AMRAE COLLECTION
**RISK MANAGEMENT**

# BUSINESS Continuity Plans

AMRAE
la Maison du risk management

# Foreword

**Version 2.0 – April 2026**

| | |
|---|---|
| Revision, coordination and overall consistency: | Benoit Vraie & Elodie Yayer Dunand |
| Based on version 1.0 (2013) – Initial drafting: | Benoit Vraie & Sophie Huberson |
| Technical contributions: | The following people have made a significant technical contribution and/or provided field experience feedback in their area of expertise.<br><br>Cyber BCP: Olivier Allaire, Christophe Pelfresne<br>Climate BCP: Elodie Yayer Dunand, Santiago Bosio, Christophe Bouvard, Linda Khelid |
| Proofreading: | Jason Crumley (overall proofreading and English translation)<br>Maureen Chagnon (consistency of climate updates) |
| Art direction: | La Nageuse Agency |

Faced with the intensification of extreme climate events, floods, heatwaves, storms, forest fires, and the explosion of cyber intrusions, ransomware, and digital sabotage, organizations must deal with increasingly systemic threats. Neither climate adaptation alone, nor the strengthening of IT defenses in isolation, will be enough to contain their effects.

In this context, implementing a Business Continuity Plan (BCP) today requires going beyond the simple analysis of internal resource unavailability.

Recent extreme events, the 2022 heatwave, storms and floods in Spain in 2024 (DANA), floods in southeastern France, forest fires in California, or major cyber crises, ransomware attacks against French hospitals in 2023, the La Poste attack in 2025, remind us to what extent organizations are interconnected systems. They depend on a network of partners, suppliers, physical infrastructure, digital systems, public services... all links whose failure can trigger domino effects, even rendering continuity solutions themselves inoperative.

Furthermore, resilience is not born at the moment of a crisis; it is prepared well in advance, and it is now that companies/organizations must update their BCP. Moreover, a BCP is never static; once developed, it must be regularly tested and updated to remain operational. Crisis exercises are an essential lever in this regard. By testing varied and sometimes complex scenarios, organizations identify previously unsuspected weaknesses. Each lesson learned and each improvement made thus contributes to strengthening the collective capacity to maintain essential activities when the situation truly deteriorates.

This is why updating the book *"Business Continuity Plans,"* published in 2013, and fully integrating the climate and cyber dimensions in 2026, appeared to be a necessity. This book offers a renewed reading of BCPs, in light of climate and cybersecurity challenges, to support organizations in their transition toward sustainable resilience.

> It is not the strongest of the species that survives, nor the most intelligent, but the one that is most adaptable to change.
>
> Charles Darwin

# Table of Contents

# Introduction

When an athlete is injured mid-competition, two questions arise: Is it serious? When can I train again? Their coach, doctors, and physical therapists know them well enough to answer quickly — drawing on two things that keep recovery on track: flawless organization and motivation. But full recovery also requires self-knowledge: understanding exactly how far each part of the body can be pushed.

The same principle applies to organizations. A Business Continuity Plan (BCP) does more than safeguard operations after a loss — it helps the company know itself better. Building a BCP means identifying vulnerabilities, yes, but it also demands a deeper exercise: introspection, inventory, and process mapping alongside the resources those processes rely on.

This work therefore extends far beyond crisis preparation. It gives the organization a chance to critically revisit its fundamental operating cycles and optimize them.

This introspection matters even more now because the threat landscape has changed radically. Business continuity was originally built around accidental disasters, but it must now confront a new reality: the criminal adversary and the systemic cyber-crisis. As we will see, preparing for breakdowns and physical damage is no longer enough — deliberate attacks now target the digital heart of the company and its ecosystem.

Business continuity is, in essence, a corporate philosophy: *"preparing for war in peacetime"*(1). By analyzing threats before(2) they occur and planning the response in advance, a BCP minimizes the operational impact of a disaster. It enables the company to keep running — in degraded mode when necessary — and to bring activities back online in order of priority, from most critical to least.

The first outlines of BCPs emerged in the **1970s and '80s,** in industrial and service processes — particularly in sectors classified as *"critical"*: banking, aerospace, defense, and food processing. At the same time, the growing importance of data and the increasing complexity of network architectures drove the development of IT Disaster Recovery Plans (DRPs) — the IT equivalent of a BCP.

The **1990s and 2000s** saw the rise of economic globalization. Two consequences followed: significant industry consolidation and the exponential growth of subcontracting — and therefore of competition — originating from emerging economies, particularly in Southeast Asia.

In the constant pursuit of higher profitability, companies made organizational choices that left them particularly exposed to supply-chain disruptions. A single adverse event in one location — an extreme climate event, for example — can cascade through the entire supply chain, triggering shortages and production stoppages across multiple regions.

Over the past two decades, business continuity has

(1) in *"Managing Major Crises: Health, Ecological, Political, and Economic"*, L. CROCQ and al. Odile JACOB

(2) Before any crisis

evolved from a best practice into a foundational regulatory requirement in several sectors deemed sensitive or systemic. Major crises — financial, digital, health, energy, and geopolitical — have accelerated this shift, underscoring the need to keep essential services running, even in degraded conditions.

The banking sector illustrates this most clearly: business continuity is now a pillar of operational resilience. Financial institutions must demonstrate their capacity to maintain critical activities, defined [unofficial translation] as the *"set of measures intended to ensure — under various crisis scenarios, including extreme-shock scenarios — the continued delivery of essential or important services and operational tasks (where appropriate, on a temporary basis and in degraded mode), followed by the planned resumption of activities"*.

Historically, the cornerstone of BCP policy, this definition now sits within a broader framework — one that also integrates governance, risk management, technological dependencies, and extended value chains.

In France, this concern began translating into collective action in the **mid-2000s**. A think tank known as Groupe de place Robustesse (Paris Financial Marketplace Resilience Group) was established in 2005 to model crisis scenarios that could simultaneously affect the players in the Paris banking and equities marketplace.

A first large-scale exercise took place on June 4, 2008, bringing together about fifteen major banks and Paris marketplace institutions, along with government representatives. The scenario simulated a major technical crisis triggered by a prolonged power outage across the Île-de-France region, producing widespread disruption for both the financial system and the real economy. This work foreshadowed today's extreme-scenario and systemic-scenario approaches.

The insurance sector faces parallel obligations. Solvency II requires insurers to put in place governance, risk management, and continuity arrangements proportionate to their activities and the risks they carry.

**Since January 17, 2025,** the regulatory framework has been significantly strengthened by the application of Regulation (EU) 2022/2554 — the Digital Operational Resilience Act (DORA) — on digital operational resilience in the financial sector.

DORA requires in-scope financial institutions to embed, within their ICT risk management framework, both business continuity plans and incident response and recovery plans. These must include documented provisions, procedures, periodic tests, and recovery mechanisms designed to keep critical functions running and maintain operational resilience through disruptions.
In practice, financial entities must design, maintain, periodically test, and revise their continuity and recovery plans as part of a comprehensive operational resilience policy. These mechanisms rely on:

- Business Impact Analyses (BIA);
- Appropriate recovery objectives (RTO — Recovery Time Objective; RPO — Recovery Point Objective);
- Mapping of critical dependencies, including third-party providers;
- Regular exercises and tests to verify that essential activities can continue even in the event of a failure or major incident.

Beyond finance, other sectors face enhanced regulatory obligations around continuity and resilience — most notably the Sectors of Vital Importance (SAIV) defined in the French Defense Code and the ministerial order of June 2, 2006. This national mechanism remains in force and now sits within a broader, modernized framework: the transposition of the European Directive on the Resilience of Critical Entities (CER).

Operators of Vital Importance (OIVs), whether public or private, carry out activities essential to the functioning of the country. As such, they must implement structured crisis management and business continuity arrangements covering every risk that could affect essential services. These arrangements must be formalized, maintained over time, and tested regularly through exercises.

The CER Directive strengthens this approach in two ways: it establishes a comprehensive view of resilience — integrating digital, physical, organizational, and human dimensions — and it reinforces coordination between public and private actors. Business continuity thus becomes part of a systemic-resilience logic, at the heart of governance and security for critical organizations.

Business continuity standards and frameworks multiplied during the 2010s, but ISO 22301 (Business Continuity Management Systems) has emerged as the central reference. It defines the requirements for structuring a business continuity management system — from business impact analysis through plans, tests, and continuous improvement.
ISO 22301 is supplemented by other standards in the ISO 22300 family and by standards addressing IT continuity. In regulated sectors, these standards work alongside sector-specific regulatory frameworks rather than replacing them.

The GSDNS (General Secretariat for Defense and National Security) also published its Guide for Creating a Business Continuity Plan in 2013 — freely available on the GSDNS website (sgdsn.gouv.fr). This guide remains a widely used methodological reference and repository of best practices, particularly in the public sector and for activities of vital importance. It should nonetheless be used in combination with — and aligned to — ISO 22301 and any applicable regulatory or sectoral frameworks.

CER DIRECTIVE

## The new pillar of European resilience

The European CER Directive (2022/2557) strengthens the capacity of critical entities to ensure the continuity of essential services, energy, water, health, transport, digital infrastructures, in the face of climate, cyber, or geopolitical crises.

It imposes an all-hazards approach, including threat analysis, the implementation of resilience plans, protection measures, regular exercises, and mandatory notification of significant incidents.

In France, at the date of publication of this work, transposition is still underway: the bill was adopted by the Senate in March 2025, then amended at the National Assembly in September 2025, and is still awaiting its final vote.

This directive marks a major turning point: it moves organizations from a protection mindset to a genuine culture of operational resilience, essential for structuring BCPs in vital sectors.

# DEFINITION AND PURPOSE OF THE BCP AND ITS ENVIRONMENT

Chapte


HICT
Q 01
Q 02
CẢNG CONG-TEN-NƠ QUỐC TẾ HẢI PHÒNG
MAERSK SARAT

# 1.1. DEFINITIONS AND PURPOSES OF THE BCP

## 1.1.1. Definitions

#### 1.1.1.1. Critical review of the given definitions

If we refer to Regulation 97-02 of the Banking Regulation Committee, the BCP is the *"Set of measures aimed at ensuring the maintenance, if necessary temporarily in a degraded mode, of the organization's essential service provisions, and then the planned resumption of activities"*.

#### 1.1.1.2. Proposed definition

The Business Continuity Plan is the alternate operating model that the organization deploys while working to resolve the disruptive event that caused the process interruption.

The BCP takes the form of a document **that identifies, lists, plans, and sequences** the continuity and/or recovery actions to be implemented in the event of undesirable events, of varying severity.

It sets the organizational and technical modalities for the company's operation in *"degraded"* mode, and then for the gradual resumption of activities, from the most sensitive to the least sensitive.

## 1.1.2. What is a BCP for?

The Business Continuity Plan ensures the sustainability of critical processes in case of unavailability of one or more resources in the work environment. In other words, the BCP serves to cushion the effects of a potential crisis, to minimize impacts in the event of a disaster, and to guarantee the continuation of the company's activity despite the occurrence of undesirable events. It is a decision-making toolkit for the crisis management team.

These objectives relate as much to financial and economic performance as to social and environmental performance, as well as the restoration of the organization's reputational capital.

## 1.1.3. Philosophy of the BCP

The BCP is not a manual gathering dust on a shelf; it is, above all, a mindset for achieving the objectives set out in the business plan.

*"Preparing for war in peacetime"* consists of answering questions before the event, to free oneself from the hazards of improvisation and

the constraint of response times when the crisis actually occurs. It is therefore essential to put in place in advance — in the *"cold"* phase, before any crisis — all the rational elements the team can draw on *"hot"*, in the very first minutes of the crisis. Of course, not everything can be anticipated, the team will need to constantly adapt to the conditions of the reality of the crisis by analyzing them and drawing conclusions to modify the order of restarting processes, depending on the context (e.g., an advertising campaign for the launch of a new product).

## 1.1.4. How to set the level of activity maintenance?

The objective of the BCP is not to *"duplicate"* the organization to allow for identical continuity, but to analyze the impact of the crisis for each business line and each process and to classify them according to a Maximum Tolerable Period of Disruption (MTPD). It therefore allows for *"degraded"* functioning of the organization's processes and their gradual resumption, from the most sensitive to the least sensitive.

Also, the level at which activity is maintained results from combining the ability to meet regulatory, technical, and societal constraints with senior management's willingness to sustain operations at a given level. Ultimately, this translates into an acceptable level of investment to prepare the plan and sustain its operation: the BCP must define the acceptable trade-off between financial commitment and the level of activity maintained.

Reducing the BCP to a set of technical solutions — without a management strategy owned by senior leadership — can render every effort and investment futile.

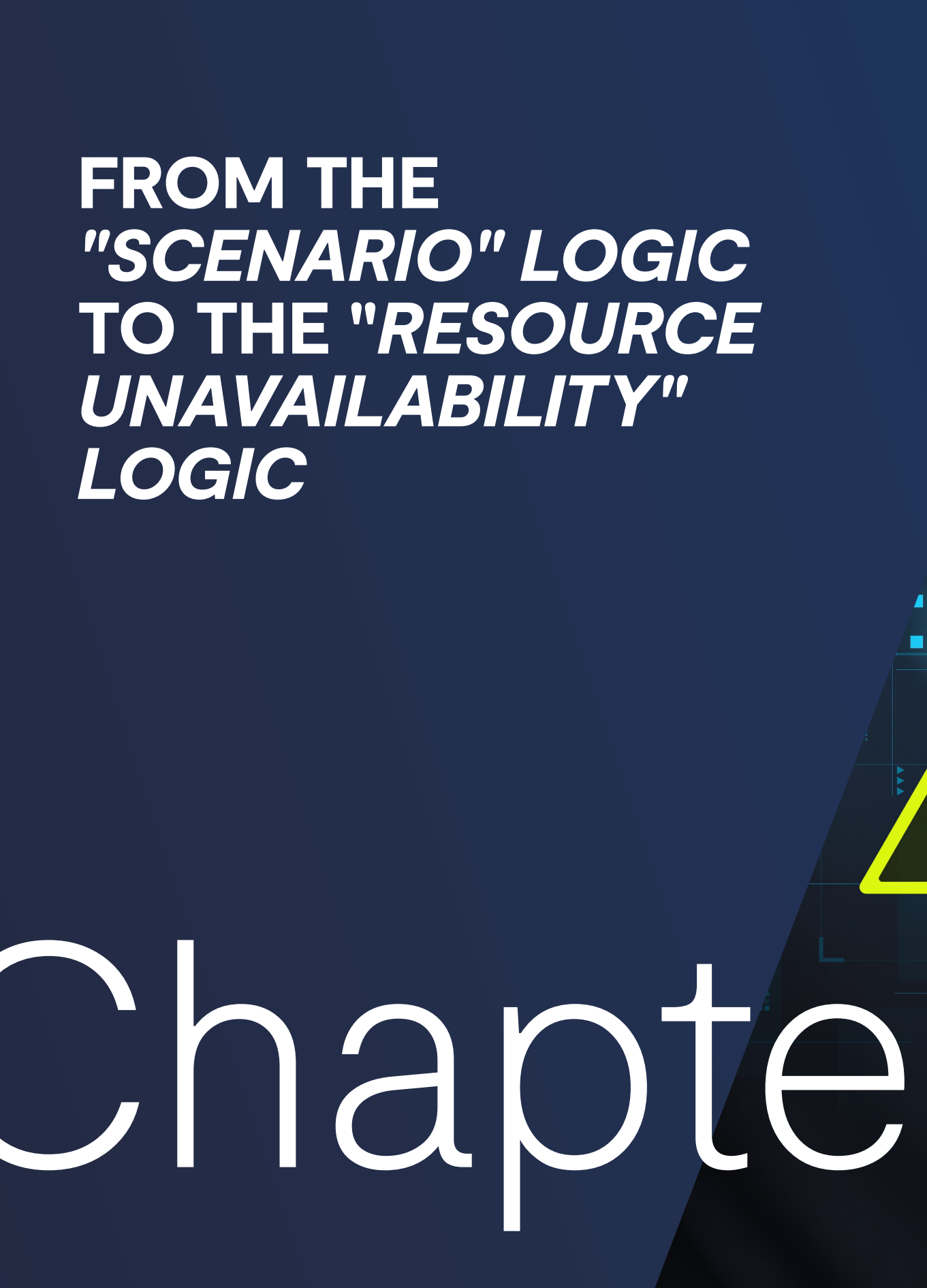
## 1.1.5. Business Continuity Plan and Emergency Plan, what is the difference?

An emergency plan is intended to organize the immediate response to a sudden event, such as a fire, a flood, or any other situation endangering people or the safety of the site. It aims above all to manage the event at the time, to protect individuals, and to stabilize the situation. However, these emergency plans do not describe continuity solutions. They must be coordinated with recovery plans and business continuity plans.

The Business Continuity Plan (BCP) intervenes once the emergency is under control or in parallel with its management, with the objective of maintaining the organization's essential activities, even in degraded mode. It provides the key elements to manage the consequences of the emergency and ensure the continuity of services in case of unavailability of infrastructure, resources, systems, or key stakeholders in the value chain. It relies on an impact analysis, the definition of priorities, and the implementation of fallback solutions allowing operations to continue despite the disruption.

The emergency plan and the BCP are complementary: the former addresses the immediate crisis, while the latter ensures the organization continues to function during and after the event.

# FROM THE *"SCENARIO" LOGIC* TO THE "*RESOURCE UNAVAILABILITY" LOGIC*




r 2

# 2.1. CRITIQUE OF THE *"SCENARIO"* METHODOLOGY/LOGIC

A crisis is always a film with no written script.

The business continuity approach based on scenarios starts from the premise that it is necessary to identify the origins of the threats weighing on the organization before implementing business continuity solutions. This principle proves dangerous because scenarios are intellectual constructs, based on hypotheses or, at best, probabilities that never fully correspond to the reality of events and facts.

Members of the crisis management team are subjected to significant stress. This stress impairs their reasoning abilities. As a result, they will tend to manage the crisis as if it fit entirely within the pre-established scenario, and to mechanically duplicate the actions prescribed in the BCP. This causes major errors, because the reality of the crisis is never fully in line with the scenario.

This BCP approach based on precise but (by design) inadequate scenarios quickly reaches its limits. Another, more modular approach allows for easier and faster adaptation to the reality of the facts.

**EXAMPLE**

### Consider the example of a major Seine river flood.

Defining a precise scenario for this *"foretold catastrophe"* is difficult. The narratives conveyed regarding the potential severity of such an event vary depending on the stakeholders' interests. Some actors emphasize that the fact that improvements and works have been carried out to slow down the water rise times and to crest the flood (water retention basins upstream of Paris), while others emphasize that today's Paris is no longer the Paris of 1910 and that the development of urbanization and the paving of an increasing number of surfaces have the direct consequence of reducing water concentration times at the watershed scale. So it is difficult to objectively grasp the severity of such a phenomenon.

**Paris and the Île-de-France region: a map of flood-prone areas**

1910 flood zone — flood zone in the basements


Credits: ©2025 idé - Le Parisien

EXAMPLE

**Let's take the example of the French government's national *"Influenza Pandemic"* prevention and control plan (2006) to address health crisis issues.**

This plan was structured based on hypotheses derived from clinical and epidemiological studies by the World Health Organization and the French Institute for Public Health Surveillance (InVS). The dynamics of the pandemic were theoretically supposed to be as follows:

- a development of the pandemic in successive waves, each wave potentially lasting 8 to 12 weeks;
- a clinical attack rate of 15 to 35%;
- a mortality rate of 1 to 2%.

- As for the magnitude of these two waves, two hypotheses were present:
  - either two identical waves (50% each);
  - or 1/3 of the affected people distributed over the first wave and 2/3 over the second [3].

This approach reflected a conceptualization of crisis dynamics, a logic of gradation of human-to-human transmission, and the geographical spread of the disease, rated from 1 *"no virus circulation"* to 6 *"influenza pandemic"*; phase 7 being that of *"return to normal."*

However, the scenario did not unfold that way. In reality, the alarmist warning signs suggesting an exponential development of the crisis gave way to a long phase of stabilization that no longer corresponded to the probabilistic logic defined by the models. The State therefore built a chronological progression of the scenario that did not prove to be in line with the reality of the crisis dynamics.

The clinical attack rate of the scenario, estimated between 15% and 35%, is based on the *"Law of Large Numbers"*, which applies only very imperfectly at a small scale (a few people or tens of people). In reality, it is quite possible that one team of employees could be decimated by the flu and unable to work, while another will not be affected. By respecting this statistical logic of homogeneous distribution of the viral attack, one cannot solve the problem of business continuity at the team level. Indeed, the logic of contamination here responds to a logic of physical proximity and not of statistical distribution.

**BCPs structured according to a scenario often prove to be rigid instruments.**

## Situations and measures

| | |
|---|---|
| Situation 1: | Absence of circulation of new highly pathogenic avian viruses in animals and humans (for reference). |
| Situation 2A: | Epizootic disease abroad caused by a highly pathogenic virus, without human cases (WHO phase 2). |
| Situation 2B: | Epizootic disease in France caused by a highly pathogenic virus, without human cases (WHO phase 2). |
| Situation 3A: | Isolated human cases abroad without human-to-human transmission (WHO phase 3). |
| Situation 3B: | Isolated human cases in France without human-to-human transmission (WHO phase 3). |
| Situation 4A: | Clustered human cases abroad, limited and localized (limited human-to-human transmission due to a virus poorly adapted to humans; WHO phase 4). |
| Situation 4B: | Clustered human cases in France, limited and localized (limited human-to-human transmission due to a virus poorly adapted to humans; WHO phase 4). |
| Situation 5A: | Large uncontrolled clusters of cases abroad (WHO phase 5) |
| Situation 5B: | Extension of clustered human cases in France (WHO phase 5). |
| Situation 6: | Influenza pandemic (WHO phase 6): a. Organization and health measures; b. Maintenance of activities. |
| Situation 7: | End of pandemic wave. |

Source: Government prevention and control plan *"Influenza Pandemic"* version 2, 2006.

(3) InVES: French Institute for Public Health Surveillance, *"Estimation of the impact of an influenza pandemic and analysis of strategies"*

# 2.2. PROPOSAL FOR AN APPROACH BASED ON RESOURCE UNAVAILABILITY

The scenario-based approach has shown its limits. Another is needed: the resource unavailability approach.

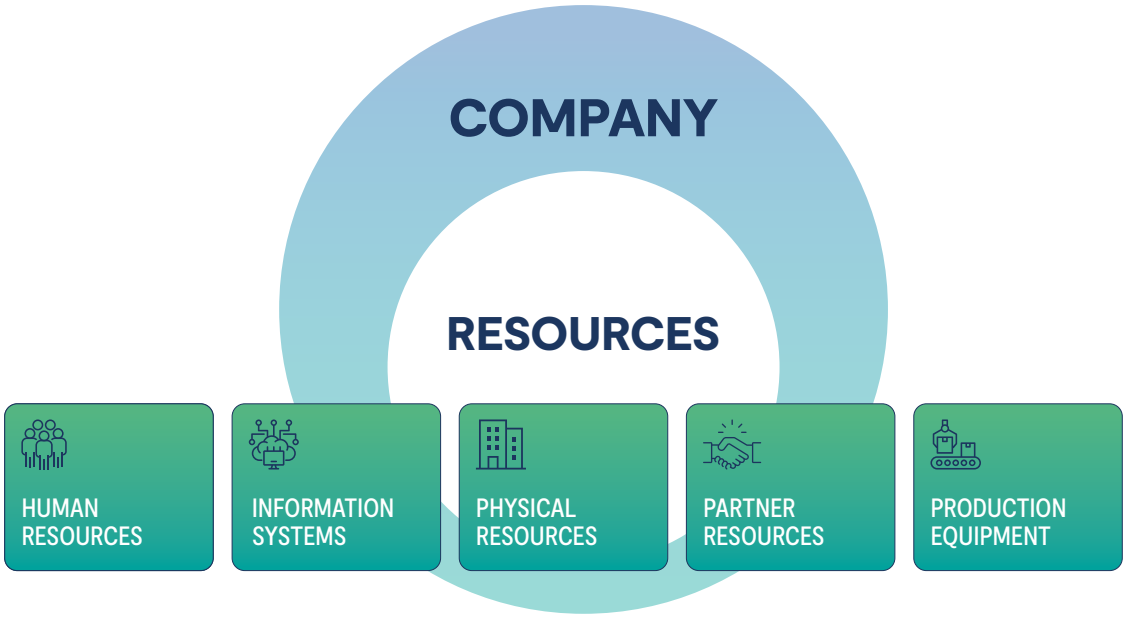
To function correctly, a company uses various resources: tangible assets (premises and production equipment, raw materials, IT infrastructure, etc.) and intangible assets (labor, data, reputation, etc.).

In the event of a malfunction, unavailability, destruction, or disappearance of a particular resource, the overall operation of the company is likely to be impaired. Beyond immediate crisis response, the BCP must reduce the impact and duration of the resource unavailability.

These resources can be broken down into five categories:

*"Resource unavailability"* refers to any undesirable event or situation that exceeds the material and/or organizational response capabilities of one or more company departments. This definition is not exclusive; it can vary depending on the company's risk appetite and the desire to structure continuity responses a priori, in the event of undesirable events occurring.

We replace the pre-established-scenario logic with resource-unavailability logic. The first step in building a BCP is therefore to examine the consequences of the unavailability, destruction, or disappearance of a particular resource within the company, regardless of the causes and origins of the disaster and without consideration of probabilities.



The specificity of crises linked to an extreme climatic event is the simultaneous unavailability of several resources on a large geographical scale. If the environment can be impacted as a *"company resource"*, the geographical perimeter of the company must be secured independently.

**BCP drafting criteria: from 'scenario' logic to 'resource-unavailability' logic**

| | Scenario-based approach | Resource unavailability approach |
|---|---|---|
| **Reasoning basis / logic** | Based on the origin and cause of the threat | Based on the impact and consequences of the resource's unavailability |
| **Principle** | A priori construction based on hypotheses | A posteriori construction based on reality |
| **Approach** | Probabilistic/statistical | Deterministic (resource unavailability) |
| **Deliverables** | Scenario-based and perimeter-based Business Continuity Plan | Combination of thematic & gradual business continuity solutions |

## 2.2.1. Unavailability of Human Resources

HUMAN RESOURCES

The guiding question here is:

"Your building is intact, your information systems are working correctly, but 30% of your staff is absent. What do you do?"

With the rise of health issues (SARS, more recently COVID-19) and social movements (political or social unrest), the scope of the BCP now extends to the issue of the scarcity or temporary disappearance of Human resources.

## 2.2.2. Unavailability of IT resources: the IT Disaster Recovery Plan

INFORMATION SYSTEMS

The guiding question here is:

"Your information systems are no longer working, can you continue to work, even in degraded mode?"

**The purpose of the IT Disaster Recovery Plan (DRP)** is to respond to any technical failure in infrastructure and information systems (server failure, network loss, etc.).

The implementation of an IT Disaster Recovery Plan (DRP) requires advanced IT skills and excellent knowledge of the company's information systems. This is why this project is generally under the responsibility of the company's IT Department (CIO).

The DRP and BCP are distinct — and should stay that way. To clarify how these two plans interact, consider the two most common scenarios:

SCENARIO **#1**

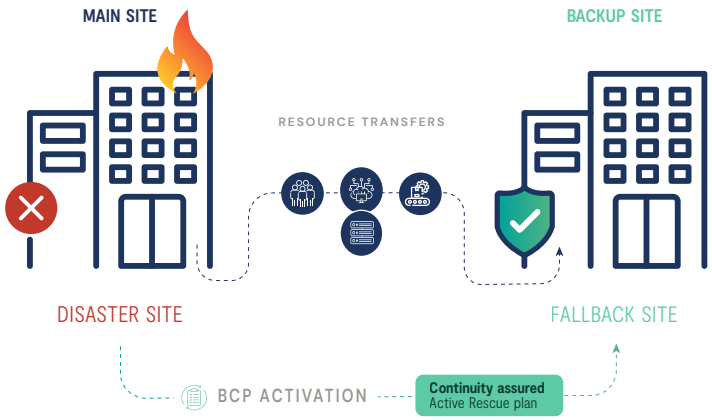
**Simultaneous activation of the 2 plans**

### Case where IT servers are located on the users' premises.

If the premises are destroyed (e.g., fire), the IT servers will also be destroyed. Both the BCP and the DRP must then be triggered.

It will be necessary to relocate the users present in the building but also to *"restore"* the information systems destroyed by the disaster.

**Business continuity solutions:**
Transfer of all resources located in the building



SCENARIO **#2**

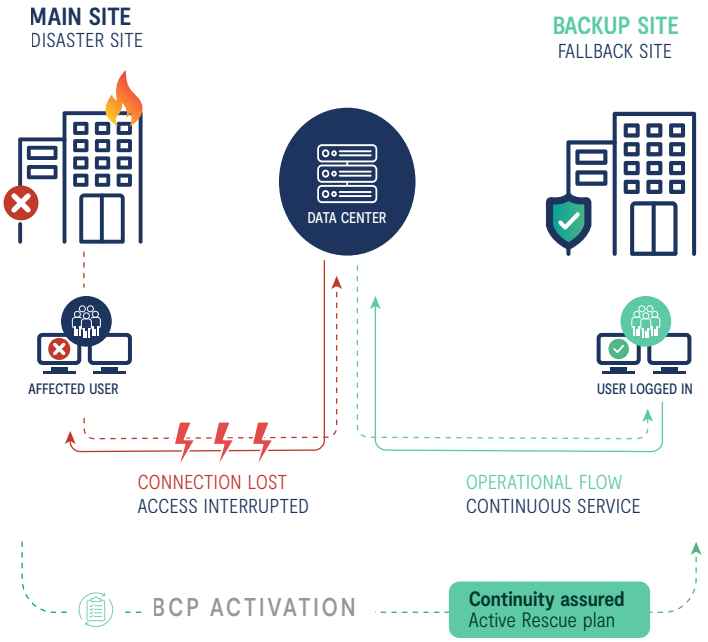
**Independent activation of the 2 plans**

## Case where servers are located in a *"Data center"*, i.e., in a place separate from the building where users are located.

In this scenario, the servers are located in a place reserved for them, the Data Center. So if the users' building is destroyed, IT flows simply reroute to the new location hosting them.

Conversely, if the Data Center in which the IT servers are located is destroyed, the IT Disaster Recovery Plan (DRP) will be triggered but not the Business Continuity Plan (BCP) (since the building in which the users are located will be spared by the disaster).

**Business continuity solutions:**
Transfer of resources constituting the work environment and rerouting of IT flows

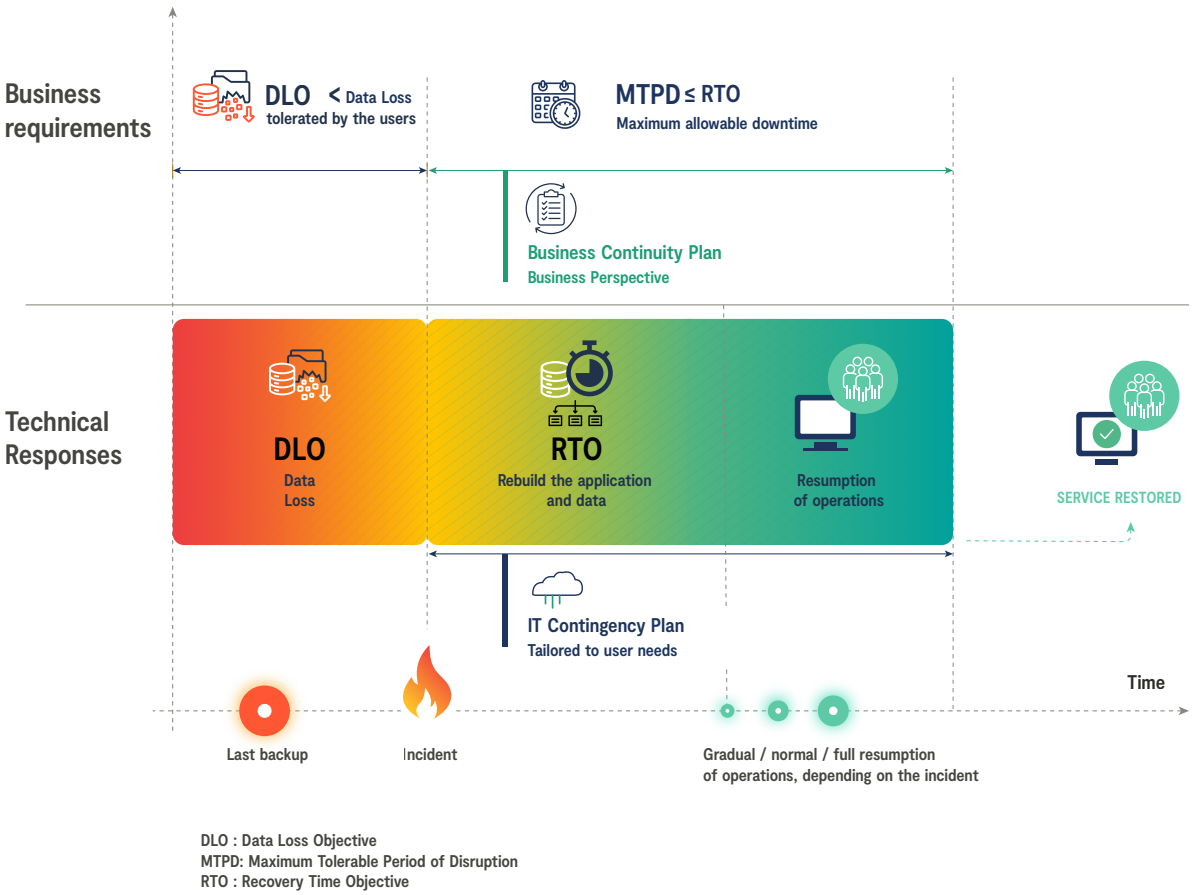



In every case — particularly when servers sit on user premises — the BCP Manager must synchronize.

→ on the issue of the restart times for IT applications requested by users and which appear in the BCP [4] on the one hand, and the technical times for restoring applications and associated data (*"Recovery Time Objective"*) which appear in the DRP on the other hand.

→ on the issue of the frequency of IT data backup (sometimes called DLO for *"Data Loss Objective"* or RPO for *"Recovery Point Objective"*). This indicator designates the maximum duration of IT data recording that it is acceptable for users to lose in the event of a disaster.

(4) Generally called *"Maximum Tolerable Period of Disruption"* (MTPD) of activities: See Chapter *"Impact analysis of process interruption"*




DLO : Data Loss Objective
MTPD: Maximum Tolerable Period of Disruption
RTO : Recovery Time Objective

In other words, if the technical times for restoring applications and their data are shorter than users request, users can operate the applications.

*Conversely*, if the technical/IT times for restoring applications and associated data are longer than those requested by users, the latter will have to work in a *"degraded"* manner, that is to say, in the partial or total absence of the IT tools usually at their disposal.

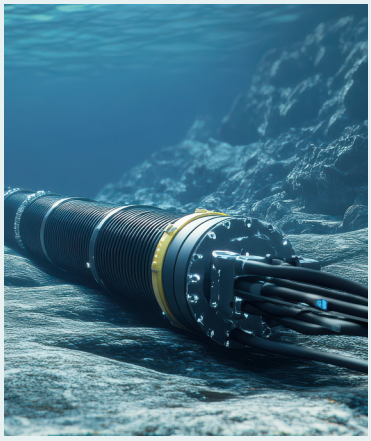
Two types of IT unavailability exist:

- Unavailability of *"management IT"* which causes disruptions in the management of company data on the one hand (suspension of invoicing, accounting-IT processing issues, etc.);
- Unavailability of *"production IT"* — the IT that runs industrial production for manufacturing companies (production-line stoppage).

EXAMPLE

### Example of the *"Ping Timeout"*: the rupture of submarine cables

One of the major disruptions that occurred in the modern telecommunications system dates back to December 2006, when a 7.1 magnitude earthquake on the Richter scale caused the breaking of submarine cables between the island of Taiwan and the Philippines, de facto causing the interruption of telecommunication links between Southeast Asia and the rest of the world. 49 days of work were necessary for the connections, provisionally redirected to other cables, to function again. Similar incidents were observed in 2008 and 2013 (breaking of 3 cables which disrupted internet access in part of the Middle East and Asia).



More often, companies lose their networks for hours or days after routine accidents — for example, cable cuts near buildings during trench-digging.

Though significant, these examples mainly illustrate physical or accidental unavailability — the historical foundation of the IT Disaster Recovery Plan (DRP). But this approach, though necessary, covers only part of a much broader risk spectrum. Chapter 4.1 will explore in detail the new criminal dimension of IT unavailability, where the threat is no longer a passive failure but an active and intelligent adversary, profoundly redefining the requirements of resilience.

## 2.2.3. Unavailability of material resources

PHYSICAL RESOURCES

The guiding question here is:

"Your building was destroyed by a fire last night, it is 8 a.m., employees are arriving... What do you do?"

Historically, it is the disappearance or inaccessibility of buildings that led to the creation of the first BCPs. The first BCPs in France were a consequence of the fire at the Crédit Lyonnais headquarters in 1996, which mobilized 600 firefighters, destroyed two-thirds of the building, and generated more than 1 billion francs in damages.

## 2.2.4. Unavailability of a Partner

PARTNER RESOURCES

The guiding question here is:

"Your strategic supplier is failing... What do you do?"


In the constant pursuit of performance, companies make organizational choices that make them more vulnerable to process interruptions, even minor ones. The specialization of sites by function (implementation of shared service centers for purchasing, accounting processes, etc.), the outsourcing of certain functions, the pooling of resources between several companies, as well as the stronger interdependence of sites with each other are aggravating factors in the event of a stoppage of production processes. So supply-chain issues — logistical dependencies and reliance on key suppliers — must be built into BCPs (Business Continuity Plans).

Beyond these physical and logistical disruptions, the interdependence with partners and the *supply chain* has become a primary cyberattack surface. A partner can not only be the target of an attack having indirect consequences on the company, but also serve as an attack vector to reach it. Chapter 4.1 explores this critical link between partner unavailability and cyber-crime risk in depth.

EXAMPLE

### Example of the *supply chain* disruption following the floods in Thailand

The 2011 floods in Thailand were one of the costliest natural disasters in recent years: 40 to 50 billion dollars in economic losses. Indeed, they caused disruptions to numerous logistics and supply chains. Thus, nearly 11,000 factories were flooded, leading to the temporary layoff of half a million workers. The main consequence was a massive shortage of electronic components on a global scale. It affected major computer manufacturers and automakers (notably Toyota and Honda) which, following the disruption of their supply chain, suffered significant production declines.

## 2.2.5. Unavailability of production equipment (machine in the production line)

**PRODUCTION EQUIPMENT**

For companies in the industrial sector, the business continuity analysis must in particular focus on the consequences of the unavailability or destruction of certain production equipment (machines, test benches, automated lines, specific equipment). In this respect, it is essential to identify critical equipment, evaluate the possibilities for replacement or repair, as well as options for relocating production, pooling, or resorting to alternative production methods.

From this perspective, the BCP is also a key input for the property damage insurer, who can assess its robustness up to the scenario of a major or even total loss, such as the complete destruction of buildings and equipment following a fire or a natural event. The company's ability to limit the consequences of such a loss, to maintain minimal activity, or to organize a structured recovery then constitutes a key factor in the evaluation of risk and insurance resilience.

Business continuity is not limited to managing internal-resource unavailability. The BCP must also integrate aggravating factors linked to the company's environment, such as regulatory or administrative constraints, supply chain disruptions, as well as the potential impacts of natural, health, or geopolitical events, likely to durably affect production and operational capacity.

# METHODOLOGY: IMPLEMENTING THE BCP IN 5 PHASES

The purpose of this document is to provide the reader with the keys to understanding and successfully implementing a BCP and maintaining the business continuity system so that the reader can autonomously carry out his/her own business continuity system.

Chapte


FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC

# Our methodology is structured into 5 phases:

- **Phase 1** — Identify the consequences of the unavailability of one or more resources.
- **Phase 2** — Analyze critical processes in terms of continuity and Identify resource needs.
- **Phase 3** — Define business continuity solutions and strategies.
- **Phase 4** — Maintain operational conditions, update business continuity plans, and run tests/ simulations.
- **Phase 5** — Communicate on the BCP project, raising awareness among managers and employees (transverse phase).

Each of these *"phases"* is broken down into *"steps."* Each *"step"* is broken down into *"actions."*

**1 Identify the consequences of the unavailability of one or more resources**

**Describe the resource unavailability and its consequences**
- Identify the geographical scope
- Identify the functional scope
- Identify the time scope

**2 Analyze critical processes in terms of continuity and Identify resource needs**

**Identify processes and operational flow (based on the scope of the study)**
- Identify and inventory processes.
- Identify internal dependencies between processes
- Identify any "sensitive" periods

**Analyze the impact of process interruption**
- Establish an impact analysis of process interruption and perform a prioritization based on 2 criteria:
  - Time criterion
  - "Business" criterion

**Indentify resource needs**
- Identify the resources associated with each process:
  - People, Applications, IT Data, Utilities...

**3 Define business continuity solutions and strategies**

**Identify the different possible business continuity strategies and assign an order of magnitude for the associated costs**

**Implement the BCP and operational sub-plans at the level of each department**

**4 Maintain, update and run tests of the BCP**

**Maintain operational readiness**
- Update and test the BCP

**5 Communicate on the BCP project, raising awareness among managers and employees.**

Phase 1

# 3.1. IDENTIFY THE CONSEQUENCES OF THE UNAVAILABILITY OF ONE OR MORE RESOURCES

1

**Identify the consequences of the unavailability of one or more resources**

**Describe the unavailability of the resource(s) and its consequences**

- Identify the geographical scope
- Identify the functional scope
- Identify the time scope

## 3.1.1. Describe the unavailability of the resource(s) and its scopes

As noted earlier, a company relies on several types of resource to function properly: material assets (premises and production equipment, raw materials, IT infrastructure, etc.) and intangible assets (labor, data, reputation, etc.). The malfunction, unavailability, destruction, or disappearance of any given resource (Material, Human, Information Systems, partnership resources, etc.) can disrupt the overall functioning of the company.

The first step in building a BCP is therefore to consider the consequences of the unavailability, destruction, or disappearance of any given resource within the company, regardless of the causes and without considering probability. The impact of resource unavailability on the company's operations is what drives the need for a Business Continuity Plan.

We propose the following definition for events requiring the implementation of a BCP
***"any undesirable event or situation that exceeds the material and/or organizational response capabilities of one or more of the company's departments".***

This definition is not exclusive; it may vary depending on the company's risk appetite and its desire to structure continuity responses in advance, in the event that undesirable events occur.

To describe each type of unavailability and its impact on the company's activities, define its geographic, functional, and temporal scope.

#### 3.1.1.1. Geographical scope

Define the geographic extent of a given resource (or group of resources), i.e., whether the unavailability of the resource is localized to a building, a neighborhood, or a region. In some cases, a strict geographical scope cannot be defined (See above).

#### 3.1.1.2. Functional scope

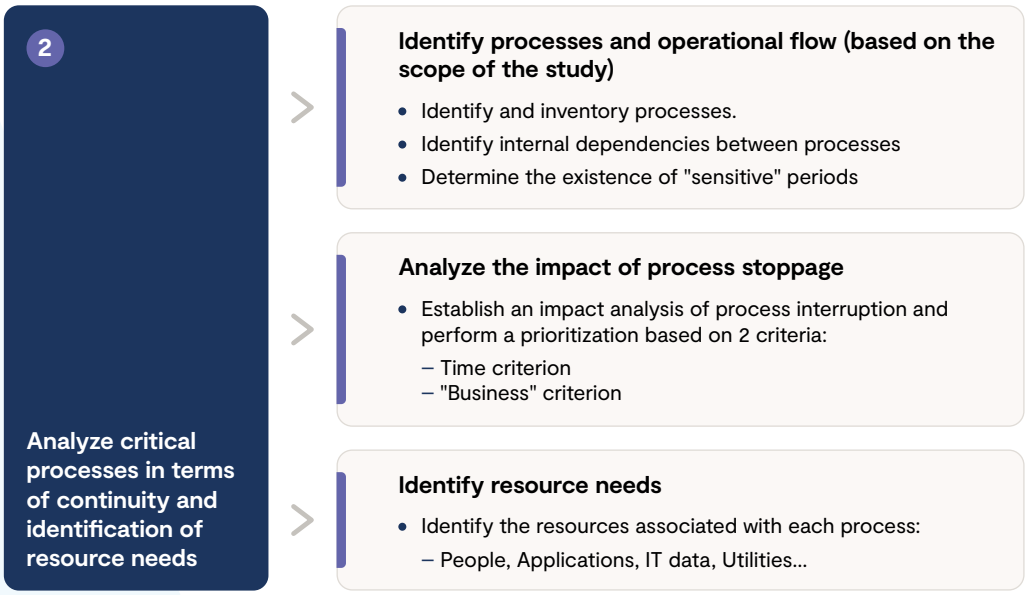
Define the activities that will be impacted by the unavailability of the resource (or group of resources). The unavailability of the resource may uniformly disrupt all of the company's activities or, conversely, only specific activities. In some cases, a strict functional scope cannot be defined.

#### 3.1.1.3. Temporal scope

Define the period during which the company will have to endure the effects of the resource unavailability. In some cases, a strict temporal scope cannot be defined.

Phase 2

## 3.2. ANALYZE CRITICAL PROCESSES IN TERMS OF CONTINUITY AND IDENTIFY RESOURCE NEEDS



The process-analysis phase for continuity has three constituent actions:

- Identify the processes;
- Analyze the impact analysis of activity stoppage;
- Identify the resources.

The objective of continuity is not to *"duplicate"* the organization to allow for identical continuity, but to analyze the impact of stopping each of the Organization's processes and the associated consequences, to observe internal and external interactions, and to proceed with an arbitration made by each business line and validated by General Management [5].

**Analyzing activity criticality for continuity and identifying resource needs is one of the most important phases of BCP implementation.**

The person in charge of collecting said data must plan interviews with each of the Department heads (whether they are Business lines or Support functions) in order to collect the relevant information necessary for implementing a BCP.

Interview and workshop format and duration should reflect two things: the quantity and complexity of the data to be collected, on the one hand, and on the Organization's appetite and maturity regarding risk management issues, on the other. It should be noted that it is necessary to find the best compromise between the reasonable assurance of having collected all relevant data for the BCP and the duration of the interviews or working groups. For example, conducting an interview that is too short creates a risk of forgetting or missing important information, while conducting an interview that is too long will correspondingly reduce the availability time of each Department Head during the operational phase of BCP implementation.

The data-collection methodology must (a) be known and shared across both the BCP project team and every in-scope department, and (b) pay particular attention to how data are collected, deployed, centralized, formalized, and compiled. Continuity strategies will be built on this data.

To collect information effectively, formalize the protocol and centralize discussions and findings in documentary tools.

We propose two documentary tools for each of these three actions (identification of processes and operational flows, analysis of the impact of process stoppage, identification of resource needs):

- An interview protocol, which is essentially an interview *"guide"*, a framework of questions that must be asked;

- An information collection matrix in which the responses collected during the interviews will be formalized.

(5) in *"Managing major crises: Health, ecological, political, and economic"*, L. CROCQ et al. Odile JACOB, 2009.

## 3.2.1. Analysis of the impact of process interruption (or *"Business Impact Analysis"*)

INTERVIEW PROTOCOL IN 5 KEY QUESTIONS

# Analyze the impact of process interruption

1. Describe and identify the activities

   → "What do you do on a daily basis? What are the major actions you perform?"

2. Maximum Tolerable Period of Disruption (MTPD): assessment of the maximum time between activity interruption and its total or partial resumption

   → "How long could this activity be stopped without generating impacts, and why?"

3. Severity beyond MTPD: assessment of the severity of the activity interruption against associated criteria and thresholds

   → "What is the severity of the activity interruption once the MTPD is exceeded?"

4. Describe the internal and external interdependencies that allow said activity to function

   → "Which other Department(s), other Service(s), other Organizational Unit(s), but also which subcontractor(s) do you need to carry out this activity?"

5. Identify the critical periods

   → "Are there one or more critical periods during the year? (e.g., quarterly closing)"

   Note: The MTPD must be evaluated over the most critical period of the process

CYBER FOCUS

The BIA evaluation criteria must be enriched to include the impact of data integrity alteration and the cascading effects on the supply chain (loss of substitutability, critical dependency). The mapping of third-party dependencies (software vendors, managed service providers, cloud providers, APIs) must be formalized within the framework of the BIA.

## Information-collection matrix *"Impact analysis of process interruption"*

→ "What do you do on a daily basis? What are the major actions you perform?"

→ "How long could this activity be stopped without generating impacts, and why?"

→ "What is the severity of the activity interruption once the MTPD is exceeded?"

→ "Which other Department(s), other Service(s), other Organizational Unit(s), but also which subcontractor(s) do you need to carry out this activity?"

→ "Are there one or more critical periods during the year? (e.g., quarterly closing)"

| Description of activities or processes | | MTPD | Impact | | Interdependencies | | Critical period(s) during the year | | | | | | Comments |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| No. | Activities or Processes | Description/ Observations/ | in days | Business | Image | Internal dependencies (between services, etc.) | External dependencies (suppliers, subcontractors) | Check | Monthly | Quarterly | Other | Start date | Duration of the critical period | |
| 1 | | | | | | | | | | | | | | |
| 2 | | | | | | | | | | | | | | |
| 3 | | | | | | | | | | | | | | |
| 4 | | | | | | | | | | | | | | |
| 5 | | | | | | | | | | | | | | |
| 6 | | | | | | | | | | | | | | |
| 7 | | | | | | | | | | | | | | |

### 3.2.1.1. Identify processes and operational flows

1 Describe and identify the activities

→ "What do you do on a daily basis? What are the major actions you perform?"

**Definition of terms used**

The vocabulary used during the process identification and description phase must be defined. Indeed, a profuse terminology (*"activities"*, *"processes"*, and other *"tasks"*) identifies all the operations carried out within an organizational unit. Numerous definitions and as many combinations exist: for example, some professionals consider an *"activity"* to be a set of *"processes"*, while others propose defining a process as a set of elementary activities or tasks.

When implementing a BCP, the project manager and the *"BCP Committee"* must focus on terminology.

In our discussion, we use the terms *"activities"* or *"processes"* interchangeably.

**Level of detail in process identification and description**

Beyond terminology, choose an appropriate level of granularity, i.e., a level of detail for processes that allows for an exhaustive description of the operations present in the organization without this work becoming too time-consuming. On average, each department manages between 5 and 15 processes. A process can be defined as an activity grouping human, material, and informational resources, which transform inputs into outputs. Each *"process"* must be described during the interview.

By way of example and non-exhaustive:

**Therefore, how do you identify the processes?**

**HR processes**

- Payroll;
- Recruitment;
- Training;
- Labor law;
- Expense and advance management;
- Relations with employee representative bodies and the Social and Economic Committee (CSE).

**IT processes**

- Development and design;
- Production;
- Help desk.

**Treasury processes**

- Centralization and optimization of investments;
- Banking relationships;
- Regulatory compliance and accounting of financial flows.

**Accounting processes**

- Account monitoring;
- Receipt/issuance of invoices;
- Receiving supplier invoices, having them validated for payment, accounting for them, and obtaining payment from the Treasury Department;
- Preparing financial statements;
- Preparing tax returns and ensuring payment of corresponding taxes.

→ **If the organization already has a process map or list**

It is possible that the organization already possesses a map (or list) of its processes. This may be through an ISO 9000 type certification, the performance of an organizational audit, or the existence of a risk map established through the lens of processes (approaches generally used by Permanent Control or Internal Control departments).

→ **If the organization does not have a process map or list**

Ask each manager for the list of processes in their department. The first question to ask is...
***"What do you do on a daily basis? What are the major actions you perform?"***

### 3.2.1.2. Impact analysis of process interruption

2. Maximum Tolerable Period of Disruption (MTPD): Evaluation of the maximum amount of time that can elapse between the interruption of the activity and the total or partial resumption of said activity

→ "How long could this activity be stopped without generating impacts, and why?"

3. Severity after MTPD: evaluation of the severity of the activity interruption based on associated criteria and thresholds

→ "What is the severity of the activity interruption once the MTPD is exceeded?"

This step identifies the business-continuity sensitivity of the processes listed in the previous step and prioritizes them.

Two main criteria drive the impact analysis of process interruption:

**A / A temporal criterion, the MTPD:** evaluation of the *"Maximum Tolerable Period of Disruption"* (MTPD) of the activities.

The *"Maximum Tolerable Period of Disruption"* (MTPD)[6] of an activity is the period during which its interruption has no impact, no negative consequence on the completion of all operations that allow for transforming an *"input"* into an *"output"*.

This MTPD can be defined in minutes (in the case of trading rooms), in hours, or in days, depending on the organization's sector of activity. The MTPD is generally expressed in calendar day(s).

**B / An impact criterion, *measurement of the impacts consecutive to the interruption of a process* after MTPD** in financial, human, or reputation terms.

In order to easily quantify the impacts of process interruption, it is advisable to create a severity scale, which takes the form of a two-way table, in which the impact criteria/indicators appear on the x-axis and the impact levels (generally from 1 to 4) on the y-axis.

(6) Sometimes also called the *"Maximum Tolerable Period of Disruption"*

## Severity scale

| Severity scale | | | |
|---|---|---|---|
| **Thresholds** | **Financial severity** | **Reputational severity** | **Human Severity** |
| **High** | > Over €100 million | > International media coverage, in the general and specialist press, across all media<br>> Long-term press campaign, with medium/long-term monitoring of the event<br>> Significant loss of credibility for the company among shareholders, customers, financial partners, subcontractors, staff and the public,<br>> Significant decline in the quality of the offering, visible to customers<br>> Lasting impact on customer confidence<br>> Impact on credit ratings,<br>> Partial or temporary loss of authorization to operate | > Fatality |
| **Intermediate** | > Between €10 million and €100 million | > National media coverage, in the general and specialist press, across all media<br>> Press campaign, limited toa few days at most<br>> Decline in the quality of the offering, visible to customers<br>> Lasting impact on customer confidence<br>> Missed opportunities for contracts (high-stakes deals) in overseas operations, particularly due to coverage in the specialist press | > Serious injury or trauma requiring the establishment of a psychological support unit |
| **Low** | > Between €1 million and €10 million | > No media coverage or very limited coverage, possibly restricted to specialist media<br>> Significant but temporary decline in the quality of services, with no lasting impact on reputation<br>> Missedcontract opportunities (minor stakes) in overseas operations, due in particular to media coverage in the specialist press | > Minor injury |
| **Very low** | > Less than €1 million | > No media coverage | > No impact |

From a methodological point of view, let us note in this example that:

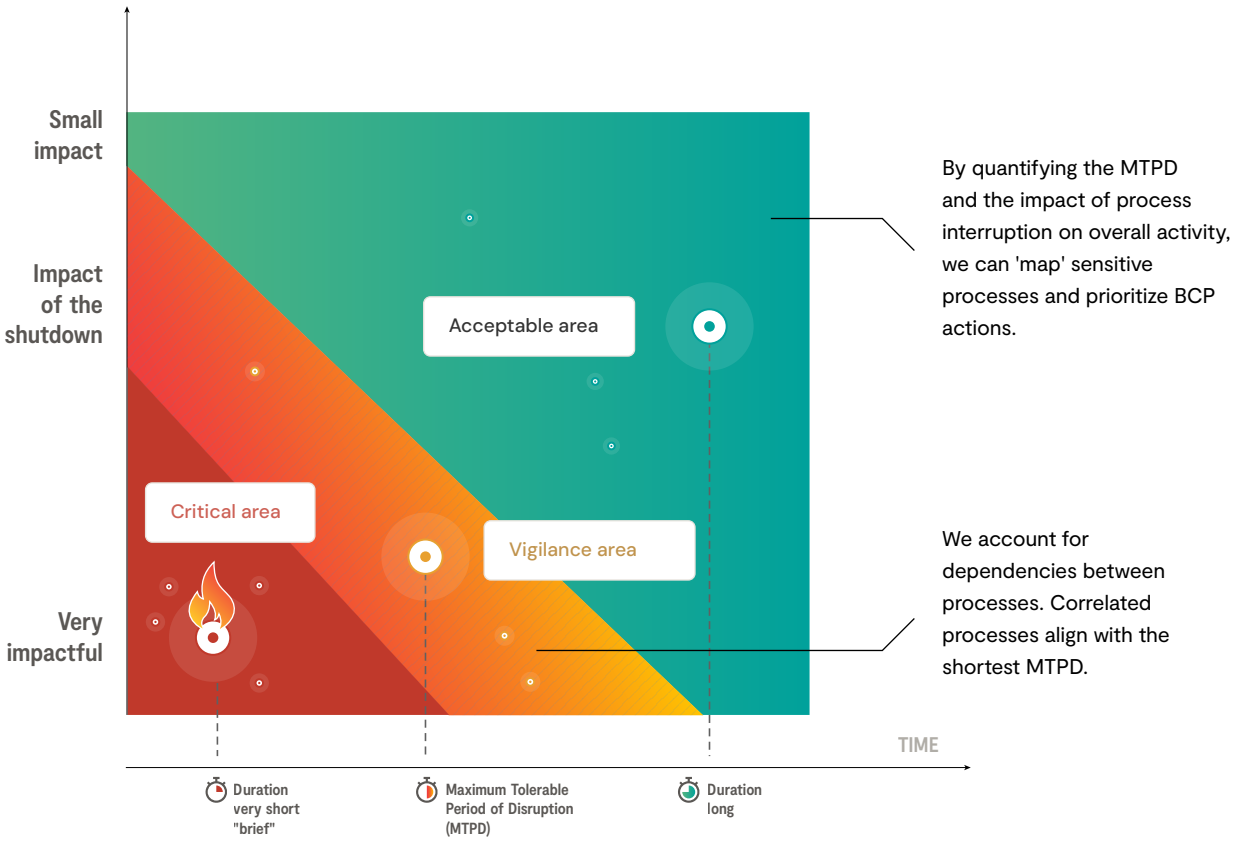
- The measurement of the impact of process interruption is carried out with the assumption that the process cannot be restarted for a full month from the date of the interruption;
- The multiplication of impact criteria/indicators leads to a complexification of the matrix. In this regard, it may be appropriate to limit oneself to the *"financial"* and *"reputation"* criteria, as other criteria such as *"legal"*... can be quantified financially;
- The thresholds for moving between impact levels (generally from 1 to 4) must be put into perspective with the organization's financial results as well as its cash-flow capabilities. In this regard, this scale must be worked on and customized according to the company's financial size.

Remember: the purpose of this step is not fine-grained quantification but prioritization — from most critical to least critical.

After this analysis, build a *"process-criticality map for business continuity"* in which an MTPD scale appears on the x-axis (from the shortest MTPDs to the longest MTPDs) and Impacts on the y-axis (from the strongest impacts to the weakest impacts).

This graphical representation constitutes an ideal communication tool to raise awareness among an Executive Committee (ExCOM) about business continuity issues and to put into perspective the costs generated by the implementation of a business continuity strategy.

## PROCESS MAPPING — MTPD & IMPACT OF INTERRUPTION



### 3.2.1.3. Identify the Interdependencies between processes

4 Description of internal and external interdependencies

→ "Which other Department(s), other Service(s), other Organizational Unit(s), but also which subcontractor(s) do you need to carry out this activity?"

A process in one department may depend on another in the production chain. The MTPD of one must then be coordinated with the MTPD of the other. It is necessary to identify the interdependencies to determine the most appropriate MTPD.

**EXAMPLE**

**For example: the BCP manager interviews the Sales Director**, who states that all the processes they own can be interrupted for three days (MTPD of 3 days). They also state that one of their processes is dependent on validation from the Legal Department. A few days later, the BCP manager interviews the Legal Director, who announces that the shortest MTPD for their department is 10 days.

A data reconciliation exercise should reveal the timing mismatch between the Sales Director's MTPD (3 days, dependent on Legal) and the Legal Department's MTPD (10 days).

Based on this finding, the Sales Director and Legal Director must agree on one of three options:

→ Extend the MTPD of process 3 of the sales department.
→ Shorten the MTPD of the Legal department (10 days → 3 days).
→ Jointly decide that in the event of activation, sales proposals will no longer be reviewed by the Legal Department and will be sent directly to clients. In this case, this decision must be endorsed during a *"BCP Committee"* session.

So verify that 'interdependencies' have been properly identified at two levels:

**1. INTERNAL INTERDEPENDENCIES**

- **Intra-Department level:**
  There is an *"interdependency"* when the successful completion of a *"critical"* activity requires the maintenance of operational conditions for another activity within the same Department (or Unit).

- **Inter-Department level:**
  There is an *"interdependency"* when the successful completion of a *"critical"* activity requires the intervention of another Service or Department of the company.

**2. EXTERNAL INTERDEPENDENCIES**

It is necessary to identify the company's main suppliers, subcontractors, and service providers. Example: the Post Office and/or Courier Companies that deliver mail, the telephone access provider(s)...

### 3.2.1.4. Identify critical periods during the year

5 Identification of critical periods

→ "Are there one or more critical periods during the year? (e.g., quarterly closing)"

Note: The MTPD must be evaluated over the most critical period of the process

Whether it is a quarterly closing for Accounting or a peak production or sales period for a business function (a fire at a toy factory has a different impact in November than in February), identify the frequency, start date, and duration of each critical period.

## 3.2.2. Collection of user needs in terms of Human and Physical Resources

INTERVIEW PROTOCOL IN 2 KEY QUESTIONS

# User needs in terms of Human and Physical Resources

### 3.2.2.1. Collection of Human Resources Requirements

1. Identification of Human Resources needs (skills and volume): day-by-day identification of Human needs and implementation of an HR recovery schedule

→ "Who do you need and after how long?"

The *"Identification of Human Resource needs in terms of business continuity"* matrix allows for the identification for each process of:

- → People who possess unique skills or delegations of authority.
- → The number of people necessary for the resumption of activity, day by day.

### 3.2.2.2. Collection of Physical Resources Requirements

2. Identification of material needs: day-by-day identification of material needs

→ "Who do you need and after how long?"

We cannot establish here an exhaustive list of all the material resources necessary for the resumption of activity. Indeed, depending on the activity, the required resources will vary (IT in the service sector, machine tools for an industrial assembly line...).

As such, we do not represent a matrix here.

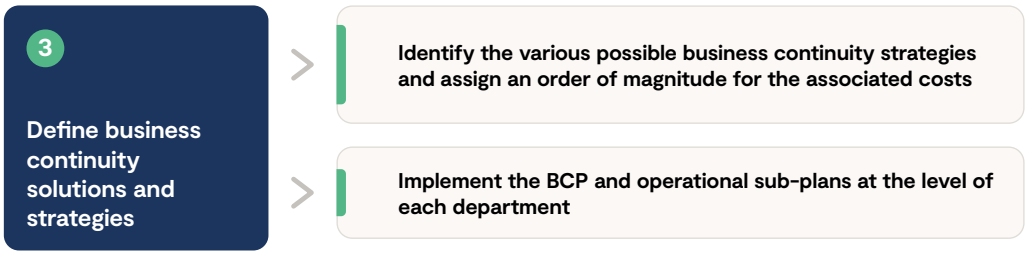
## Information collection matrix *"Identification of Human Resource needs in terms of business continuity"*

| Total number of people involved in carrying out the processes listed below (in "full-time equivalents") | |
|---|---|

| | Description of activities or processes | | MTPD | Impact | | Human Resources | Human Resources Planning for Business Continuity *(value in "full-time equivalents")* | | | | | | | | | Comment |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| No. | Activities or Processes | Description/ Comments/ | (in days) | Business | Image | Sole Responsibility or Delegation of Authority | ASAP | 12 hours | 24 hours or 1 day | 2 days | 3 days | 5 days | 10 days | 15 days | 20 days | 30 days | |
| 1 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 2 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 3 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 4 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 5 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 6 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 7 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 8 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 9 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 10 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 11 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 12 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 13 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 14 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 15 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 16 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 17 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 18 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 19 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| 20 | | | 0 | 0 | 0 | | | | | | | | | | | | |
| | | | | | | TOTAL | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| | | | | | | Staff reserve | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |

Phase 3

# 3.3. DEFINE BUSINESS CONTINUITY SOLUTIONS AND STRATEGIES




## 3.3.1. Defining solutions

With the analysis phase complete and each department's critical processes and continuity needs identified, research the available continuity strategies and estimate the order-of-magnitude cost of each.

This means a comprehensive search: calls for tender to service providers (fallback sites), quotes for equipment purchases (backup servers), and so on. The results of this research are generally documented in a file that identifies the various possible responses in technical, material, and organizational terms. It presents and explains the strengths and weaknesses of each of the different strategies. As a result, some of them may be abandoned (for cost reasons in particular) and others may be explored further.

This document then supports the final validation of the continuity strategy and the development of continuity solutions.

The diagrams [7] below present the main continuity strategies for each BCP issue.

(7) The diagrams were created by Chloé Sibilat and Francesca Serio, students of the *"Global Risk and Crisis Management"* master's program at Paris 1 Sorbonne.

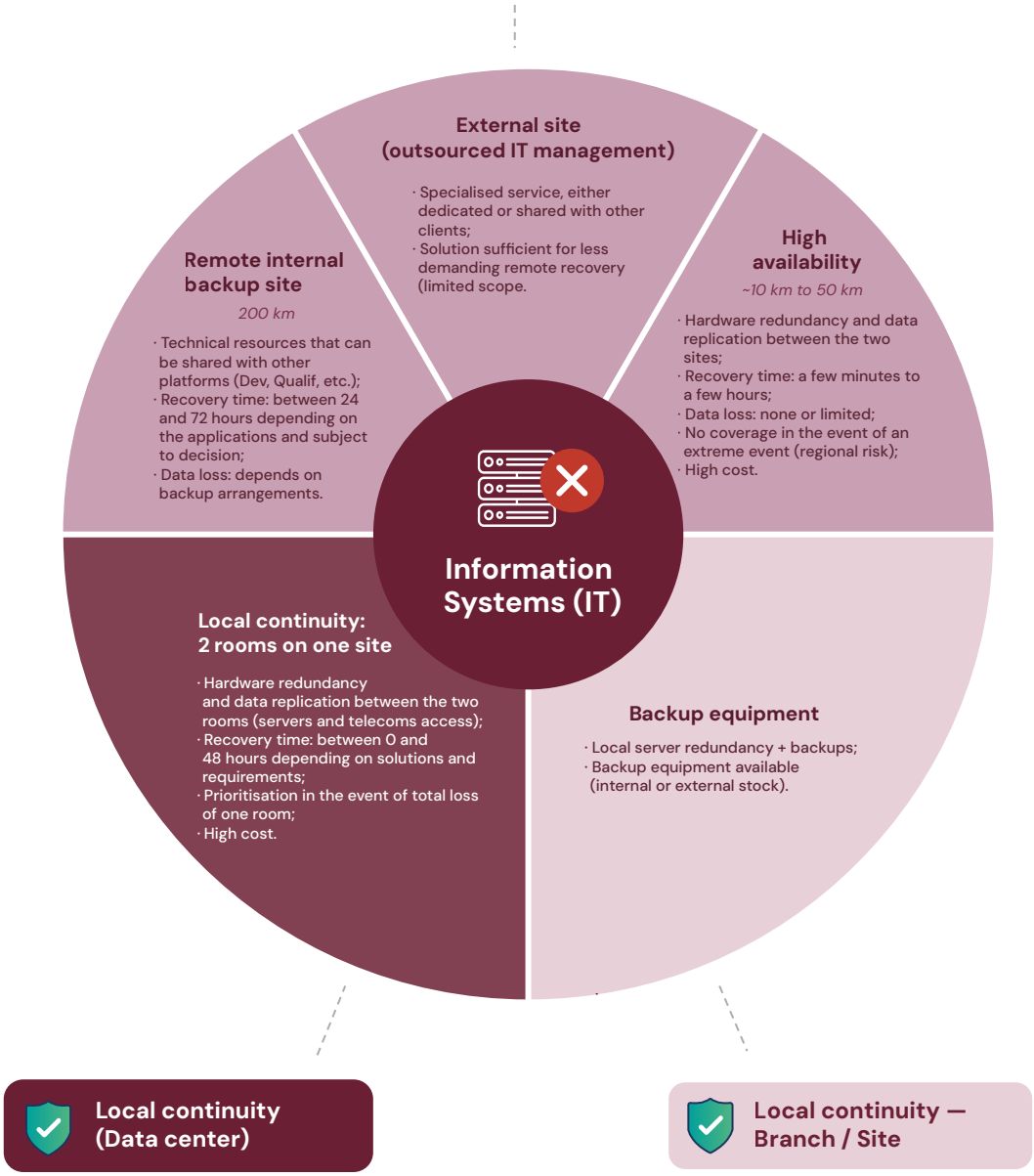
## Issues of premises unavailability


* A climate hazard of regional scale can simultaneously make the main site and the fallback site unavailable, either through direct exposure or through the unavailability of infrastructure and access.

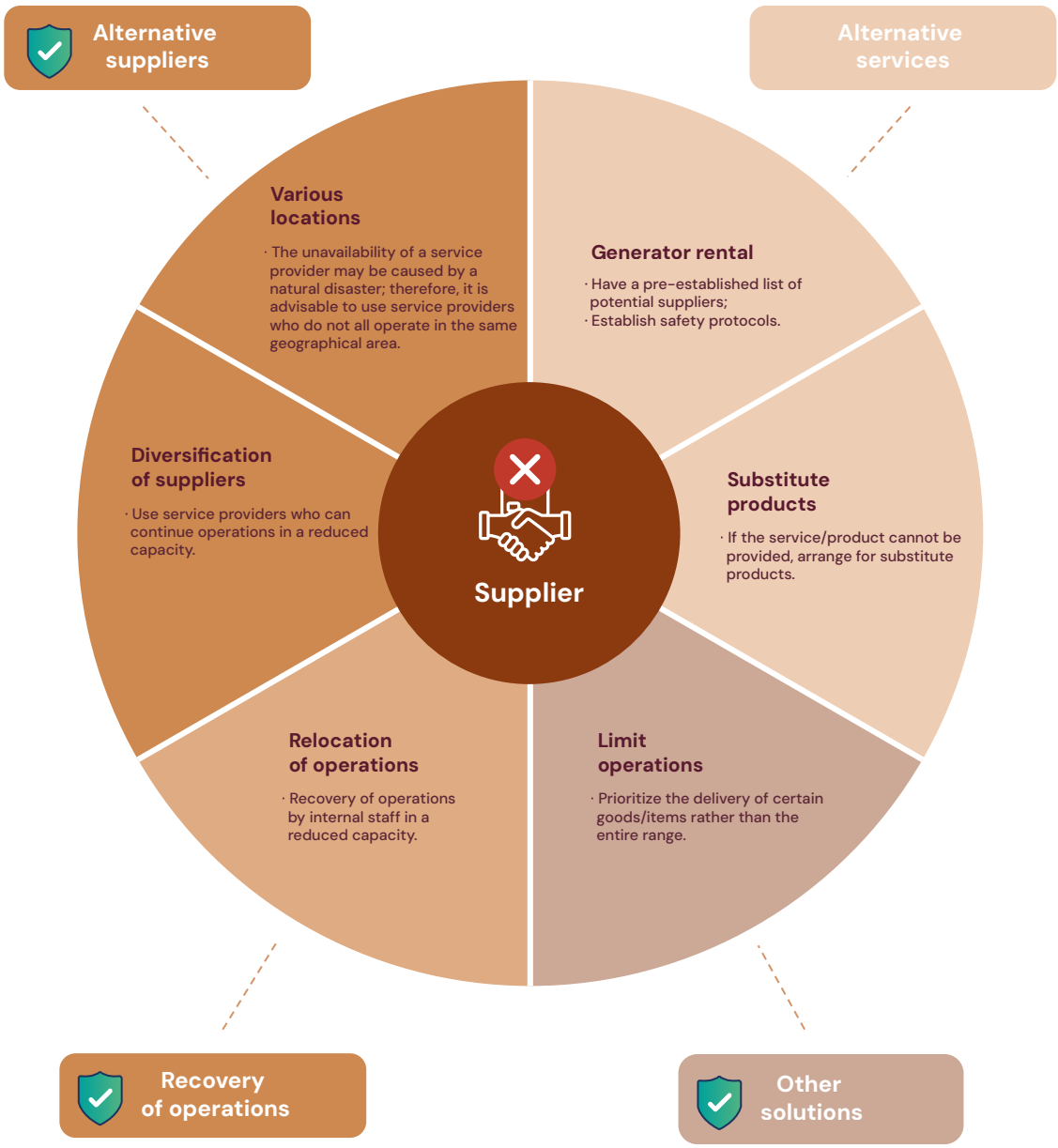
## Human Resources unavailability issues


*In the scenario of a climate hazard, human resources can be simultaneously impacted by the same hazard, due to travel difficulties, personal constraints, or the unavailability of infrastructure at their place of residence.

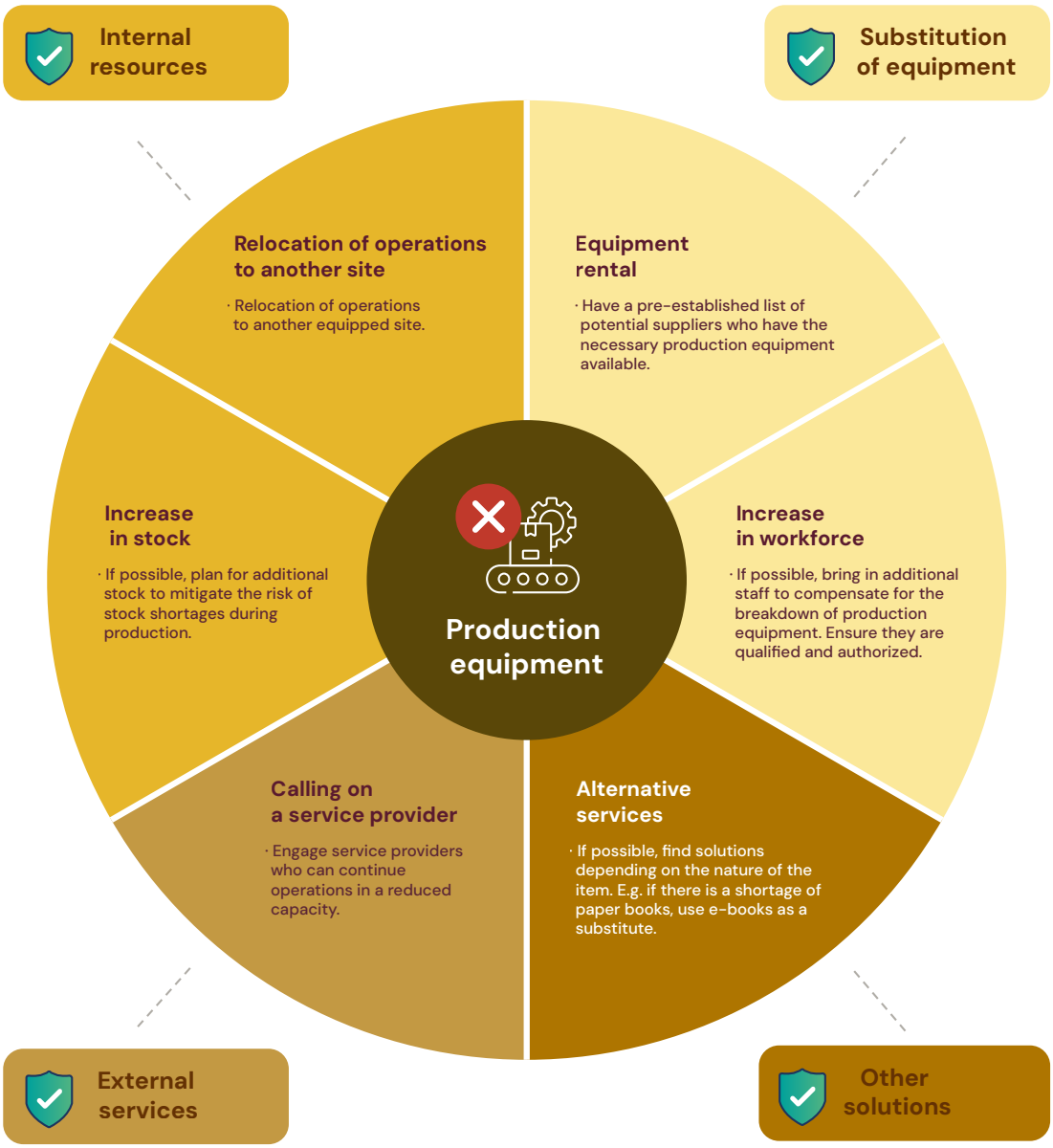
## Information Systems unavailability issues



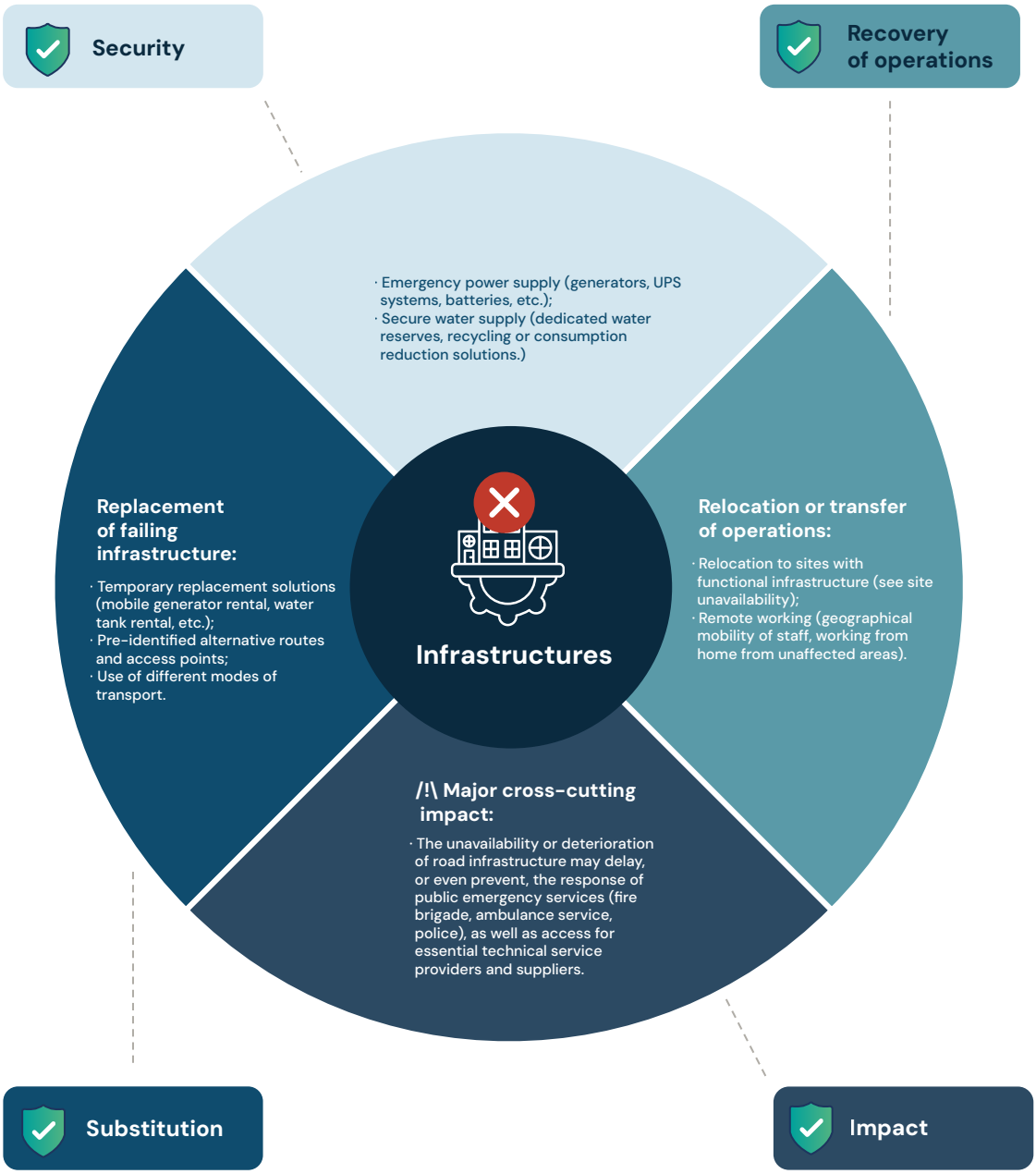
## Supplier(s) unavailability issues



## Production equipment unavailability issues



## Infrastructure unavailability issues



## 3.3.2. Implementation of the BCP

### 3.3.2.1. The implementation of the *"Business Continuity Plan"*

The Business Continuity Plan takes the form of a set of formalized and regularly updated documents, **planning the actions to be implemented following the occurrence of a catastrophe or a serious disaster. It sets the material, technical, and organizational modalities for operating in *"degraded"* mode for the company's activity and for the gradual resumption of activities, from the most sensitive to the least sensitive.**

In this capacity, the Business Continuity Plan therefore proposes an alternative organization that the company applies while remedying the disruptive event at the origin of the process stoppage and facilitates **the gradual resumption of the company's critical processes** (from the most sensitive to the least sensitive) and the mobilization of associated resources with regard to the Maximum Tolerable Period of Disruption (MTPD) and the severity of the process stoppage.

It takes the form of an overall diagram presenting the material, technical, and organizational modalities allowing the resumption of activity[8] as well as all the business continuity provisions common to all departments, such as procedures for activating fallback sites; *"mail rerouting plans" and "telephone rerouting plans"* must appear in this document. This set is supplemented by summary documents and operational charts: Gantt chart, human resource needs planning in the form of an Excel table...

This set of documents allows for acquiring **a global and optimal view of the operational steering of the BCP** in the event of the mechanism being triggered.

### 3.3.2.2. Breakdown of operational solutions for each department

The *"Business Continuity Plan"* document is a summary to be completed by operational business continuity sheets at the level of each department (one sheet per department). These sheets must be simple, clear, incorporating charts if necessary, and adopt a unique formalism common to all departments.

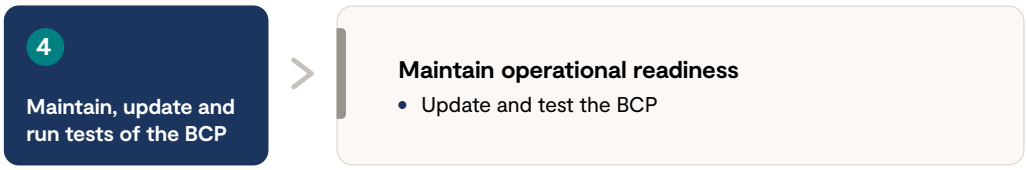
From a methodological point of view, the BCP manager will take care to pre-fill all the sheets with the information collected during the previous analysis phases and to prioritize the processes in order of restart, from the shortest to the longest RTOs (Recovery Time Objectives). A simple *"Excel Macro"* type application will allow for the automation of the compilation and concatenation of data from the different sheets.
Also, schedule an interview with each department head to describe how they plan to restart each process. They should include the list of actions that will enable each restart.

In this respect, it is necessary to raise awareness among department heads (or BCP correspondents) about their responsibilities in implementing business continuity solutions and to remind them of the imperative need to document their own business continuity policy, in coherence with the group-wide level. Well-understood, properly-implemented continuity documentation at department level is the foundation of effective operational steering during recovery.

(8) Let us also note that some BCPs split the resumption of activity into 3 stages and, in this respect, include emergency provisions (reflex action sheet), activity resumption (resumption of activity at a fallback site, for example), and return to normal (return to the nominal site after the period of activity resumption at the fallback site).

Phase 4

# 3.4. MAINTAIN OPERATIONAL CONDITIONS, UPDATE BUSINESS CONTINUITY PLANS, AND RUN TESTS/SIMULATIONS




## 3.4.1. Updating BCPs

The BCP must be kept in operational condition and updated regularly so it is effective the moment a crisis occurs. BCP updates must reflect the company's technical, functional, and organizational changes — and evolving regulatory constraints and technology choices.

**Updating the BCP consists of verifying the adequacy of existing solutions with continuity requirements.**

## 3.4.2. Test / Simulations

Like crisis management, good procedures are tested through simulation exercises. These exercises allow for testing the quality of the documentation, the functioning of technical equipment, but also the knowledge and mastery of the people who use them.

Simulations allow BCP managers to assess employee knowledge, skills, and behavior, and to make any adjustments needed. Regular exercises also remind stakeholders that a crisis can happen — and that they must be ready.

Test the crisis management plan on one side and the BCP on the other, but also test the coordination of the implementation of both.

EXAMPLE

**Example of a crisis exercise scenario that allows for testing the BCP:** a sudden flood prevents access to building A. The crisis cell is mobilized in a so-called *"secondary"* crisis room outside the building and decides to trigger the BCP. From then on, the employees who must go to the fallback room (or *"back-up room"*) comply and present themselves there according to the order and operational procedures described in the BCP document. One or more dedicated member(s) of the crisis cell supervise the logistical dimension and welcome the employees. They actually start working in the fallback room, if necessary in *"degraded"* mode, and thus test the "*proper* functioning" of the BCP. For their part, the members of the crisis cell control the situation and ensure the restart of activity while also responding to requests from journalists and company stakeholders.

Phase 5

# 3.5. COMMUNICATE ON THE BCP PROJECT, RAISING AWARENESS AMONG MANAGERS AND EMPLOYEES

5

**Communicate on the BCP Project**
- **Awareness-raising for Executives and Employees**

Central to the organization, the BCP project manager needs strong communication skills. The cross-functional dimension of their mission leads them to meet with employees at all hierarchical levels: from support functions to production units.

## 3.5.1. The *KISS principle*

It is therefore absolutely necessary to implement, in parallel with the technical progress of the project, communication, awareness, and training actions in order to equip the company with a culture of business continuity. This communication can take various forms: films, quizzes, pastiches of TV game shows (*"Money Drop"*), etc.

The principle here is KISS:
***"Keep It Simple and Straightforward"***

# CYBER-ATTACKS: THE NEW CHALLENGES OF THE BCP

Chapte


r4

# 4.1. IT RESOURCES: FROM ACCIDENTAL TO CRIMINAL

## 4.1.1. Cyber-Attack, what are we talking about?

A cyberattack can take several forms:

| | |
|---|---|
| **External website defacement** | → This threat, less frequent nowadays, mainly has a reputational impact. |
| **DDoS (unavailability of institutional sites)** | → Identically, this is mainly an reputational risk with little operational impact. |
| **DDoS (unavailability of business sites)** | → This type of attack is rather rare but had a strong impact at the end of 2025 with the attack on the La Poste group, which disrupted parcel distribution and made access to the Banque Postale account management application unavailable for customers. This type of attack affects a company's digital storefront but does not call into question the integrity of its internal IT. |
| ***"CEO" fraud attacks*** | → A CEO fraud attack consists of usurping the identity or authority of an executive in order to deceive employees and misappropriate a company's funds. With the new risks linked to AI, this fraud now relies on voice or video deepfakes and hyper-personalized messages generated automatically, making the manipulation more credible and difficult to detect. This is a social-engineering type attack (and not really Cyber). |
| **Reputation attacks (fake cyberattack)** | → A reputation attack consists of inventing a fake cyberattack aims to make people believe that the company has suffered a serious security breach, in order to sow doubt about its reliability. By spreading false information or fake technical reports, the perpetrators seek to damage the brand image and cause a loss of trust from customers and partners. |
| **The *"loss"* of personal data** | → Attacks aimed at stealing customers' personal data consist of infiltrating a company's systems to extract sensitive information such as identities, addresses, or banking data. Cybercriminals then use this data for fraud, identity theft, or to resell it on illegal markets, causing significant damage to customers as well as to the company's reputation. |

| | |
|---|---|
| **Access to confidential data by third parties** | → This type of attack consists of penetrating systems to recover strategic information such as plans, patents, internal processes, or R&D data. This sensitive data is then exploited to gain a competitive advantage, weaken the company, or sold to malicious actors or competitors. |
| **Intrusion and destruction of the internal IT system (Ransomware, Wiper...)** | → A ransomware-type attack encrypts the company's data and blocks access to its systems, then demands a ransom to restore the situation. A wiper, on the other hand, permanently destroys data instead of encrypting it, causing a major and often irreversible interruption of activity. These types of attacks can be supplemented by theft of company data and the threat of publishing it if no ransom is paid, adding additional pressure and a high risk to reputation. |

This last type of attack is defined by the immediate and major destabilization of an organization's current operations (stoppage of activities, inability to deliver services, heavy financial losses, major loss of integrity, etc.). It is therefore a high-impact event, which cannot be handled by the usual processes and within the framework of the organization's normal operation.

## Rethinking resilience metrics: from RTO to Recovery of Integrity Objective (RIO)

One of the main risks highlighted by this chapter lies in the disconnect between traditional resilience metrics, historically centered on technical recovery times (RTO), and the reality of major crises involving a loss of trust in data. In this type of situation, restoring systems to service is not enough: as long as the integrity and reliability of the data are not established, the organization's real capacity to resume its activities remains limited.

It is therefore essential that risk and resilience managers use these concepts to evolve the dialogue with executive committees and boards of directors. Reporting can no longer be limited to RTO-type indicators, but must integrate a more qualitative reflection around the RIO (Recovery of Integrity Objective), that is to say, the time necessary to restore operational and decision-making trust in the data.

This approach benefits from being based on concrete scenarios that are understandable at the governance level. For example: **what would be the impact for the company of a prolonged unavailability of its ERP, not because of a technical breakdown, but because of the time required to verify, reconcile, and certify the integrity of the data before any effective resumption?**

## 4.1.2. The paradigm shift and the obsolescence of the traditional Disaster Recovery Plan

The IT Disaster Recovery Plan (DRP), as described previously, constitutes the historical foundation of information system resilience. Designed to respond to accidental events (hardware failure, cable breakage, data center fire, etc.), its objective is to restore operational capacity within a defined time (RTO) with acceptable data loss (RPO). This approach remains essential, but it has become fundamentally inadequate for dealing with a new class of threats: the malicious actors.

The DRP prepares the organization to recover from a static and circumscribed event; it is, however, poorly equipped to manage a dynamic and persistent intrusion led by an intelligent and malicious actor. The nature of the risk has changed: it is no longer a passive failure, but an active strategic compromise. Consequently, exclusive reliance on a traditional DRP can create a dangerous sense of false security. A DRP assumes that the data to be restored is intact and that the perimeter of the disaster is known. However, a malicious actor who obtains administrator access to the heart of the information system does not just seek to cause an interruption; they aim to exfiltrate, or even subtly alter, the data. In this context, restoring a recent backup could mean reintroducing an already compromised system.

This situation reveals a critical governance failure. An organization that relies solely on its DRP might estimate its recovery time at 48 hours, whereas the reality, when faced with a compromise of data integrity, may be a production stoppage of one month. This dissonance between perceived resilience, often measured by simplistic RTO metrics, and the reality of recovery constitutes a strategic blind spot for many management teams.

## 4.1.3. Anatomy of a systemic cyber-crisis: a case study

To illustrate this paradigm shift, the incident that occurred in September 2025 at a leading global automotive manufacturer offers an edifying case study. This event was not a simple technical incident, but a *"systemic shock"* that paralyzed all of its global operations and caused measurable repercussions on the national economy.

### FROM THE FAULTY COMPONENT TO THE COMPROMISED CRITICAL SYSTEM

The systemic nature of this crisis depended less on the sophistication of the attack tool than on the criticality of the targeted asset. The attackers did not target a peripheral system, but the *"digital brain"* of the company: its SAP enterprise resource planning (ERP) software, which orchestrates production, finance, and logistics globally. The initial attack vector was not an unknown *"zero-day"* vulnerability, but the exploitation of two publicly documented critical flaws (CVE-2025-31324 and CVE-2025-42999), for which patches had been available for more than four months.

The incident does not stem from technological inevitability, but from a failure in the fundamental processes of *"cyber hygiene"* and vulnerability management. Failing to apply a patch to such a central system, in the face of such a clearly identified threat, is not mere operational negligence; it is a strategic failure.

## THE STRATEGIC SHUTDOWN: A NEW TRIGGER FOR BUSINESS CONTINUITY

The complete and global production shutdown for one month was not the direct result of the attack, such as ransomware encryption. It was a *"deliberate defensive containment measure,"* a strategic decision made by the company's crisis management team. This *"scorched earth"* strategy was deemed essential to achieve two vital objectives: first, to stop the massive exfiltration of data (approximately 350 GB of intellectual property) and, second, to prevent an even greater risk: the attacker pivoting from the IT network to the operational technology (OT) environment. A compromise of the industrial control systems on the assembly lines could have allowed for physical sabotage of production or the creation of serious security incidents.

This reality reverses the traditional logic of BCP. Usually, a BCP is activated by an external event that causes unavailability (fire, flood). Here, the trigger was an internal, proactive decision, made to prevent a worse scenario, but which was only potential at that stage. The BCP must therefore now be designed not only as a catalog of responses to confirmed disasters, but also as an action plan to manage the consequences of a strategic decision by the crisis management team. The BCP is activated by the crisis management team, and no longer just for it.

## THE PRIMACY OF DATA INTEGRITY: THE ADVENT OF THE RECOVERY INTEGRITY OBJECTIVE (RIO)

The reason why recovery required an entire month does not lie in the complexity of rebuilding the servers, but in the much more arduous challenge of *"validating and reconciling data integrity"* within the compromised ERP. Having obtained full administrative control, the attackers could have subtly altered critical records: stock levels, payment orders, product bills of materials. Restarting global production with unreliable data would have been an unacceptable business risk.

This imperative gives rise to a new concept that supersedes traditional metrics: the **Recovery of Integrity Objective (RIO)**. It contrasts with the classic **Recovery Time Objective (RTO)**.

→ The RTO asks the question: **"How quickly can we be operational again?".**

→ The RIO, for its part, asks: **"At what point can we trust our data and processes again?".**

In the case of a systemic compromise, the RIO becomes the dominant metric. Achieving the RIO transforms recovery from an IT task into a large-scale forensic audit, requiring different skills (forensic accounting experts, data analysts) than those of a standard restoration team. Organizations must therefore anticipate this reality by including in their BCP a *"Data Validation Plan"* that identifies in advance the external sources of trust and the necessary expertise.

# 4.2. THE ECOSYSTEM AS A BATTLEFIELD: THE SUPPLY CHAIN DILEMMA

The impact of the cyberattack was not limited to the company's borders. The supply chain played a dual role: that of victim and that of threat vector.

## 4.2.1. The domino effect: the supply chain as a victim

The production shutdown jeopardized approximately 200,000 jobs within the supply chain ecosystem. Many suppliers, whose business depended almost exclusively on the manufacturer, were forced to lay off employees. The situation was aggravated by the taking offline of payment systems, causing an acute liquidity crisis for these partners. The shockwave was so violent that it required unprecedented state intervention: the British government had to grant a £1.5 billion loan guarantee to avoid a wave of cascading bankruptcies. This event demonstrates that a cyberattack against an entity of systemic importance is a threat to national economic security.

## 4.2.2. The Trojan horse: the supply chain as a vector

The supply chain is increasingly recognized as a major threat vector, a trend confirmed by agencies such as ENISA and ANSSI. Two main attack scenarios are emerging:

- **Compromise of a partner** (lateral movement): Attackers target a supplier or service provider, often less well secured, to exploit the access and trust relationships it maintains with its primary target;
- **Compromise of a product or service** (software supply chain attack): This approach consists of injecting malicious code directly into a product, component, or software update provided by a third party.

The hyper-integration of modern supply chains, optimized for maximum efficiency via *"just-in-time"* models, has unintentionally created an equally effective vector for risk contagion. The resilience of the ecosystem therefore requires a paradigm shift: it is no longer just about optimizing each link, but about ensuring the stability of the whole, even at the cost of sacrificing some efficiency for the sake of robustness.

# 4.3. SPECIFICITY OF A RANSOMWARE-TYPE CYBER CRISIS COMPARED TO OTHER CLASSIC UNAVAILABILITY

Compared with other types of crisis, ransomware-type cyber crises have specific characteristics that are important to understand:

→ **The initial diagnosis is often uncertain.**
- The affected systems are inaccessible or partially paralyzed, which prevents immediate identification of the true extent of the intrusion. Furthermore, attackers deliberately mask their tracks, making it difficult to know if data has been exfiltrated, how many machines are compromised, or if other dormant threats are still active.

→ **An attack can continue to spread during the activation of the BCP (Business Continuity Plan).**
- Either because the attacker is still active and will adapt to the containment measures put in place by the company;
- Or because even if a system is healthy, the company may choose to shut it down voluntarily to ensure its integrity while waiting to have a better view of the situation.

→ **A lack of a single location for the incident.**
- Potential spread to other organizations due to the interconnection of the IS (Information Systems) to which the organization's information systems and those of its service providers are linked.

→ **Crisis management tools may be unavailable.**
- Whether for documentation;
- Or means of communication (Email, instant messaging, directory, etc.).

→ **The needs for evidence collection and communication are present with constrained reporting deadlines** to various bodies (Authorities, insurers, etc.). This constraint exists with other types of crises, but what is specific here is the lack of tools and reference materials available to do so (unavailability of usual IT tools).

→ **Recovery times are difficult to estimate.**

→ **The reconstruction of the IS** can be: partial, gradual, and uncertain with possible setbacks and uncertainty about data quality.

→ **A strong dependence on technical experts** (who are rare...).

→ **The compromise may date back several months,** with the need to have the ability to rebuild a healthy system without any guarantee of having usable backups (compromised, deleted, unusable, etc.).

# 4.4. TOWARD AN INTEGRATED CYBER-RESILIENCE FRAMEWORK

The BCP (Business Continuity Plan) and the DRP (Disaster Recovery Plan), as traditionally designed, are necessary but insufficient tools when facing an active and intelligent adversary. The answer does not lie in a single plan, but in breaking down silos and orchestrating three distinct but interdependent functions: Incident Management, Crisis Management, and Business Continuity.

- **Incident Management (technical response)**

  → Carried out by technical teams (SOC, CERT/CSIRT), its role is to detect, analyze, contain, and eradicate the threat at the system level. This is the tactical battle, conducted on a time scale of a few minutes to a few hours.

- **Crisis Management (strategic steering)**

  → Led by the crisis cell (management, legal, communication), it makes high-impact strategic decisions (e.g., *"Should we stop global production?"*) and manages stakeholders. It operates on a time scale of a few hours to a few days.

- **Business Continuity (operational recovery)**

  → Executed by business teams, it implements the BCP solutions to restart critical activities once the crisis cell has stabilized the situation. Its time scale extends from a few days to several weeks.

A systemic cyber-crisis requires a perfect choreography of these three functions, as illustrated in the following table. This table provides a visual map of a complex process, allowing different teams to understand their role and interdependencies at each phase of the crisis, moving from siloed actions to a coordinated response.

| Crisis Phase | Cyber Incident Management (Objectives & Key Actions) | Crisis Management (Objectives & Key Actions) | Business Continuity (Objectives & Key Actions) |
|---|---|---|---|
| 1 Preparation | Prepare detection/ response tools (SIEM, EDR). Develop technical response plans (playbooks). Train the teams. | Establish and train the crisis unit. Prepare communication plans. Identify stakeholders. | Develop and test BCPs/DRPs. Conduct BIAs. Implement backup solutions (sites, data). |
| 2 Detection & Alert | Detect the anomaly. Qualify the alert. Trigger the alert to the crisis unit. | Activate the crisis unit. Assess the initial business impact. Trigger internal communication. | Put continuity teams on pre-alert. Verify the availability of backup resources. |
| 3 Containment & Investigation | Isolate compromised systems. Analyze the attacker's operating modes. Preserve digital evidence. | Monitor the evolution of the business impact. Make wider-scale containment decisions (e.g., cut internet access). | Assess the impact of the incident on the planned continuity strategies. |
| 4 Strategic Decision | Provide factual technical reports to the crisis unit. | Decide on radical measures (e.g., stopping production). Validate and disseminate external communication. Manage regulators. | Adapt recovery plans based on the crisis unit's decisions. |
| 5 Recovery & Validation | Eradicate the threat. Rebuild systems in a secure manner. Monitor the return to normal. | Manage the overall recovery strategy. Manage communication regarding the recovery. | Trigger the BCP (Business Continuity Plan). Migrate activities to backup solutions. Validate data integrity (RIO) before restarting. |
| 6 Post-Crisis & REX (Feedback/ Lessons Learned) | Analyze root causes. Produce a detailed forensic report. | Conduct a strategic REX. Manage long-term consequences (legal, reputational). | Conduct an operational REX. Update BIAs and BCPs based on lessons learned. |

# 4.5. IMPLEMENTATION RECOMMENDATIONS: UPDATE THE DRP* METHODOLOGY

**The DRP must define** the resources necessary for the operation of the business and for an orderly and structured IT recovery

- Address infrastructure, support services, and applications;
- Test the ability to restore and rebuild AD, technical services, and applications
- Test the availability of non-infected workstations
- Compare restoration and reconstruction times against the priorities set;
- Maintain communication channels outside the IS — and use them regularly, because they will be unusable on the day of the crisis if untested;
- Design integrated exercises — go beyond siloed IT recovery tests. Design and run large-scale simulations that involve the technical incident-response team, the strategic crisis cell, and the business continuity teams simultaneously, using complex scenarios such as an attack on data integrity;
- Integrating *"compromised data" (dirty data)* tests — during exercises, test the teams' ability to detect that a restored backup contains subtly altered data, thus validating their ability to achieve the RIO.

→ **The DRP must guarantee a tested IT recovery, consistent with business priorities and ensuring data integrity.**

*DRP: Disaster Recovery Plan

# 4.6. ADDITIONAL ELEMENTS THE BCP MUST INCLUDE FOR CYBER RISK COVERAGE

- A prioritized **list of infrastructures and applications to rebuild**, taking into account the dependencies (application, data, version, etc.) necessary for reconstruction.
- **Reflex sheets** by business line and by role.
- ***"Red Button"*** procedures, which aim to quickly isolate segments of the IS (by formalizing the operational impacts of these isolations) and *"green button"* procedures to quickly set up the environment for crisis response and continuity.
  - Ideally, these procedures can include automation in their execution.
- A **reconstruction procedure specific to each critical application/infrastructure** (reconstruction from scratch, copying, backup restoration, etc.), taking into account:
  - The **technological specificities** of the solution to be rebuilt;
  - The **means to recover healthy backups** and necessary data, as well as minimal interconnections.
- The **unit testing strategy**.
- The integrated testing strategy (large-scale simulations that simultaneously involve the technical incident response team, the strategic crisis cell, and the business continuity teams).
- A **strategy for employee acculturation and communication of the continuity plan**, particularly regarding the regulatory framework, which specifies the rules in force and best practices to be applied by employees.

FOCUS THIRD-PARTY RISKS

# Management of third-party risk

Controlling supplier risk involves:

**1** **Identification and classification of suppliers:**

- Map all service providers according to their role, the services they provide, and their criticality to the business (impact on continuity, security, sensitive data);
- Prioritize suppliers according to their importance (e.g., critical vs. secondary suppliers).

**2** **Due diligence before contracting:**

- Conduct risk assessments before signing with a supplier: security, compliance, financial stability, dependencies;
- Verify certifications, security audits, cyber posture, business continuity, etc.;
- Add security and resilience criteria to calls for tender and selection processes.

**3** **Robust contractual clauses:**

- Include **audit and information access clauses**, service level agreements (SLAs), supervision rights, and resilience KPIs in contracts;
- Provide for **exit plans / exit strategies**, substitution mechanisms, and obligations in case of failure;
- Control subcontracting rights and sensitive data flows.

**4** **Continuous operational monitoring:**

- Implement **performance and risk monitoring** throughout the relationship;
- Regularly reassess criticality and impacts in the event of changes to services or the environment;
- Integrate alerts and indicators to detect degradation.

**5** **Continuity and recovery plans:**

- Ensure that suppliers also have their own continuity plans consistent with the company's needs;
- Test resilience via scenarios (outages, major incidents, service disruption).

**6** **Information and capitalization of incidents:**

- In the event of an incident involving a supplier, document, analyze, and incorporate lessons learned to avoid recurrence in other relationships.

**7** **Be aware that even if a service is outsourced, the company itself remains responsible for overall compliance and the management of associated risks. This last point is, for example, a requirement formulated in the DORA regulation.**

FOCUS RECOVERY TIME

# What to do if the announced RTO is not compatible with business objectives?

## 1

**PROPOSE TO BUSINESS LINES HOW TO CONTINUE OPERATING WITHOUT IT OR WITHOUT NOMINAL IT:**

- Manual or semi-manual procedures;
- Backup office tools (Excel, forms, emails);
- Deferred processing with catch-up afterwards;
- Reduced functional scope (priority clients, essential operations).

→ To be formalized in a business BCP, not just IT.

## 2

**STRONG PRIORITIZATION AND REDUCED SCOPE**

- Propose a partial restoration of service (vital functions only);
- Identify a minimal baseline
- Define what will not be restored immediately.

Key message: *"We don't restore everything, but we restore the essentials faster."*

## 3

**ALTERNATIVE BACKUP SOLUTIONS**

Depending on the case:

- Backup applications or platforms available on another technical environment (even if less efficient);
- Temporary recourse to an external service provider,
- Switch to a third-party or group tool (if a multi-entity group);
- Duplication of certain key data outside the main IT system.

FOCUS BACKUP

# The backup strategy, a pillar of the Disaster Recovery Plan (DRP)

Backup rules must be built in the context of a cyber reconstruction. The underlying elements of the infrastructure (binaries, versions, configuration, etc.) must be **documented**, and this documentation must be protected. Scheduling and automation are solutions that can help industrialize these steps for virtualized environments; this will be more difficult for physical or proprietary infrastructures.

Furthermore, the existence of a backup is not a sufficient criterion for a successful reconstruction. It is necessary to consider

- Their **depth** (to ensure the existence of a backup sufficiently far back so that the attacker is not present in it);
- Their **protection** (to avoid destruction by the attacker, for example via immutability mechanisms or out-of-band storage);
- Their **compatibility** (notably the need for synchronization between different systems).

Finally, it is necessary to think about streamlining the backed-up elements according to their sensitivity and importance in the reconstruction process, to avoid "polluting" the latter with an overabundance of unusable backups.

It is necessary to establish a **target for information systems** (through the restart bubble strategy, see below) that is sustainable, healthy, and capable of being available and protected in the event of a cyber crisis. Depending on the modalities of the applications to be rebuilt and the organization, a primary, outsourced, or even Cloud environment can be considered.

Once the target is defined, it is necessary to build a **complete testing strategy**. Indeed, an organization with processes and tools will face problems if the reconstruction has not been tested beforehand. This strategy must rely on unit tests for each building block of the infrastructure, but also on tests of the entire business value chain to ensure that it will work at the time of reconstruction.

FOCUS THE TRUST BUBBLE

## Confidence bubble and/or restart bubble ?

It is a network isolated from the infected IS from which the reconstruction of the IS is likely to be carried out. This reconstruction is done on a foundation of trust, in which only the services vital to the organization are initially deployed.

Depending on company strategies, this confidence bubble can be set up from new systems (e.g., installation of a new Active Directory) or from the restoration of non-compromised backups.

To allow the maintenance of trust in this isolated network, it is advisable to think about:

- Limiting the elements deployed to the strict minimum for the operation of vital services, particularly regarding authentication and network aspects;
- Ensuring the proper security level of the deployed elements, particularly with regard to the vulnerabilities used for the initial compromise of the IS;
- Implementing increased supervision on the IS to verify that the attacker has not returned.

# THE IMPACT OF CLIMATE CHANGE ON BCPS: AN URGENT PRIORITY

The increasing frequency and intensity of climate crises are profoundly transforming the way organizations must consider their business continuity. Recent events have demonstrated that these crises go far beyond classic unavailability scenarios, simultaneously affecting infrastructures, human resources, networks, and supply chains. In this context, the Business Continuity Plan (BCP) must evolve towards a systemic approach, closely integrating risk analysis, coordination with local authorities, and enhanced anticipation of critical interdependencies.

Chapte


r 5

# 5.1. CLIMATE CRISIS: RETHINKING YOUR BCP THROUGH A SYSTEMIC APPROACH TO THE COMPANY

Climate crises differ significantly from conventional resource-unavailability events due to their geographical scale, their cumulative effect, and their ability to simultaneously disrupt multiple critical resources.

The floods in Germany and Belgium (2021) led to the simultaneous destruction of infrastructure, prolonged power outages, and the impossibility of accessing large industrial areas. The extreme heatwaves in France and England in 2022 led to the overheating of data centers, the slowing down of logistics chains, and the unavailability of personnel. These situations demonstrate the need for a systemic analysis including interdependencies, local infrastructures, available energy, and the potential geographical extent of the crisis.

When building the BCP, it is therefore essential to adopt a systemic approach that integrates:

- critical dependency chains;
- local vulnerabilities (infrastructures, energy, access routes);
- the geographical area potentially affected by the climate event;
- domino effects between resources, sites, and infrastructures.

This analysis is an essential preliminary step to prevent the envisaged continuity strategies from being rendered inoperative by the same climate event.

Regardless of the scale or geographical extent of the crisis, the organization's critical processes must be able to continue or restart within the allotted time. We use the term *"fractal"* to define a level of homogeneous resilience, regardless of the geographical scale chosen. This notion implies that business continuity must remain robust, whether the disruption affects a single site, a set of regional sites, or an entire national territory.

The company's response level must be identical regardless of the geographical scale of the crisis.

- of a circumscribed location: the loss of a building in a fire;
- of a geographical mesh: the Seine watershed in the event of a flood of the Seine;
- of a country/state: Hurricane Katrina which hit the state of Louisiana;
- of a zone: Storm Boris in September 2024 which caused devastating floods in Eastern European countries;
- of the entire world: the COVID-19 pandemic episode of 2020.

Consequently, securing the company's business continuity at any geographical scale requires measuring the level of insertion and dependence on the territory, local, departmental, regional, national, in order to understand how the territory's vulnerabilities can propagate to the organization's critical activities. This understanding is a prerequisite for the ability to design truly resilient strategies capable of absorbing or bypassing the effects of a climate crisis, regardless of its scope.

# 5.2. RE-EVALUATING CONTINUITY STRATEGIES IN LIGHT OF CLIMATE RISK

A climate crisis can invalidate continuity options that are relevant in standard situations. It is therefore necessary to re-examine existing BCP measures, in particular:

### → VALIDATION OF THE AVAILABILITY OF FALLBACK SITES

A backup site located in the same geographical area is at risk of being affected by the climate event. During Storm Xynthia (2010), several coastal fallback sites considered by companies were rendered inaccessible due to simultaneous flooding throughout the coastal area.

It is recommended to:
- systematically verify the climate exposure of the fallback site;
- plan for an alternative, geographically separate site;
- document selection criteria (altitude, networks, access, exposure).

### → HUMAN RESOURCES MANAGEMENT IN A CLIMATE CRISIS SITUATION

Members of the crisis management team can be affected both professionally and personally.

The passage of Cyclone Garance over Reunion Island on February 28, 2025, demonstrated very concretely the extent to which members of a crisis management team can be affected both professionally and personally. The event caused winds exceeding 200 km/h, exceptional rainfall, in some places more than 500 mm in a few hours, as well as heavy damage to essential infrastructure: roads cut off, homes destroyed, and hundreds of thousands of people deprived of water, electricity, or the Internet. In this context, several professionals mobilized to manage the crisis saw their own personal situations severely affected. Some lost their homes or found themselves unable to travel due to collapsed or flooded roads. Garance demonstrates that in a major climate disaster, members of a crisis management team are not just actors mobilized for the organization's continuity: they are also inhabitants of the territory, exposed and vulnerable, facing the same losses and trauma as the rest of the population. This reality requires the systematic integration of human backups, a flexible organization, and crisis scenarios that take into account the sudden or prolonged unavailability of key personnel.

It is essential to:
- plan for operational backups for every key role in the crisis management team;
- organize minimal cross-training for critical functions;
- integrate the unavailability of crisis management team members into the BCP.

The habitability of a territory is a factor to consider in BCPs following an extreme event such as an earthquake, hurricane, or devastating flood. The human resources necessary for operations will no longer have housing or means of transport. To ensure business continuity, the company may decide to provide a transport service, rent vehicles, or relocate employees and their families near the place of work.

Source: Behind the Scenes of Crisis Communication podcast, Communicating in the middle of a storm: Feedback on Cyclone Garance – 04/12/2025

# 5.3. EVALUATING THE RESILIENCE OF THE INTERVENTION CHAIN

As part of the BIA (Business Impact Analysis) and the definition of RTO/RPO, it is necessary to take into account the vulnerabilities of critical suppliers and service providers involved in continuity (e.g., cleaning companies, roof repair, pumping, etc.),

**Consider the case of the floods in Valencia**, Spain, in October 2024 (DANA, Depresión Aislada en Niveles Altos):

At the end of October 2024, the Valencia region was hit by a DANA of exceptional intensity. In the space of a few hours, more than 400 mm of rain fell on the provinces of Valencia, Alicante, and Castellón, causing massive infrastructure destruction, the flooding of entire neighborhoods, and a human toll exceeding two hundred victims. The material damage, estimated at nearly 29 billion euros, testifies to the scale of the disaster, which has become one of the most serious climate catastrophes in Spain's recent history.

In the hours and days that followed, public and private organizations attempted to activate their emergency plans. However, the combination of a very extensive impact zone and the simultaneous destruction of essential infrastructure led to the rapid saturation of specialized service providers: pumping, drying, electrical restoration, IT, industrial cleaning, or heavy logistics. Local companies were no longer able to meet demand, while several damaged roads blocked access to certain areas.

This episode provides a major lesson for organizations: during a large-scale climate crisis, local service providers quickly become unavailable, even when they are theoretically contractually committed to intervene. For Risk Managers, this reality requires rethinking the BCP by integrating alternative suppliers located outside the exposure zone, adjusting RTOs to account for significantly longer response times, and anticipating the simultaneous unavailability of critical resources. The Valencia example highlights the need for resilience across the emergency response chain — beyond the company's internal resilience.

In this context, to further secure the continuity of essential activities, it may be relevant to establish partnerships with post-disaster specialists. This can involve setting up pre-established contracts with companies expert in restoration, in order to guarantee rapid intervention in the event of significant damage. It is also possible to formalize priority intervention agreements, allowing the organization to be treated first during a crisis affecting a large number of clients. Finally, carrying out preliminary audits with these service providers helps to accelerate their mobilization on the day of the event, by clarifying technical procedures, site access, and the company's specific needs in advance.

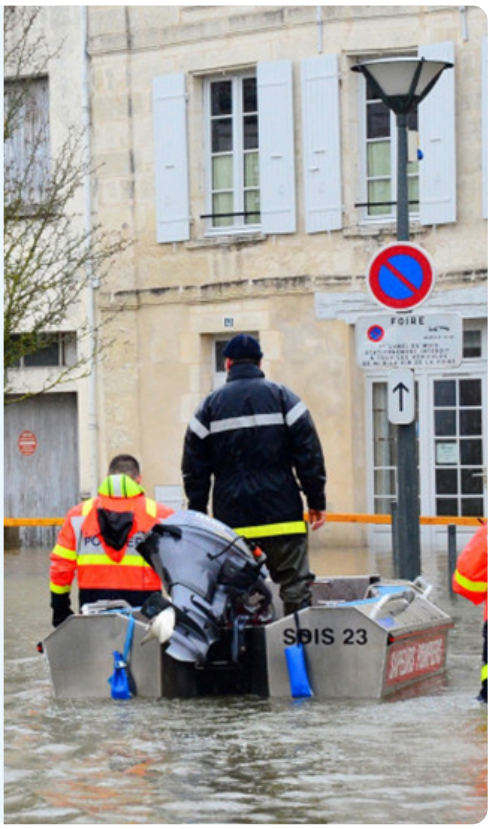
## Structuring a climate alert system

The implementation of an early and gradual warning system makes it possible to anticipate climate events and trigger BCP measures in advance. This anticipation reduces operational impacts by securing people, assets, and facilities before the crisis. It facilitates the rapid activation of fallback solutions and the coordination of teams. By relying on defined alert thresholds and reliable sources, the organization gains responsiveness. Result: a significantly reduced recovery time and strengthened resilience.

### Importance of coordination with local authorities during a climate crisis

During a climate crisis, coordination with local authorities is essential, as they are the first to have an operational view of the situation: state of roads, evacuation priorities, dangerous areas, critical infrastructure failures, or access restrictions. They also concentrate emergency resources (firefighters, law enforcement, technical services) and manage the dissemination of alerts to the population. A company that does not rely on this information risks endangering its teams, unnecessarily mobilizing resources, or aggravating its own vulnerability.

In addition, authorities orchestrate the management of public infrastructure, roads, electricity networks, water, telecoms, which directly condition an organization's ability to activate its BCP. Good coordination therefore makes it possible to obtain reliable information, anticipate logistical constraints, and adjust recovery priorities to the real context.




## 5.4. LONGER BUSINESS RECOVERY TIMES

Compared to a classic crisis, a climate crisis generally leads to much longer recovery times, particularly because several essential resources may be unavailable simultaneously. It also causes the joint degradation of multiple infrastructures, whether it be water, roads, telecommunications, or electricity, making recovery more complex and slower. Added to this is a massive mobilization of emergency responders, often overwhelmed by the volume of interventions to be carried out across an entire territory.

Faced with these constraints, the BCP must incorporate additional time margins for each of the identified dependencies. It also becomes essential to adjust RTOs so that they reflect major climate scenarios and no longer just isolated incidents. Finally, recovery priorities must be reinforced to concentrate limited resources on the most critical activities from the first hours of the crisis.

FOCUS: SEINE FLOODING

## Let's take the example of the *"Seine flood"*

In the event of a flood, if the electricity supplier is no longer able to power a neighborhood, the companies residing there will have to equip themselves with generators to continue their activities.

Similarly, high-rise buildings (HRB) present a specific vulnerability. Indeed, specific regulations require the permanent presence of a fire safety and assistance service (FSPAS) within the building's Security Control Center. However, the disruption or even interruption of public transport and potential traffic restrictions could prevent the necessary continuity of service. Thus, it is possible that some high-rise buildings could become inaccessible, not by the direct impact of the Seine flood (flooding) but by the absence of FSPAS personnel, which ipso facto leads to an administrative closure of the building.

Furthermore, companies using *"data center"*, i.e., buildings in which all or part of the computer data is hosted, present a particular vulnerability. Indeed, they are generally located in the Ile-de-France region, a few tens of kilometers from office buildings.

In this scenario, the office building and the data center are connected by a computer network (which can carry data and/or *"voice"*).

However, we know that these cables and fibers *"run"* in the RATP tunnels and the sewers of Paris. In the first case, the RATP has warned that it would voluntarily flood some of these tunnels in the first days of the crisis to prevent water pressure from damaging the infrastructure. In the second case, all of Paris's sewers will be completely flooded. Even if the cables are waterproof, it is highly foreseeable that certain parts of said communication devices will present vulnerabilities (splices, repeaters, etc.) which could cause more or less significant malfunctions across the entire network. As a result, even if the office building and the data center are outside the geographical flood zone of the Seine, it is possible that the company will be strongly affected by the fact that it will no longer have access to its network. We can then speak of collateral damage.

| Resources | Vulnerability | Impact | BCP Mesure |
|---|---|---|---|
| **Power supply**<br>Public grid supplier | **Flooding**<br>in neighbourhood < loss of power<br>Level: high | **Total shutdown**<br>of office, IT, security, lighting | **Generator**<br>Supplier contract<br>Delivery within 4 hours<br>Resp. : Facility Manager |
| **HRB — FSPAS**<br>Permanent security service mandatory | **Transport blocked**<br>FSPAS staff unreachable<br>Level: critical | **Administration Closure**<br>Building inaccessible without flooding | **On-site accommodation**<br>On-call agreement<br>Rotation plan<br>Resp. : HR Director / FSPAS |
| **Data center**<br>Located in the Ile-de-France region | **Flooding**<br>Infrastructure or power cut<br>Level: critical | **Loss of IT access**<br>Data inaccessible<br>Applications down<br>RTO to be defined | **Fallback site / cloud**<br>Data replication<br>Transfer < RTO<br>Resp.: CIO |

# 5.5. CLIMATE RISKS THAT GENERATE THEMATIC & GRADUAL RESPONSES

Faced with the increasing complexity of business continuity issues, the binary approach (usual operating mode / BCP operating mode) is no longer enough. It is therefore necessary to identify gradual recovery actions (from the simplest to the most complex threats) and to adopt responses proportionate to a set of undesirable events, which are more or less disruptive.

Beyond their own vulnerability, companies must worry about the repercussions of a break in the value chain: the continuity of a just-in-time flow with suppliers, the availability of infrastructure, or even the clients on whom they depend.

The approach of a single, structuring but rigid *"plan"* is not suitable. It must give way to the creation of a *"toolbox"* allowing for gradation and a proportionate response in the business continuity actions to be implemented (reflex action sheets or Checklists that present the main actions that each Department must implement in the event of a disaster, a recovery schedule for Human Resources activities that presents, day by day and department by department, the number of employees who must report to the fallback site, etc.). BCPs must be designed to be flexible and adaptable, because real crises never follow anticipated scenarios exactly.

The quote *"The exact scenario will never happen: you must prepare for the unpredictable"* is even truer with climate risks!

Beyond their own vulnerability, companies must be concerned about the ability of their partners or critical service providers to meet their service obligations in the event of a major disaster, including the service capacity of emergency resources. Indeed, the company is at the heart of the dependency networks of its partners and subcontractors (suppliers of drinking water, electricity, telephone networks, mail, etc.). The failure of any one of them effectively affects the company's operations.

# 5.6. DELIVERABLES AND ADDITIONS TO INTEGRATE INTO THE BCP

Following the BCP update process to cover unavailability linked to climate events, several additional elements must be formalized:

- Reflex action sheets adapted to the climate hazards to which the site is exposed (flooding, storms, heatwaves...)
- Mapping of access routes and alternative roads. Include priority roads, high-risk roads (floods, landslides...), and contingency routes.
- The location of fallback sites and backups (document: the main fallback site, the secondary site geographically separated from the hazard being studied, verify energy autonomy in the event of a prolonged power outage in the area...).

# COORDINATION BETWEEN THE BCP AND OTHER RISK MANAGEMENT TOOLS

The Business Continuity Plan must be integrated into a broader global risk and crisis management framework.

Chapte


r 6

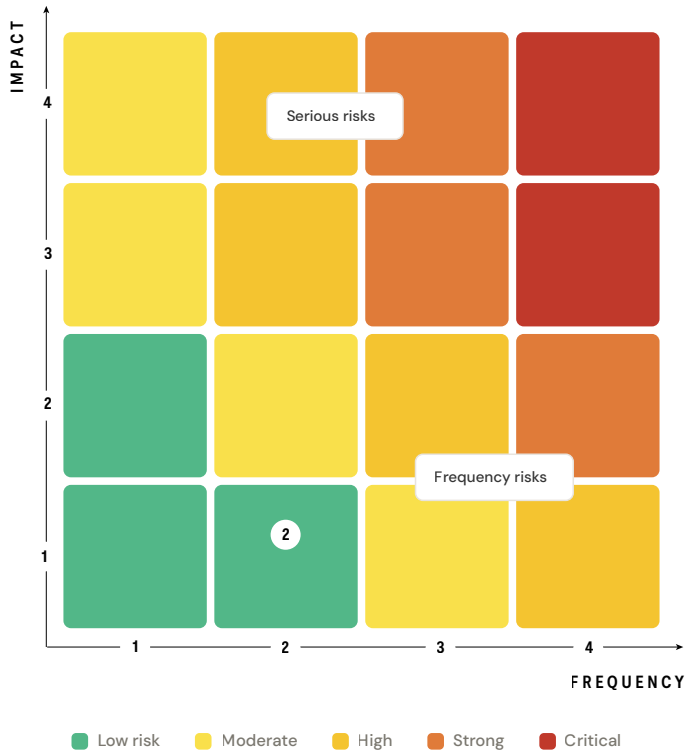
# 6.1. BUSINESS CONTINUITY PLAN AND RISK MAPPING

Risk mapping and the Business Continuity Plan are closely linked: the former identifies and prioritizes threats, while the latter organizes the operational response aimed at limiting their impacts on essential activities.

Climate risk, like cyber risk, can be integrated into risk maps in different ways: as an autonomous risk, as a contributing or aggravating factor of existing risks, or according to a hybrid approach, now favored because it is more representative of interdependencies and systemic effects.

These risks present potentially critical impacts on business continuity, including when they materialize indirectly or with a delay. Their integration into Likelihood/impact matrices therefore requires adapting analysis methods in order to better take into account low-frequency but very high-severity phenomena, the effects of which can exceed traditional recovery and crisis management capabilities.

## 6.1.1. Frequency risks and severity risks



Risk mapping is a tool for identifying, cataloging, and quantifying risks. This risk quantification is carried out using a statistical approach.
Thus, in this sense, *"risk"* is defined as the product of *the frequency of occurrence* of the undesirable event and the feared impacts of the threat that the risk poses to the organization.

CLIMATE FOCUS

## Climate risk

Climate risk analysis requires an in-depth approach to identify threats linked to the physical effects of climate change, whether chronic (rising temperatures, water stress, etc.) or acute (heat waves, heavy rain, storms, etc.) as well as risks of non-adaptation.

It is based on three key steps:

- Identify climate hazards (a climate-related event – such as heat waves, heavy rain, etc.);
- Assess asset exposure (the location, physical attributes, and value of assets or people that could be affected by a hazard);
- Assess asset vulnerability (propensity or predisposition to be negatively affected by a certain danger and encompasses a variety of concepts and elements, including sensitivity or susceptibility to damage).

This *"Probability/Impact"* diptych approach also makes it possible to determine groups of risks:

#### 6.1.1.1. The frequency risk group

It is measured by the *"frequency of occurrence"* indicator. Indeed, even if the unit impact of the risk materializing is minor, the fact that it occurs often or frequently ipso facto generates significant financial consequences for the organization.

EXAMPLE

**A typical example is the company car fleet:** a group of sales representatives has company vehicles. Because these personnel carry out long and numerous professional journeys, it is likely that they will cause or be victims of collisions resulting in material damage without bodily injury. Taken individually, a collision will generate a repair cost of a few thousand euros. On the other hand, the large number of company vehicles will multiply the risk of collisions, and therefore the total financial volume of repairs will be very significant.

Consequently, it will be appropriate to implement preventive actions aimed at reducing the frequency of occurrence of the undesirable event. In this example, *"sustainable"* driving courses on a track will allow the company's sales representatives to better control their vehicles, adopt better driving habits, and thus avoid the occurrence of collisions: the number of collisions will decrease, and therefore the financial impact on the company will be lower.

#### 6.1.1.2. The severity risk group (or crisis risks)

It is measured by the *"impact severity"* indicator. Unlike frequency risk, the unit impact of the risk materializing here is very significant, or even vital for the company, while the risk of it occurring is unlikely. It will be necessary to implement treatment plans in order to reduce the impacts associated with the event occurring. Thus, the crisis management plan and the business continuity plan are part of the risk treatment tools, curative tools, and protective measures.

In summary, within the overall risk management process, risk mapping is the reference tool during the risk identification, cataloging, and prioritization phase. It is used before the implementation of risk treatment tools, including the BCP. The latter's purpose is to reduce the impacts of the occurrence of a severity risk, i.e., a crisis.

### Let us therefore remember that:

1. mapping is a tool for identifying and quantifying all of the organization's risks.
2. The BCP is a tool for treating severity risks (low probability of occurrence/high impact severity). Its purpose is operational.
3. Risk mapping methodologies use probabilistic approaches to quantify risks. The BCP methodology uses a deterministic approach to ensure the continuity of processes identified as critical.
4. Unlike other severity risks, which are generally one-off events, a cyberattack combines several aggravating characteristics: intentionality (the attacker adapts to defenses), persistence (the threat remains active), systemic effect (rapid propagation to the entire IS), and contamination of trust (doubt regarding data integrity). These specificities require a dedicated approach detailed in chapter 4.

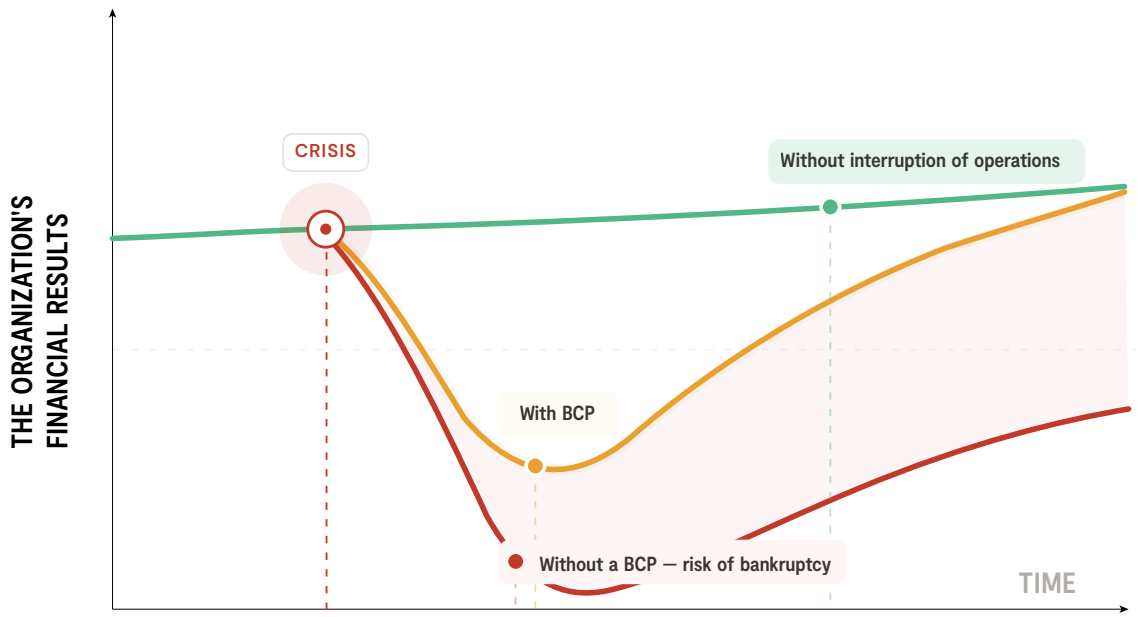
# 6.2. BUSINESS CONTINUITY PLAN AND USE OF INSURANCE SYSTEMS

The BCP can be a tool for optimizing insurance costs: all operations implemented to cushion the financial impact of a crisis on results will be factors in reducing the damages provided for in insurance contracts.

It will then be easier to negotiate the amount of the insurance premium by proving that the company has set itself in motion to reduce the impacts of the crisis (updated BCP and crisis management plan).

Also, with insurance coverage, and in particular the "*Property Damage/Business Interruption*" policy, the company can protect itself against the costs of triggering the BCP (such as renting a back-up site, telephone and mail re-routing costs). Include insurance stakeholders in the development of the BCP, without forgetting to leverage competition.

FINANCIAL IMPACT OF A CRISIS — BCP



**CLIMATE FOCUS**

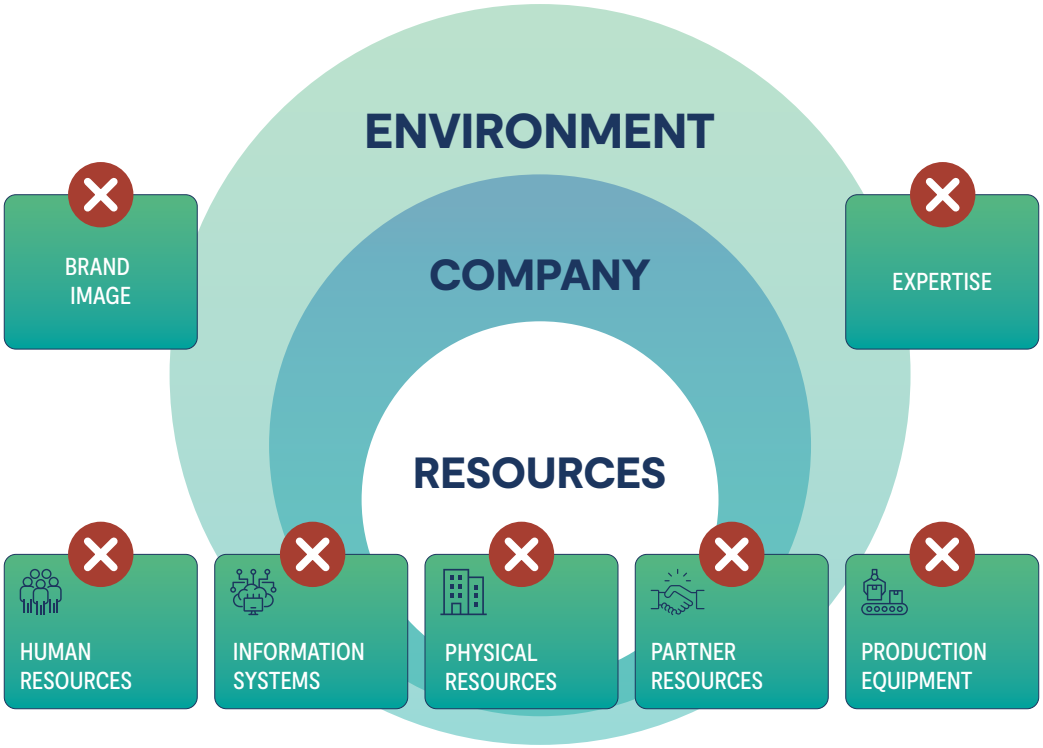
In the face of insurable extreme weather events, such as storms, floods, or episodes of intense rainfall, a robust Business Continuity Plan (BCP) makes it possible to demonstrate the organization's ability to limit the operational and financial impacts of a disaster. The BCP is therefore a key lever for dialogue and negotiation with the property damage insurer — particularly for business interruption — by making explicit the prevention, adaptation, and recovery measures put in place to deal with major climate risks. For local authorities, this issue is particularly sensitive: they are currently facing a multiplication of coverage refusals or a tightening of insurance conditions linked to climate risks. The ability to demonstrate the existence of a robust, updated, and tested BCP then becomes an essential lever for securing insurance coverage and strengthening the authority's credibility with its insurer partners.

# 6.3. COORDINATION BETWEEN "*CRISIS MANAGEMENT*" AND "*BUSINESS CONTINUITY*" ISSUES

There is a consensus that the issues of *"crisis management"* and *"business continuity"* must be linked. However, there are no standards for how these two concepts should be linked. Some professionals integrate crisis management into business continuity policies, while others propose inserting the BCP into more global crisis management frameworks. It is necessary to clarify this point and propose a link.

This link is particularly tested during modern cyber-crises. Unlike a circumscribed physical disaster, an advanced computer intrusion is a dynamic event that requires perfect choreography between technical response (incident management), strategic decision-making (crisis management), and restoration of operations (business continuity). Chapter 4.4 will return to this essential convergence, which constitutes one of the major evolutions in thinking on corporate resilience.

## 6.3.1. Typology of crisis: *"Operational crises"* and *"visibility crises"*




We have seen previously that the normal operation of a company requires the use of a set of resources. In the event of the disappearance or unavailability of one or more resources, triggering the Business Continuity Plan will allow it to mitigate the unavailability as much as possible.

### THE OPERATIONAL CRISIS

This first type of crisis, which affects the company's resources and consequently requires the triggering of the BCP, is qualified as an *"operational crisis"*. However, there is a second type of crisis that affects the company's capital but does not require the triggering of the BCP.

### THE VISIBILITY CRISIS

It is a crisis in which *"our visibility system"* (detection, inventory, evaluation) is failing[9]. Indeed, the common denominator of this type of crisis is the challenging of the trust that all stakeholders place in the company, which can occur as soon as one or more of the company's stakeholders (shareholders, customers, NGOs, etc.) questions or even challenges it on a particular issue (financial, societal, ethical, etc.). Consequently, if the organization cannot provide an immediate response that is consistent with the representations, aspirations, and expectations of the stakeholders, it finds itself in a *"visibility crisis"*.

(9) The concept of *"Visibility Crisis"* is defined in the book *"Gérer les grandes crises" (Managing Major Crises)*, Louis CROCQ, Sophie HUBERSON, Benoit VRAIE, Odile Jacob editions, 2009.

EXAMPLE

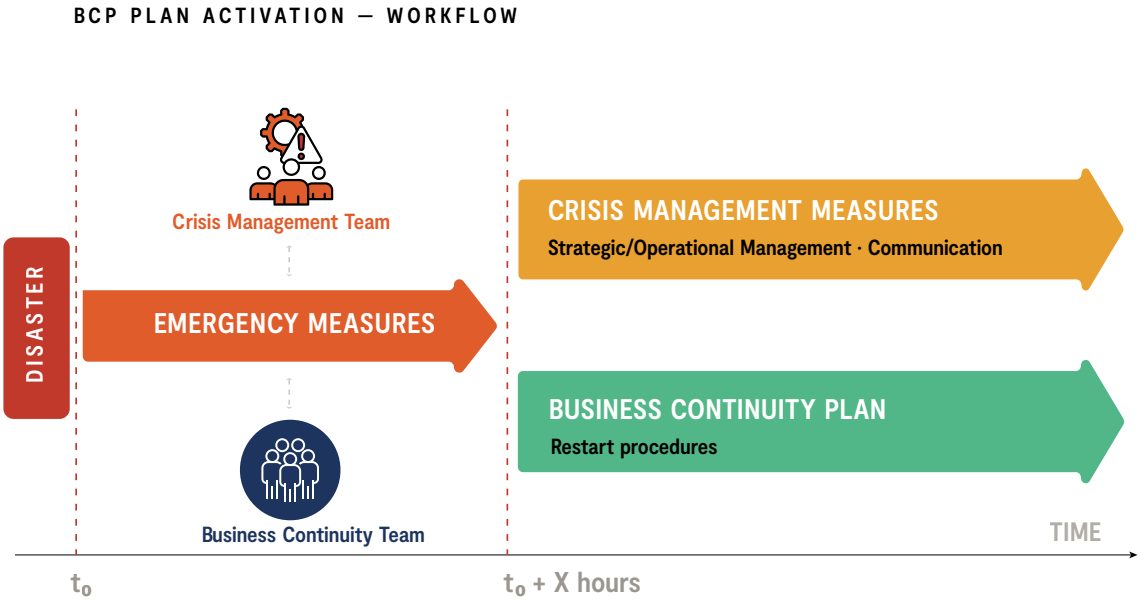
**The *"visibility crisis"* was experienced by Nike in the 1990s.** An NGO revealed that the company was employing children in Southeast Asia, moreover in precarious conditions. Faced with the scale of the scandal, Nike was forced to immediately cease this practice, which did not correspond to the ethical expectations of its customers.

The pandemic crisis episode is eloquent. Experts predicted a global extension of the H5N1 virus, initially present in an endemic state in Southeast Asia. But it was another virus, the H1N1 virus, that appeared in Mexico and spread rapidly. From the beginning, experts provided divergent opinions, both on the pandemic nature and on the danger of the virus. Thus, each State, according to its own logic (context, history, sensitivity of the population, etc.), exercised its precautionary principle to varying degrees, without coordination at either the international or European level, nor an accurate assessment of the perception, mental representations, and reactions of public opinion. These different positions and the divergences expressed within the scientific world therefore contributed very largely to the appearance of a visibility crisis.

We therefore see that these organizations went through very significant crises even though all the resources of the company in the first case, and of the States in the second case, were still available. As such, it is not necessary to trigger the business continuity plan. On the other hand, the restoration of the organization's reputation will be the subject of the implementation of *"extraordinary"* communication measures.

In addition, it is possible for a crisis to be successively or simultaneously an *"operational crisis"* and a *"visibility crisis"*.

## 6.3.2. Roles and responsibilities of crisis management teams and business continuity teams



### ROLES AND RESPONSIBILITIES OF CRISIS MANAGEMENT TEAMS

Within the company, a small group of employees gathered in crisis cells will implement ***"extraordinary"*** actions (in the primary sense of the term, i.e., outside of the daily routine). Each member of the crisis cell will hold a function that may be different from the one they usually perform within the company. Example: the financial director finds themselves *"coordinator"* of the company's crisis management cell and therefore no longer uses their accounting and financial expertise but rather their coordination talents in order to organize the collective crisis management action.

### ROLES AND RESPONSIBILITIES OF BUSINESS CONTINUITY TEAMS

Unlike crisis management, all or part of the employees (depending on the continuity strategy adopted by the company) will continue to **practice their *"usual"*** actions within the company (the accountant will continue to do the accounting, the maintenance agent the maintenance) but in **a framework and with modalities that will be *"extraordinary"*** for them, such as working at a fallback site or working remotely (teleworking).

## 6.4. BCP & OTHER RISK MANAGEMENT METHODS

As we have seen, the BCP is not a definitive answer; it is one of several risk management tools. There are therefore situations where the BCP is not an appropriate/effective solution, where the investment effort should be made in terms of prevention rather than protection.

**EXAMPLES**

#### Example of a very specific machine tool (few units produced worldwide) within a production line

In the event of a disaster, it will be very difficult to replace the machine tool. In this respect, it is preferable to prevent any incident likely to damage the integrity of the machine tool (by installing, for example, an automatic gas extinguishing system in the event of a fire) rather than implementing a BCP.

#### Example : regarding supply chains

It is advisable to respect two principles of prevention even before considering a *"critical suppliers"* BCP. Firstly, do not depend on a single supplier but share your activity between several providers, and secondly, use providers working in distinct and clearly identified geographical areas.

# THE HUMAN FACTOR IN A CRISIS SITUATION: THE HUMAN AND SYMBOLIC DIMENSIONS

Chapte


r 7

# 7.1. ASSESSMENT OF THE PERCEPTION OF RISK SEVERITY BY EMPLOYEES

Like the 2009 flu pandemic, the COVID-19 crisis revealed the difficulties and levers associated with the perception of risk by populations, while highlighting the importance of developing a culture of risk and crisis that is durably anchored in the collective consciousness.

During the pandemic episode, the State's crisis communication policy was triggered. The communication plan was rolled out automatically without systematically taking into account the sensitive dimension of the collective imagination, stress, and behaviors. The State did not carry out sufficient diagnosis and monitoring of the population's expectations in terms of communication. It underestimated the capacity for adherence, indifference, or rejection by citizens. In other words, it did not take into account the fact that the population could perceive the threat in a different way and with a different intensity than what it had foreseen.

The forecasting of individual and collective behaviors in a situation of threat or pandemic reality was lacking. The public authorities were content to distill, in a top-down manner, communication aimed at *"mitigating the fears and anxiety of the population and avoiding the risk of disinformation, rumors, or even destabilization"* (Government Plan), but they neither explored nor inventoried the predictable behaviors of the population.

The development of BCPs (Business Continuity Plans) takes into account the forecasting of these individual and collective behaviors in a situation of unusual threat. The BCP must integrate the human factor, both individual and collective. It aggregates the collective mental representations of the threat and the risk and the aberrant individual or collective behaviors (carelessness, underestimation and denial of danger, or conversely, agitation and panic exacerbated by the effect of rumors).

In the first place, these are adapted and responsible behaviors. To return to the example of the pandemic, this corresponds to anticipating the danger, adopting appropriate measures, then staying informed day by day about the state of the threat, without panicking, not believing in rumors and not spreading them, applying prevention measures (washing hands, wearing masks), getting vaccinated if health authorities advise it, consulting at the first symptoms of flu, getting treated, avoiding contaminating loved ones.

In the second place, these are behaviors of carelessness, negligence, or even denial, which are irresponsible: not believing (out of reckless optimism) in the possibility of the crisis, not informing oneself about the danger it presents, not becoming aware of the prevention measures, displaying systematic critical skepticism regarding the information provided, not informing oneself about the progression of the threat.

In the third place, these are behaviors of exaggerated fear, agitation, and panic: a state of

exaggerated worry at the announcement of the possibility of a crisis, excess in the search for information about this danger, then in the daily investigation of its progression, experiencing an exacerbated sensitivity to rumors, proceeding to reckless and excessive purchases of equipment...
Depending on the issues covered by a given BCP, identify the employees' mental representations and establish sufficient diagnosis and monitoring of the population's expectations. It is therefore more a work of long-term education and acculturation of the population than ad hoc, technical, and thematic responses to this or that crisis.

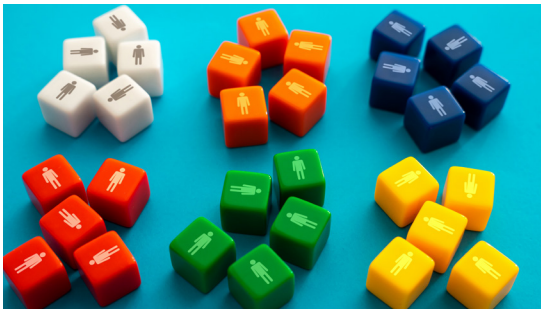
## 7.2. RESPECTING *"WORK/REST"* BALANCES

In times of crisis, aggravating physiological factors are omnipresent; it is necessary to respect *"work/rest"* balances. Fatigue caused by work overload and poor ergonomics of the workstation, sleep deprivation, and frugal and hasty meals can wear down individual energy and exacerbate susceptibilities.

Thus, beyond biological aspects, it is essential that the individual respects *"work/rest"* balances and that they practice relaxation exercises at regular intervals. In a crisis situation, it is therefore advisable to maintain an adequate lifestyle.

## 7.3. OVERLAPPING CONTINUITY TEAMS FOR SUSTAINABILITY

The crisis can last for several days or several weeks. The Organization must plan for operation in pairs and an *"overlap"* of teams. More than a simple briefing during the shift handover, it is important that the two people work together long enough for the transmission of information to be as complete and accurate as possible in order to ensure true continuity despite the change.



# 7.4. STRESS AND ITS IMPACTS

The perception of the crisis, the risk, and the danger can become a constituent or aggravating factor of the crisis itself. The emotional shock can generate a real *"disorganizing"* tide in all the cognitive and operational capacities of individuals and groups: this is the irruption of stress.

Drawing on a definition proposed by Selye, Louis Crocq defined (1999) stress as: *"the neuro-biological, physiological, and psychological reaction of alarm, mobilization, and defense of the individual faced with an aggression or a threat, a threat to their life, their physical integrity, or their psychic balance"*.

Stress is a useful, adaptive reaction. Thanks to their stress, the individual escapes danger or finds themselves in a position to face it, which corresponds to the English word *"coping"*.

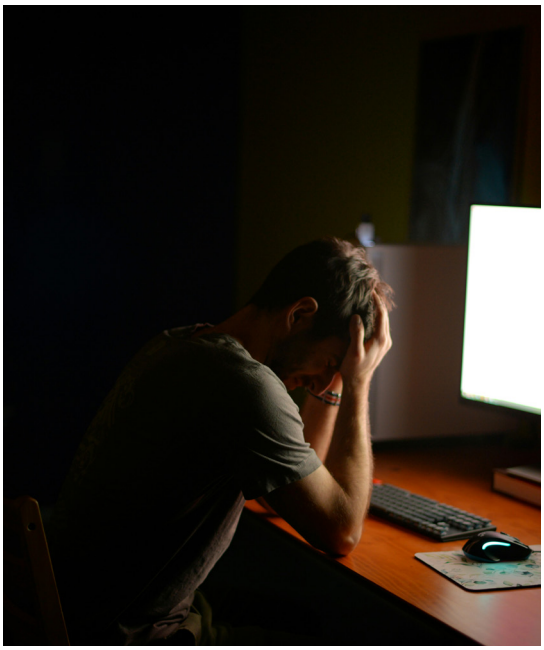


Photo credit: laram-BpTqCNotBLI-unsplash

It is accepted that stress has three main psychological effects:

1. **it focuses attention on the threatening situation, temporarily driving other ongoing preoccupations and thoughts out of consciousness,**
2. **it mobilizes cognitive capacities (attention, memorization, evaluation, reasoning),**
3. **it encourages decision-making and action.**

The downside is that stress is burdened with bothersome symptoms (paleness, sweating, tachycardia, visceral spasms) and is energy-intensive. In its most intense phase, we speak of *"post-traumatic"* stress and obtain the following clinical picture [10]:

- **stupefaction** : the individual is stunned, stuporous, abulic, petrified;
- **sterile agitation**: the subject is in a state of psychic, verbal, and motor excitement;
- **panic flight**: the person under stress is *"launched"* into a frantic flight, a state of generalized panic;
- **automaton** behavior: the individual performs repetitive mechanical gestures that they will not remember.

(10) See on this subject the work of General Physician Louis CROCQ and Benoit VRAIE

# 7.5. *"PREPARE TO BE READY"*[11]

The Red Cross offers an awareness campaign whose paradigm is *"self-resilience,"* that is to say, the citizen's ability to take care of themselves in the event of a crisis. *"Preventing, reflecting, and anticipating in order to act better means considerably reducing the consequences that can arise from these emergency situations: everyone can become an actor in their own survival and that of others thanks to essential reflexes that allow for reacting to exceptional situations."* [12]

This principle is transferable to company employees. In the case of the Seine flood issue, some companies have a BCP (Business Continuity Plan) in which the number of employees necessary for the resumption of activity is listed. However, beyond the numerical value, these employees may not be available to the company on D-Day. Indeed, the Seine flood phenomenon will generate significant disruptions at various levels of state services, institutions, and all infrastructure as well as critical networks: water, electricity, telecommunications, transport, heating, household waste...

The employee will therefore have to manage the fact that their family no longer has drinking water, electricity, internet, telephony... So there is no certainty that unprepared employees will be present for their company. As a result, companies, in their reflections on business continuity problems, must reposition *"the employee"* at the center of the system and put in place, for critical functions, support measures for employees. To return to the example of the Seine flood, companies must raise employee awareness about the attitude to adopt in order to prepare them personally for this scenario and support them (financially and/or through practical arrangements) in securing their family.

(11) (12) Website *"French Red Cross"*

# *"PREPARING FOR WAR IN TIMES OF PEACE"* AS A BCP PHILOSOPHY

The toolbox used to develop the different types of BCPs is well-stocked. Each tool has a specific function but will only be effective if it is well used by trained, competent, and motivated personnel.

Chapte


r8

# 8.1. CRISIS CULTURE

Crisis culture and business continuity culture go hand in hand. The objective is to constitute a body of values, convictions, and knowledge shared within the community of employees that aims to properly grasp crisis situations and mobilize the capacities of these teams to overcome them.

This posture therefore consists of collectively adopting a philosophy of reasoned acceptance of risks, vigilance, and situational awareness [13] in the face of undesirable events. It *de facto* entails an empowerment of all personnel holding a share of responsibility in three distinct functions:

- sentinel function, as a lookout in the identification of risks;
- alert function in the detection of weak signals, near-accidents, accidents, and crises;
- management function in the methods of dealing with risks and crises.

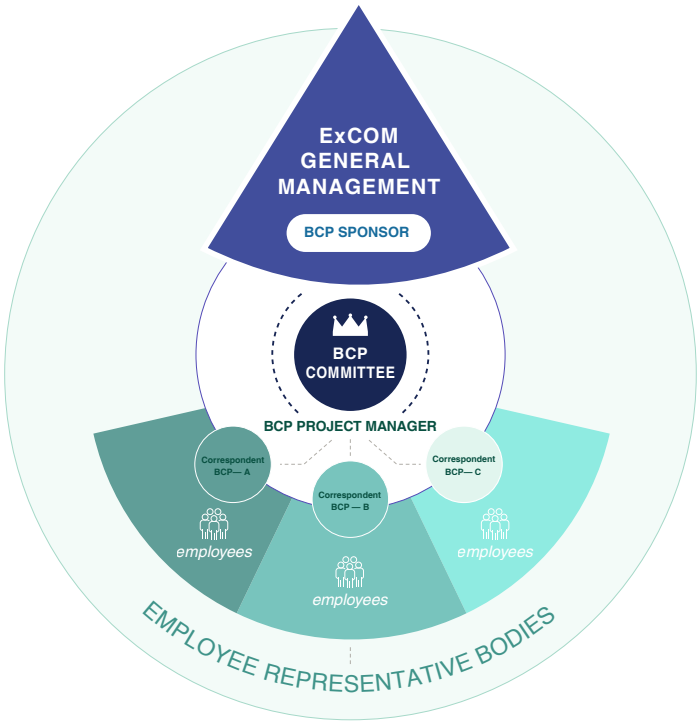
This *"crisis culture"* is essential but cannot be decreed: when a population, an organization, or a company is confronted with a crisis at a moment in its history, it is already conditioned by its habits and dependent on its own markers. Its norms, its operating framework, its *"breeding ground"* will be conducive to generating specific behaviors to react or even to deal with the crisis. If for employees who have been in their positions for a long time, this body of knowledge has been acquired during BCP tests and crisis management exercises (or real-life crisis management), it must be transmitted to new recruits as ways and attitudes to adopt to face future crises.

The active participation of each employee at their level in risk management systems improves the coherence and resilience of the entire system. It multiplies the effectiveness of the overall actions carried out by the *"risk manager,"* the *"BCP manager,"* and the *"crisis manager"* (functions that can also be performed by one and the same person).

The *"risk manager"* is too often considered the *"in-house expert"* capable of handling all risk management issues alone. Yet, they are above all, in their ERM (Enterprise Risk Management) and Insurance function, a coordinator, a facilitator, an animator of the company's actors. It is therefore up to everyone in the company to *"think about the conceivable, the unpredictable, and the unimaginable"* and thus become an actor in risk management. To do this, the involvement of the human resources department is decisive.

(13) *"Managing major crises"*, Crocq, Huberson, Vraie; 2009.

# 8.2. BCP PROJECT GOVERNANCE




## 8.2.1. A company-wide approach accepted by all and funded by Senior Management

The role of Senior Management is obviously paramount in structuring and maintaining a culture of risk and crisis management. It involves:

- clarifying political and strategic guidelines to give meaning to the action of restoring assets damaged by the crisis;
- providing a monitoring and information system to anticipate crises;
- implementing a specific work organization in which the parameter of *"occurrence of a crisis"* plays an important role: making it known, understood, and accepted that one may work under conditions other than those initially set, for extraordinary reasons;
- training the organization's stakeholders in crisis management and working in "degraded mode";
- establishing a climate of social dialogue conducive to accepting working conditions that are different and sometimes more restrictive than in a normal state.

The Organization's Senior Management promotes and supports the BCP initiative as a unifying project because it involves and mobilizes the various departments, whether operational or cross-functional. To do this, the latter must itself be convinced of the usefulness of funding BCPs.

## For a favorable reception of the BCP by Senior Management: the arguments to present.

They fall into two categories:

**1** **A "*quantitative*" order because the BCP allows for the evaluation of:**

- the company's losses in the event that an adequate business continuity organization is not implemented. (See graph on page 28 regarding the company's results without the implementation of a BCP.);
- the reduction of the insurance premium due to better protection of the company: the stronger the shield, the less the insurance company will need to compensate.…

**2** **A "*qualitative*" order because the BCP contributes to building better performance in terms of Human Resources:**

- Mobilizing staff around a unifying theme: safeguarding the company and thereby employment;
- Improving quality in the company by conducting an organizational audit, testing procedures, and running crisis exercises;
- Improving the flow of information within the company by encouraging different departments to work together;
- By demonstrating the educational value of developing and implementing a BCP: one cares as much about people as about assets. Internal and external communications are improved as a result.

#### 8.2.1.1. The sponsor

Finding a *"sponsor"*, ideally an Executive sponsor or champion, within Senior Management, is a guarantee of the project's success. The latter will be particularly convinced of the superior interest of their mission and will be valued accordingly. They will be endowed with the necessary powers and authority, in short, the hierarchical legitimacy necessary for the accomplishment of their mission.

This sponsor allows the BCP manager to benefit from support and a facilitator in the deployment, but also from help in managing and resolving the problems and pitfalls inherent in carrying out such a project.

#### 8.2.1.2. The BCP project manager

Generally, this is the *"Risk Manager"* or the *"Security Manager"* of the organization (except for large organizations where the *"BCP Manager"* function is a full-time role). In any case, they are the bearer of the BCP project. As such, they steer the project, ensure its monitoring and smooth running, manage the network of BCP Correspondents (this organizational chart is to be sized according to the size and risk exposure of the company), chair the *"Business Continuity Plan"* Committee, consolidate data, and assist the *"Business Lines"* and *"Support Functions"* in the implementation of business continuity solutions. They are also the guarantor of maintaining the BCP in operational conditions. As such, they carry out the tests.

#### 8.2.1.3. The "Business Continuity Plan" *Committee*

The BCP Project Manager establishes a *"Business Continuity Plan"* Committee composed of the Directors (or *"BCP Correspondents"*) of all support functions and Business lines. The composition of said Committee is validated by Senior Management.

The mission of this committee is to design and implement the BCP, to validate the various stages and phases of the project that should be rolled out to each unit/department of the company through *"BCP correspondents"*.

The committee will also *"balance"* the quantified results, re-calibrate them, and compare the information provided by each department (MTPD, business impact of interrupting a given process, etc.), so as to reduce discrepancies caused by over- or under-estimation. Individual interviews with employees can produce distortions in how the severity of a service interruption is perceived across departments.

This work of homogenizing the data makes it possible to compare and consolidate all the data provided by each of the departments. Finally, this committee proposes business continuity guidelines to Senior Management.

#### 8.2.1.4. BCP Correspondents

In large organizations, it is possible that BCP relays are present at the level of each Department: these are the *"BCP Correspondents"*. Their function is to roll out all the operations for setting up a BCP at the level of their scope of responsibility (collecting information, implementing BCP principles and rules, etc.).

#### 8.2.1.5. Employees

Thucydides reminds us that *"the safety of the city depends less on the strength of its fortifications than on the firmness of mind of its inhabitants"*. This quote takes on its full meaning when applied to the field of crisis management and business continuity. Indeed, while the creation of a reference documentary corpus and the implementation of technical tools for risk management and reporting are necessary steps for setting up a BCP, it is essential that all employees possess at least a culture of risk and crisis management: safety is everyone's business.

# CONCLUSION

A company faced with a crisis must have put in place the best conditions to resume as quickly as possible a level of activity comparable to the previous state, in order to fulfill the objectives initially set. As such, the continuity strategy can no longer reside solely in a technical response or a financial transfer of risk to insurers, because of the impact on brand image and because the survival of the company depends less on its ability to compensate third parties than on its aptitude to react effectively and communicate in the face of a crisis.

Chapte

r 9

The effectiveness of business continuity arrangements in a crisis depends directly on the depth of the questioning and investigation previously conducted across the three constituent dimensions of the problem.

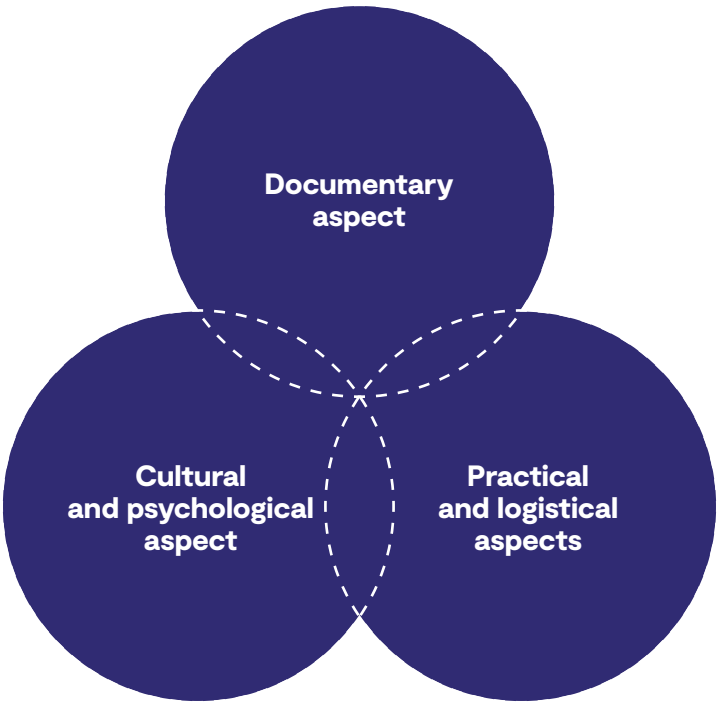
→ *"Documentary"* dimension first, which takes concrete form through the drafting of formalized and regularly updated documents, for planning the reaction to a catastrophe or a serious disaster.

→ *"Material and logistical"* dimensions, which allow teams to have the appropriate equipment and materials to respond to the problem of the destruction of this or that resource (buildings, health issues, unavailability of IT systems, etc.).

→ *"Cultural and psychological"* dimensions, finally, too often forgotten in BCP (Business Continuity Plan) issues and which, in our opinion, constitute the most important dimension. On an individual level, but also on the level of business continuity teams, it is necessary to *"Think the unpredictable,"* that is to say, to adopt the following mental posture: *"I must be ready to face an event or a deterioration of the situation that my knowledge, my experience, and my intelligence cannot imagine; I do not know what the nature of the aggression will be, but I must inventory my capabilities and my strengths to face the unknown aggression."* In addition, at the company level, it is necessary to inform and train all employees on business continuity and crisis management issues, but also on the effects of stress in order to prevent any atypical or pathogenic behavior (on an individual and collective level) on the day the crisis occurs.

In an environment marked by uncertainty and the multiplication of crises, the link between risk analysis and BCP therefore becomes fundamental.

**The 3 pillars of BCP efficiency**



# In summary,

Risk analysis is no longer limited to a preliminary exercise of ranking threats: it constitutes the backbone of the BCP, by making it possible to identify the major scenarios likely to affect critical activities and to size realistic continuity strategies. Without a fine understanding of vulnerabilities, internal and external interdependencies, and human and technical points of fragility, the BCP risks being based on inoperative hypotheses at the time of the crisis.

This requirement is particularly evident in the face of climate and cyber crises, which far exceed traditional unavailability schemes. Climate crises, by their extensive, progressive, or brutal nature, can cause simultaneous ruptures of infrastructure, supplies, and essential services, durably affecting territories, goods, and people. They call into question the usual continuity hypotheses and make it necessary to rethink fallback strategies, recovery times, and geographical redundancy needs.

Cyber crises, for their part, illustrate the critical dependence of contemporary organizations on digital technology. Their capacity for rapid propagation, their cross-functional nature, and their potential for a domino effect on internal systems and supply chains make an in-depth risk analysis essential, focused on critical assets, technological dependencies, and scenarios of loss of control or trust in data. Without this analysis, the BCP cannot guarantee either the continuity of essential digital services or a controlled restart of activities.

Business continuity must be understood as a true corporate strategy, integrated into governance and overall risk management. It constitutes a major lever for resilience, but also a key factor of differentiation and credibility. By strengthening the capacity to face climate and cyber crises, the BCP contributes to securing economic trajectories, maintaining the trust of customers, financiers, and insurers, and durably strengthening the sustainability of organizations. Conversely, those who neglect this approach expose themselves to structural weakening in a context where crises are no longer exceptions, but recurring issues.

**AD**: Active Directory - Centralized directory service for managing Windows user identities and access.

**ANSSI**: The National Cybersecurity Agency of France

**API**: Application Programming Interface

**BCP**: Business Continuity Plan

**BCPM**: Business Continuity Plan Manager

**BIA**: Business Impact Analysis

**CER**: Resilience of Critical Entities

**CERT**: Computer Emergency Response Team.

**CSE**: Social and Economic Committee

**CSIRT**: Computer Security Incident Response Team

**CVE** : Common Vulnerabilities and Exposures

**DANA**: Depresión Aislada en Niveles Altos - Isolated depression at high altitude (often referred to as a "cold drop")

**DDOS**: Distributed Denial of Service

**DORA**: Digital Operational Resilience Act - European regulation on digital operational resilience for the financial sector

**DRP**: IT Disaster Recovery Plan

**DSI**: Chief Information Officer (CIO)

**EDR** : Endpoint Detection and Response

**ENISA**: European Union Agency for Cybersecurity

**ERP**: Enterprise Resource Planning

**FSPAS**: Fire Safety and Personal Assistance Service

**GSDNS**: General Secretariat for Defense and National Security

**HRB**: High-Rise Building

**KISS**: Keep It Simple and Straightforward

**KPI**: Key Performance Indicator

**MTPD:** Maximum Tolerable Period of Disruption

**OT**: Operational Technology

**REX**: Feedback / Lessons Learned

**RIO**: Recovery of Integrity Objective. Maximum time to restore data integrity after an incident.

**RPO**: Recovery Point Objective

**RTO**: Recovery Time Objective

**SAIV** : Sectors of Vital Importance

**SIEM** : Security Information and Event Management

**SLA**: Service Level Agreement

**SOC**: Security Operations Center

**SARS**: Severe Acute Respiratory Syndrome

ABOUT AMRAE

# Anchoring risk management at the heart of organizational performance and resilience.

**Amrae** (Association for Risk Management and Corporate Insurance) brings together the main players in risk management (risk management, internal control and audit, insurance, and legal). Through its scientific committees, publications, position papers, and congress, it works for excellence in risk management, which contributes to securing corporate strategy and organizing their resilience. Amrae brings together approximately 2,000 members from 850 private and public organizations.

Informed and long-term risk management forms the foundation of corporate resilience. It aims to absorb shocks, assume responsibility, and seize opportunities, while deploying sustainable and responsible growth. Its benefits flow through companies, their ecosystem, and the entire economic fabric.

Amrae's fundamental missions are:

→ **RISK CULTURE**
→ **EXPERTISE**
→ **TRAINING & CONGRESS**

AMRAE
la Maison du risk management

36 boulevard Sébastopol
75004 Paris - FRANCE
Tel. : +33 (0)1 42 89 33 16

**amrae.fr**