysis of the activities of our site was carried out. Receiving inspections were particularly targeted. To everyone's surprise, it turned out that the cost was really disproportionate to that of the nonconformities found.*

*A reduction in activities (and a transfer of staff) was quickly implemented.*

The results of the inspection and analyses help to:

* assess:
  + the performance of the BCMS
  + the need to improve the BCMS
  + the conformity of the product produced and the service provided
  + the performance of:
* processes
* external providers
* confirm skillful planning of the business continuity management system
* implement actions to address risks
* seize opportunities for continual improvement

***Good practices***

* *the results of the data evaluation lead to numerous improvement decisions*
* *inspection results of key characteristics of activities that may impact business continuity are used as relevant data to assess BCMS compliance*
* *the location of each piece of equipment is established in the master list of equipment*

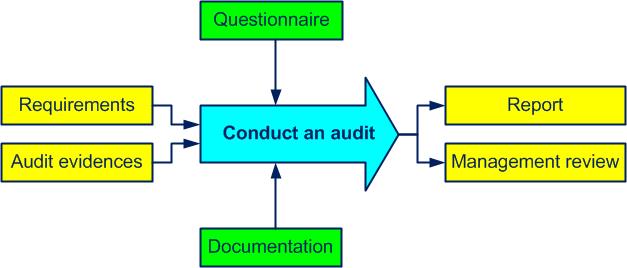
***Bad practices***

* *decisions from the analysis of inspection results are not retained*
* *BCMS performance measures are not available*
* *monthly inspections of activities with impact on business continuity not kept*
* *inspection activities are neither defined nor planned*

**9.2 Internal audit** *(requirements* [*197 to 207*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#9.2)*)*

**The quality control should verify the process, not the product. Edwards Deming**

The “Conduct an audit” process (see figure 9-2) makes it possible to assess the compliance and effectiveness of the business continuity management system, cf. annex 04.  



*Figure 9-2. The conduct an audit process*

Internal audits regularly check whether the business continuity management system is correctly implemented and remains operational.

Compliance is determined in relation to:

* planned and agreed arrangements
* compliance with the requirements of:
  + ISO 22301
  + the company’s business continuity management system

Audit: *systematic and independent survey to determine whether activities and results comply with pre-established measures and are capable of achieving the objectives*

An audit can be of:

* the business continuity management system
* a process
* a product
* a service

Audit evidence: *demonstrably true data related to audit criteria*

Examples of audit evidence:

* process sheet
* job description
* training attendance sheet
* information on customer returns
* level of indicators

Audit planning (annual Audit program) is done based on the status and importance of processes, products and services and their impacts on business continuity, cf. annex 16. 

When planning and implementing the audit program, the following are taken into account:

* the results of previous audits
* business continuity objectives
* feedback
* the changes introduced
* threats and opportunities

An auditor cannot audit his department because:

**No one should be a judge in his own case. Latin proverb**

The competence of internal auditors is based on:

* experience in carrying out audits
* training followed
* knowledge of:
  + ISO 19011 recommendations
  + ISO 22301 requirements
* business continuity management principles

The business continuity manager defines for the audits:

* responsibilities
* selection of auditors
* requirements for:
  + plan
  + conduct audits
  + record the results (audit report)
  + communicate the results
* audit criteria
* the scope (the area of application)
* frequency
* the methods

The audit follow-up (which can be a complementary audit) makes it possible to verify the implementation of corrective actions and identified opportunities for improvement.

Documents of the implementation of the audit program and the results of the audits (Audit report) are kept, cf. annex 16. 

The results of internal audits are presented to the relevant department heads. These results are one of the input elements of the management review and make it possible to seize opportunities for improving the business continuity management system.

Internal audit activities are carried out using ISO 19011 as a basis, see paragraph 2.2 and training T 56v19 ISO 22301 Internal Audit.

***True story***

*Following a customer complaint, the director asked the quality manager to immediately conduct an unplanned process audit. Later we understood that this audit was the final straw and led to the dismissal of the quality manager because he did not find the time to go to the workshop (he only looked at the documentation).*

*Therefore, audit documentation is important, but within certain limits.*

Description : smileMinute of relaxation. Cf. joke "[The engineer and the shepherd](http://www.pqbweb.eu/page.php?id=31#engineer)"

***Good practices***

* *the crossover audit (exchange between two companies) is very judicious and rich in findings*
* *the audit program covers all essential processes of the business continuity management system*
* *the objectives of the audit program are consistent with the business continuity policy and the specificities of the company*
* *the audit program is communicated to the people concerned well before the first audit*
* *each audit report contains identified good practices*
* *any improvement opportunities found during an audit are applied to other processes or products*
* *an unscheduled audit requested by a department at a delicate stage very often brings added value*

***Bad practices***

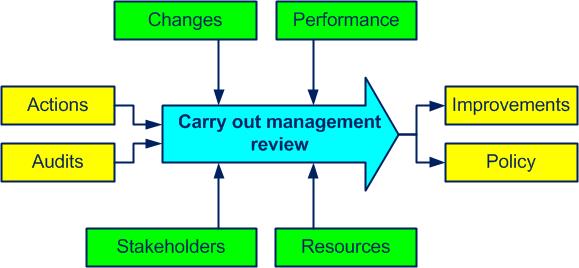
* *the audit program is neither respected nor updated*
* *the audit program does not cover all the requirements of the ISO 22301 standard*
* *the list of internal auditors is not updated*
* *the scope of the audit falls within the responsibilities of the auditor*
* *audit report not retained*
* *the audit report does not contain any track for improvement or any action*
* *the action requested in the audit report is not implemented within the proposed deadline*
* *audit conducted by a trainee without sufficient skills and experience (and is not part of the list of auditors)*
* *the results of audits are not systematically proposed as an input to the management review*

**9.3 Management review** *(requirements* [*208 to 228*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#9.3)*)*

**No system is perfect**

Top management plans and carries out (at least once a year) a review of the BCMS.

The “Carry out management review” process is shown in figure 9-3, cf. annex 04.  



*Figure 9-3. The carry out management review process*

The results of the Management review are recorded (see annex 17). 

Its objective is to review whether the business continuity management system is relevant, effective and adequate with the company's vision.

Management review: *periodic survey of the management system for its continual improvement carried out by top management*

Management review inputs include:

* audit results
* inspection results
* the situation of the necessary resources
* the results of the assessment of compliance with legal and regulatory requirements
* feedback from stakeholders (satisfaction and complaints)
* the level of achievement of business continuity objectives and associated indicators
* monitoring of actions:
  + resulting from decisions from the previous management review
  + treatment of nonconformities
* information on the performance of:
  + processes, products and services
  + competitors
  + external providers
  + partners
* changes in external and internal issues that may affect the business continuity management system and the associated threats and opportunities
* the results of the business impact analysis and the risk assessment
* procedures and resources that can improve the BCMS
* the results of the BCMS evaluation
* untreated risks
* lessons learned from disruptions and near misses

Management review outputs include decisions related to:

* opportunities for improvement:
  + the business continuity management system and its processes
  + of the product and service
* needs for change of:
  + the business continuity management system (business continuity policy and objectives)
  + the scope
  + the business impact analysis
  + risk assessment
  + strategies and solutions
  + BCPs
* procedures and means of control
* means of control and measurement of their effectiveness
* resource requirements in order to maintain the business continuity management system and continually improve its effectiveness

The results of the management review are communicated to relevant stakeholders.

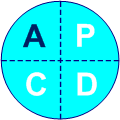
The actions decided in the management review are applied and their effectiveness will be reviewed by the business continuity manager.

***Good practices***

* *process review occurs prior to management review*
* *analysis of process performance is presented by each process owner*
* *any change proposal is preceded by an impact assessment*
* *when the favorable opportunity presents itself, people who deserve it are congratulated*
* *decisions are communicated to all staff*
* *process risks are analyzed, and the effectiveness of actions evaluated*

***Bad practices***

* *follow-up of actions from the previous review is not presented*
* *the frequency of the chosen management review is not respected*
* *the level of achievement of objectives is not analyzed*
* *the state of current actions is not commented on*
* *no decision to change objectives and indicators*
* *decisions relating to improving the efficiency of the BCMS and processes are non-existent*
* *personnel and material resource requirements are not quantified*

**10 Improvement **

**10.1 Nonconformity** *(requirements* [*229 to 240*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#10.1)*)*

**Where there is a problem, there is potential for improvement. Masaaki Imai**

Staff seek, find and implement improvement opportunities primarily to achieve BCMS objectives.

The improvement is carried out on:

* the process
* products and services
* undesirable effects
* the business continuity management system

Opportunities for improvement exist in cases such as:

* the reduction of nonconformities
* respect for deadlines
* cost reduction
* the establishment of operational means of control

***True story***

*The paradox of decreased costs by product when the size of the batches decreases.*

*Logically, the bigger the batch size, the lesser the unit cost.*

*But this is not what Taiichi Ohno, known for his anti-common-sense solutions, thought. He showed that mass production often has hidden costs (waste) that substantially increase the unit cost.*

*The hidden costs are related to defects that are discovered very late, including activities (and resources) needed in order to sort the products and repair defects, to transport and store a large quantity of products, the size of the storage area required to keep inactive products (and money too); and the need for cut-price sales (due to products having become obsolete in the meantime) and exceptional transportation (to meet the deadline).*

Responsibilities and authorities necessary for handling nonconformities are established.

Any nonconformity is identified, analyzed and dealt with. Treating nonconformities includes activities such as:

* identify and analyze nonconformities (customer complaints are part of this)
* isolate nonconformities
* implement curative actions
* determine the causes
* assess risks
* assess the need for corrective actions to prevent the reappearance of nonconformities or significantly reduce their frequency of occurrence
* implement corrective actions
* monitor the effectiveness of actions carried out

If necessary:

* update the list of risks
* change the business continuity management system

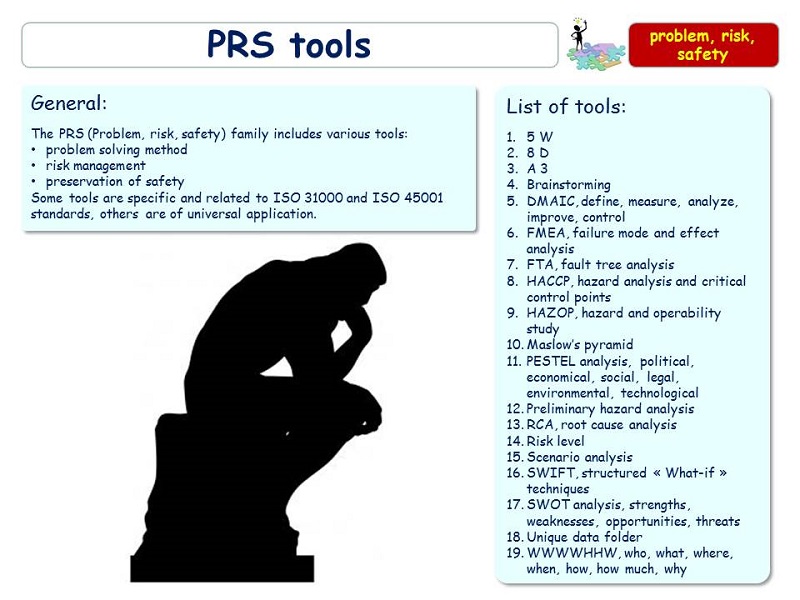
Corrective actions are proportional to the consequences of nonconformities (do not go overboard on quality).

Examples of nonconformities:

* legal requirement not respected
* operational instruction not respected
* unaddressed stakeholder complaint
* gaps found during an audit
* business continuity objective not achieved
* action in the face of an identified risk not implemented

Nonconformities (nature, quantity, frequency of occurrence), corrective actions undertaken and the results obtained are kept and communicated to the people concerned.

Some examples of PRS tools (problem, risk, safety) are shown in figure 10-1 and the detailed sheets in annex 07. 



*Figure 10-1. PRS family tools*

You can find more quality tools in the [*D 12*](https://www.pqbweb.eu/document-d-12-quality-tools-for-your-operational-management-system-set-of-documents.php) set.

***Good practices***

* *any improvement opportunity found during corrective action is applied to other departments, processes, products, services*
* *each nonconformity is used to improve the process*
* *repaired products are 100% inspected before entering the normal flow*
* *monitoring of the effectiveness of corrective actions is carried out systematically*

***Bad practices***

* *certain opportunities for improvement are identified without any action being taken*
* *responsibility and authority for controlling nonconformities are not defined*
* *after the analysis of the causes no corrective action follows*
* *absence of analysis of the causes of nonconformities*
* *lack of evidence of elimination of the causes of nonconformities*

**10.2 Continual improvement** *(requirements* [*241 to 242*](https://www.pqbweb.eu/page-iso-22301-version-2019-requirements-business-continuity-management-systems.php#10.2)*)*

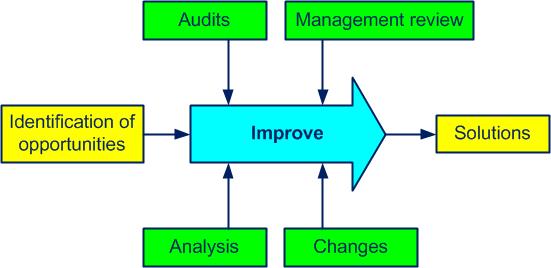
**Life is like riding a bicycle. To keep your balance, you must keep moving. Albert Einstein**

The implementation of the BCMS makes it possible to seize opportunities for improvement in various areas such as:

* improving the BCMS and its:
  + suitability
  + effectiveness (achievement of objectives)
* optimization of process efficiency (cost/benefit ratio)
* consolidation of responsibilities
* better organization
* the spreading of good practices
* flexible improvement plans

The “Improve” process (see figure 10-2 and annex 04) is based, among other things, on:  

* stable processes
* the results of internal audits
* management review decisions
* business impact analysis
* lessons learned following:
  + exercises and tests
  + past incidents and disruptions
* good practices among partners and competitors
* establishing new improvement objectives
* the search and justification of solutions
* implementing solutions and measuring results
* the formalization of changes when the objectives are achieved



*Figure 10-2. The improve process*

**If you want to move a mountain, start by removing the small stones. Chinese proverb**

The Kaizen method (attitude, event) (from the Japanese kai = to study, zen = to improve) of continual improvement is based on the principle of small concrete improvements made by everyone and all the time. It is a formidable tool in the fight against waste in all its forms.

Continual improvement: *process allowing the improvement of the global performance of the organization*

***Good practices***

* *the effectiveness of the BCMS is demonstrated via qualitative and quantitative measurements*
* *the results of the management review are used to improve the BCMS*

***Bad practices***

* *proposed opportunities for improvement are not seized*
* *the results of the management review are not communicated to staff*

**Annexes**

Annex 01 Certification project plan (PQBD26V19A01)

Annex 02 Business continuity successes and failures (PQBD26V19A02)

Annex 03 Process review (PQBD26V19A03)

Annex 04 Specific processes (PQBD26V19A04)

Annex 05 Process approach (PQBD26V19A05)

Annex 06 Glossary (PQBD26v19A06)

Annex 07 PRS tools (PQBD26V19A07)

Annex 08 List of stakeholders (PQBD26V19A08)

Annex 09 Scope (PQBD26V19A09)

Annex 10 Business continuity policy (PQBD26V19A10)

Annex 11 List of risks (PQBD26V19A11)

Annex 12 Risk level (PQBD26V19A12)

Annex 13 Specific procedures (PQBD26V19A13)

Annex 14 Risk support, Excel (PQBD26V19A14)

Annex 15 Risk treatment plan, Excel (PQBD26V19A15)

Annex 16 Specific records (PQBD26V19A16)

Annex 17 Management review (PQBD26V19A17)

Annex 18 Good practices (PQBD26V19A18)

Annex 19Bad practices (PQBD26V19A19)

Annex 20MCT ISO 22301 (PQBD26V19A20)

Annex 21 Quiz ISO 22301 (PQBD26V19A21)

Annex 22 Case studies (PQBD26V19A22)