EU-CIRCLE

A pan-European framework for strengthening Critical Infrastructure resilience to climate change

D4.4 CI climate related business continuity model

Contractual Delivery Date: 7/2017	**Actual Delivery Date**: 9/2017
Type: Report	**Version**: v1.0

Dissemination Level: Public Deliverable

***Statement** (max 3-5 lines on what the main point of this Deliverable)*

This is a report regarding Deliverable 4.4, which is a CI climate related business continuity model, produced in the framework of EU-CIRCLE project. In order to present a common and interrelated business continuity plan, this report takes under consideration the Resilience Framework developed in EU-CIRCLE (D4.1), incorporating all the specific characteristics of climate hazards. Through this Business Continuity Model, CIs will achieve effective and efficient allocation of resources and response to large scale climate hazards.

EU-CIRCLE is a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653824. Please see http://www.eu-circle.eu/for more information.

Preparation Slip			
	Name	Partner	Date
From	Ilias Gkotsis George Eftychidis	KEMEA	28/08/2017
Reviewer	Nenad Petrovic	UVG	30/08/2017
Reviewer	A. Sfetsos	NCSRD	31/08/2017
For delivery	A. Sfetsos	NCSRD	1/9/2017

Document Log			
Issue	Date	Comment	Author / Organization
V0.1	5/12/2016	TOC of D4.4 for comments	KEMEA
V0.2	7/5/2017	Updated TOC and initial contribution	KEMEA
V0.3	31/7/2017	Questionnaires and contribution per sector	Fraunhofer, NCSRD, GMU, UNEXE, TORB, ARTELIA, CEREN
V0.6	28/8/2017	Integration, Elaboration, Ready for review	KEMEA
V0.7	30/8/2017	Internal review	UVG
V0.8	31/8/2017	Internal review	NCSRD
V1.0	1/9/2017	Final version	KEMEA

Executive Summary

The main purpose of this document is to present the Business Continuity model that has been created for EU-CIRCLE and will be used during the case studies. Mainly it is linked with D4.3, which presents the final version of the analytical framework for resilience of critical infrastructure in the context of EU-CIRCLE and proposes an analytical framework and a conceptual model for critical infrastructure resilience to disaster impacts, in the short run, and climate change, in the long run. Additional link has been established with D1.5, D3.4, D4.1, D4.2 and D4.5. Finally, it will provide also input for D4.6 regarding adaptation to climate hazards model. Further to EU-CIRCLE deliverables, the work in this deliverable is aligned with several BC standards and guidelines, such as ISO 22301.

In this direction, in this document a background analysis has been performed, introducing to Business Continuity Management System and climate change sector specific climate impacts. BCM covers the whole lifecycle of disaster prevention and recovery. Guidelines are presented, in order to provide a planned and controlled method of anticipating and responding to events that are likely to interrupt key business activities. Also, guidelines on adaptation of BCM to climate change are presented for each part of the BCM cycle and its procedures.

Regarding the BCM and its adaptation, EU-CIRCLE has designed a specific questionnaire which has been distributed and completed by CI owners and stakeholders. Information collected have been further analysed and combined with the above guidelines the BC model have been shaped. This model will be used in EU-CIRCLE case studies, through CIRP end-to-end collaborative modelling environment, as BC strategies and solutions aiming to reduce the recovery time after an unplanned event.

Contents

1 Introduction

1.1 Background

Many business activities and the resources that support them depend on aspects of the weather or climate and can be disrupted by severe weather and its impacts. A survey by the Chartered Management Institute found that 54 % of businesses reported being disrupted by severe weather in 2012, making it the number one cause of business disruption for the fourth year running. Most recently the winter of 2013/14 has been reported as the wettest winter in England and Wales since records began with heavy rainfall and storms causing widespread flooding and disruption [5].

It is not possible to say that climate change alone is causing the increase in these disruptive events. Other changes are putting more value at risk, such as increasingly lean and complex supply chains and development in vulnerable locations. However, what is clear is that both the frequency of severe weather events and the value at risk are increasing. This has implications for business continuity (BC) and broader business objectives. For example:

- Increasing frequency of heavy rain and rising sea levels will contribute to an increasing frequency and severity of flooding causing damage or loss of access to business premises and disruption to staff travel, supply chains or critical infrastructure
- Rising temperatures can lead to a decline in productivity through overheating of work places and disruption or quality issues where processes or products are temperature sensitive
- Increasing frequency or severity of drought, putting pressure on water demand and potentially leading to higher costs or a lack of availability. Low flows in rivers will also put pressure on the quality of water discharged under effluent consents.

Organizations need to be prepared for severe weather regardless of the cause. This can involve making physical, operational or strategic changes and includes actions that tackle the likelihood of damage or disruption as well as those aimed at managing its impacts. It can include preparing for opportunities as well as threats.

Recent research on the impact of an unplanned event has revealed some worrying trends. One in five of all organisations will suffer fire, flood or storm, power failures, terrorism and hardware or software disaster. Of those without a business continuity plan [14]:

- 43% will never reopen
- 80% will fail within 13 months
- 53% of claimants never recoup the losses caused by the disaster
- 90% of businesses that lose data from a disaster are forced to shut down within 2 years of the disaster
- 50% of businesses experiencing a computer outage will be forced to close within 5 years
- Major systems downtime costs 15% of organisations over £50,000 per hour

1.2 Sector specific issues

All kinds of infrastructures – transport, power grids, water supply, sewage, buildings and dykes – are all crucial for the functioning of the economy and society in Europe, now and in the future. One of the policy

areas of the European Union is to assess infrastructures for resilience to current risks and future climate changes.

Evidence collected by the European Commission indicates that climate impacts on infrastructures will vary across the EU depending on their geophysical risk exposure, the existing adaptive capacity and resilience, and the level of regional economic development.

Climate impacts show regional and seasonal patterns, e.g. north/south, winter/summer, urban/rural/coastal, requiring complex, site-based analysis of different trends and impact patterns.

Climate change will also affect the environmental and social systems around infrastructure assets and their interactions with these systems. This highlights the importance of acting in an integrated, cross-sector way on climate risks and resilience.

Vulnerability is also strongly sector specific and closely linked to the technology used for construction and operation. For example, less precipitation causes decreased efficiency of hydro-power plants. Cities and urban areas play an essential role in providing infrastructures to citizens and are sensitive to many impacts. Many of these impacts are accelerated or accentuated in built-up areas that may create unique micro-climates in terms of temperatures, wind, and precipitation. Infrastructures in coastal areas as well as off-shore installations, such as transmission lines and wind turbines, will be particularly affected by sea level rise, by changes in ocean currents and by coastal erosion.

In this section an overview of resilience from each CI sector point of view is presented, in order to describe the similarities and deviations in the approach of each one [6,7].

1.2.1 ENERGY

Energy is at the core of economic and social activity. As the European Environmental Agency (EEA) [13] states, energy is essential for the generation of industrial, commercial and societal wealth. It also provides personal comfort and mobility. However, energy production and consumption place considerable pressure on the environment: greenhouse gas and air pollutant emissions, land use, and waste generation.

A European Commission White Paper [10] published in 2009 outlines the main direct impacts of climate change in the energy sector in terms of both supply and demand.

The projected impact of climate change on precipitation and glacier melt indicate that hydropower production could increase by 5% or more in northern Europe and decrease by 25% or more in southern Europe. Decreased precipitation and heat waves are also expected to influence negatively the cooling process of thermal power plants. On the demand side, increasing summer peaks for cooling and impacts from extreme weather events will affect in particular electricity distribution.

Enhancing the EU's resilience to the impacts of climate change also means the chance to invest in a low-carbon economy, for instance, by promoting energy efficiency and the uptake of green products [8]. In 2014, the Commission presented a framework for climate and energy policies in the period 2020 to 2030, setting out ambitious targets for greenhouse gas emissions reduction and renewable energy as part of the Union's transition to a competitive low carbon economy. For example, by 2020, at least 20% of the energy supply in the European Union should come from renewable sources.

1.2.2 ICT

Many improvements in climate resilience frequently offer additional benefits (such as cost savings, improved efficiency, or resource efficiency). In ICT, as elsewhere, adaptation actions to address climate risks will rarely (if ever) be undertaken as a response to climate change alone. Adaptation decisions should not be taken in isolation since they should represent a proportionate response in the context of dealing

with the whole range of current and future risks affecting organisations in the sector, whether that is at the level of an individual ICT provider looking to improve the quality of the service it offers, or at the level of an end-user looking to ensure business continuity [1].

Opportunities for building climate resilience in the sector, will involve action on the part of customers, telecommunications and IT service providers, government, and a number of wider stakeholders at national and local levels. The main areas for action are presented hereafter:

- Enhancing climate resilience of the network
- Enhancing climate resilience of devices
- Taking advantage of rapidly developing technology
- Improving planning and business processes
- Improving responses to weather events

Regarding planning and business process, organisational protocols for system back-up and information security already exist. Good practice in this regard will also provide resilience, at an organisational level, against disruption from climate events. The adoption of business continuity standards by both providers and consumers of ICT will help, though this may need specific consideration in the context of climate change.

Furthermore, many organisations can cope in the very short-term with a system failure or system outage: they may have back-up manual systems, paper records or alternate delivery plans which enable them to provide a level of service. For business continuity purposes organisations should have regular back up systems and disaster recovery mechanisms in place anyway.

In a nutshell, ICT infrastructure providers will have a key role to play in this issue of business continuity. While providing links to individual homes (and having contracts with individual home occupiers), providers may need to ensure the resilience of their systems can address corporate levels of service and reliability rather than domestic ones.

1.2.3 WATER

A rise in global temperatures will lead to an intensification of the hydrological cycle, causing more severe dry seasons and wetter rainy seasons, as well as more frequent extreme events.

According to the European Environment Agency, the main climate change consequences related to water resources are increases in temperature, shifts in precipitation patterns and snow cover and a likely increase in the frequency of flooding and droughts.

Precipitation changes are expected to differ from region-to-region with some areas becoming wetter and some dryer.

Annual precipitation trends in Europe indicate that northern Europe has become 10%-40% wetter over the last century, whereas southern Europe has become up to 20% drier.

Changes in Europe's water resource will have consequences for several sectors particularly agriculture, forestry, energy and drinking water provision.

Activities that depend on high water abstraction and use, such as irrigated agriculture, hydropower generation and use of cooling water will be affected by changed flow regimes and reduced annual water availability.

1.2.4 TRANSPORT

Climate change threatens to compromise transport services that are indispensable for Europe's economy and society; climate impacts that cause changes in the organisation of society and economy - such as different tourist destinations or agricultural productions – can have an impact on transport demand.

A report by the European Environment Agency (EEA) on Adaptation of transport to climate change in Europe [12] outlines these on the challenges for the transport sector which include:

- Rising temperatures and extended heat-wave periods increasing the problems of rail buckling, pavement deterioration and thermal comfort for passengers in vehicles.
- Weather extremes generating floods or landslides leading to delays, interruptions and detouring needs.
- Sea-level rise threatening harbours and other transport infrastructure and services in coastal areas.
- Air transport challenged by changing wind patterns, flooding of airport infrastructure and other weather events.

1.2.5 PUBLIC (EMERGENCY SERVICES, HEALTH, GOVERNMENT)

Health

The World Health Organisation reports that climate change related variations to weather patterns such as more intense and frequent extreme events, changes in water, air, food quality and quantity, and to ecosystems, agriculture, livelihoods and infrastructure, will all have an impact on health.

Heat, flood and drought-related mortality and morbidity may increase; changes in the distribution of plant species and animals are likely to contribute to changing ranges of infectious diseases and allergic disorders; higher concentrations of ground-level ozone and particulate matter in urban areas may increase the frequency of cardio-respiratory and cardio-vascular diseases.

A report on the impacts of climate change on human health [11] published by the European Commission Joint Research Council also shows that coastal flooding and high sea-level rise scenarios could have significant negative effects on mental health, in addition to high economic costs.

The WHO-Europe report [15] highlights the critical need of health systems to develop and implement adaptation and mitigation strategies and to strengthen a range of key areas of work, from disease surveillance and control and research, to disaster risk reduction, which are essential elements of the capacity for rapid detection of and action to protect health from climate change.

Buildings

Buildings can be vulnerable to climate change. In the future there may be an increase in the risk of collapse, declining state and significant loss of value as a result of more storms, snow or subsidence damage, water encroachment, deteriorating indoor climate and reduced building lifetime. The European Commission aims to increase the climate resilience of infrastructure, including buildings. New and existing buildings need to be assessed for resilience to current risks and future climate changes, and planned or upgraded accordingly.

1.3 Deliverable Methodological Framework

Accordingly, the objective of this report is to develop a Business Continuity Model for Critical Infrastructures under climate pressures by;

i) presenting a business continuity plan based on existing operating principles and best practices

ii) presenting how critical processes will continue operating to a minimal under recovery management

iii) examining the feasibility of CI owners in specific regions to have a common and interrelated business continuity plan

In order to develop and implement the BC model of EU-CIRCLE, inputs and links with different work packages and deliverables has been established. As indicated in the following figure from D4.3, contributions particularly from the following are needed: D1.5 with regards to the methodology and particularly integrates the findings D3.1, D3.4, D4.2, D4.5 and D4.6.

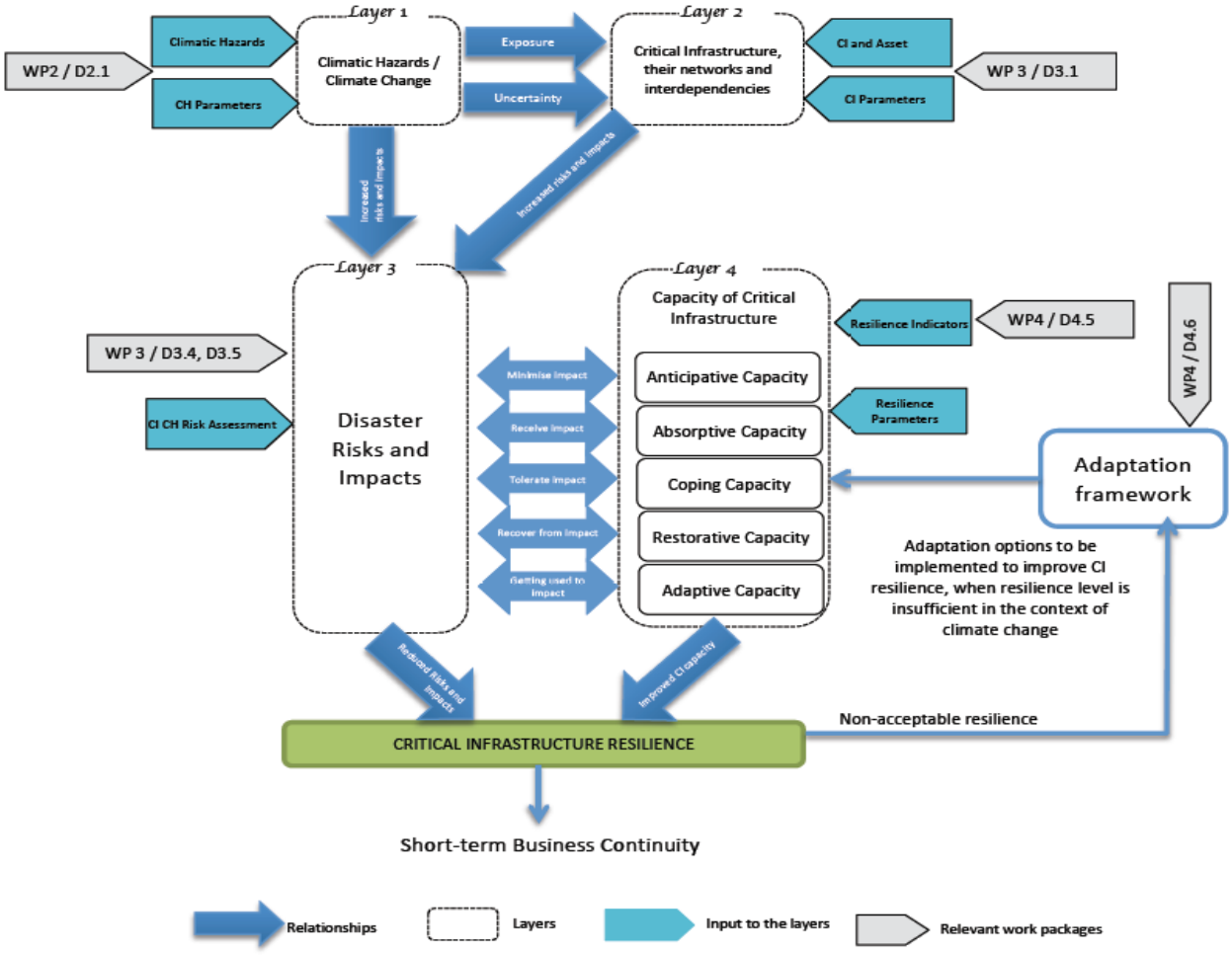

Figure 1 EU-CIRCLE Resilience Framework's inputs and relationships

By using the framework as described in detail in D4.3, in combination with D4.2 prioritization module and D4.5 Resilience indicators, CI asset stakeholders such as CI operators and service providers can: (i) quantitatively compare different hazard response strategies for the same CI asset; (ii) compare the system performance of different CI assets to similar hazard events; and/or (iii) extend this analysis to compare the system performance of CI network and network of networks.

Figure 2 EU-CIRCL Resilience Framework modules

As depicted in the figure above, the following modules will be used:

- Adaptation module: provides a mechanism for comparing adaptation options
- Business continuity module: provides a framework to consider the different options required to increase/maintain resilience in the face of events
- Cost/Benefit module: provides a framework to compare and contrast increase in resilience with investments

Developing a simulation approach to modelling impacts from shocks like hazard events is increasingly important for choosing the most effective strategy for investing in protective measures if a shock happens. Although many preventative measures may look to be cost-effective in certain conditions, decision makers need tools to help them rank adaptation option or choices to efficiently allocate limited budgets. This has been clearly indicated in D1.5 and D4.6 Adaptation module as an essential tool in EU-CIRCLE.

2 Business Continuity Management

As defined by Japan International Cooperation Agency and introduced in [3], the Area BCP is a framework and direction of disaster risk management by stakeholders. These stakeholders include individual enterprises, industrial area managers, local authorities and administrators of the infrastructures in order for business continuation of the industrial agglomerated area as a whole.

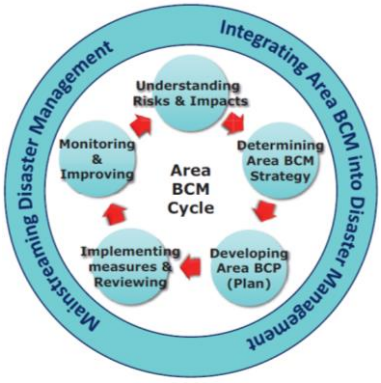

Figure 3 Area BCM cycle

Further to the above, in [2] the definition of Area Business Continuity Management (Area BCM) is proposed as a cyclic process of sharing risk information or impact estimation, determining the strategy, developing the Area BCP, implementing preparedness measures and effective recovery actions and monitoring to continuously improve the Area BCM system, in coordination among stakeholders, in order to improve the capability of effective business continuity in the area (Figure 1).

The formulation of the Area BCP in the three pilot areas was conducted by JICA study team who facilitated the discussion of the stakeholders to take steps as Figure 2 which is designed by the team referring to the standard procedure of the ISO22301.

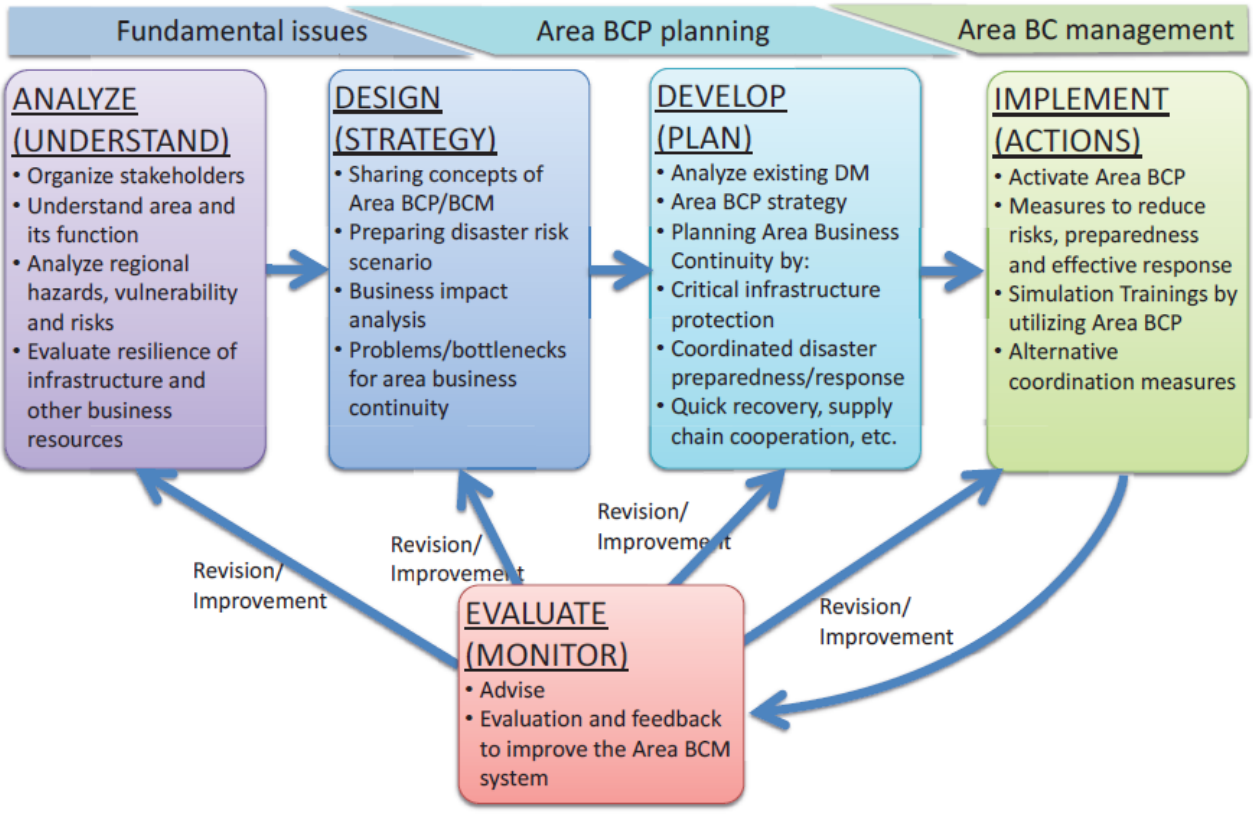

Figure 4 Steps to formulate Area BCP and to implement Area BCM

2.1 Business Continuity Management

Business Continuity Management (BCM) is a business-owned, business-driven process that establishes a fit-for-purpose strategic and operational framework that:

- Proactively improves an organization's resilience against the disruption of its ability to achieve its key objectives.
- Provides a rehearsed method of restoring an organization' ability to supply its key products and services to an agreed level within an agreed time after a disruption.
- Delivers a proven capability to manage a business disruption and reputation and brand.

2.2 BCM relationship with Risk Management

BCM is complementary to a risk management framework that sets out to understand the risks to operations or business, and the consequences of those risks.

Risk Management seeks to manage risk around the key products and services that an organization delivers. BCM, by focusing on the impact of disruption, identifies those products and services on which the organization depends for its survival, and can identify what is required for the organization to continue to meet its obligations.

Through the application of BCM, an organization is capable of recognize what actions have to be implemented before an incident occurs in order to protect people, premises, technology, information, supply chain, stakeholders and reputation. With this analysis, the organization can then take a realistic view on the responses that are likely to be needed as when a disruption occurs, so it can be confident that it will manage an incident without an unacceptable delay in delivering its products or services.

2.3 Benefits of a BCM program

The benefits of an effective BCM program are that the organization:

- Is able to proactively identify the impacts of an operational disruption.
- Has in place an effective response to disruptions which minimizes the impact on the organization.
- Maintains an ability to manage uninsurable risks.
- Encourages cross-team working.
- Is able to demonstrate a credible response through a process of exercising.
- Could enhance its reputation.
- Might gain a competitive advantage, conferred by the demonstrated ability to maintain delivery.

2.4 BCM lifecycle

The BCM lifecycle comprises six elements:

1. BCM program management

Program management enables the business continuity capability to be both established (if necessary) and maintained in a manner appropriate to the size and complexity of the organization.

2. Understanding the organization

The activities provide information that enables prioritization of an organization's products and services and the urgency of the activities that are required to deliver them. This sets the requirements that will determine the selection of appropriate BCM strategies.

3. Determining business continuity strategy

Determining business continuity strategy enables a range of strategies to be evaluated. This allows an appropriate response to be chosen for each product or service, such that the organization can continue to deliver those products and services.

4. Developing and implementing a BCM response

Developing and implementing a BCM response results in the creation of a management framework and a structure of incident management, business continuity and business recovery plans that detail the steps to be taken during and after an incident to maintain or restore operations.

5. BCM exercising, maintaining and reviewing BCM arrangements

BCM exercising, maintenance, review and audit leads to the organization being able to:

- Demonstrate the extent to which its strategies and plans are complete, current and accurate.
- Identify opportunities for improvement.

6. Embedding BCM in the organization's culture

Embedding BCM in the organization's culture enables BC to become part of the organization's core values and instils confidence in all stakeholders in the ability of the organization to cope with disruptions.

3 Business Continuity Planning Guidelines

3.1 Starting a BCM project

This first phase of the a BCM project is focused in the identification of the steps that will help to develop a Business Continuity Plan. All the steps set the principles to the success of the project. These steps are:

i. Definition of the scope

ii. Business Continuity Management Policy

iii. Disclosure and presentation

3.1.1 Definition of the scope

Initially, during a BCM project, and as in any project, the scope is identified in order to achieve a respective gaol. In this direction, an Impact Analysis is a prerequisite. To perform this analysis, first aspects such as a) organisational areas affected, b) technological structure, c) locations of assets and d) personnel involved in each operation, should be defined. The areas that can be affected in any infrastructure are the following:

- Buildings/Equipment
- Business units
- Processes or services
- Information/data
- Technological/non-technological resources
- Personnel
- Providers

The next step is to set the parameters that will be considered for the asset evaluation, such as impact level, recovery time objectives, maximum time of return period, maximum degradation levels for services, scale of dependencies.

Finally, requirements, either legal or organizational, must be identified. In many cases services and processes that are analyzed and affected may be subject to legislation, laws, organization rules or standards adopted.

3.1.2 Business Continuity Management Policy

Following the last phase of scope definition, regarding legal and organizational requirements, in this step, the organization should develop a tailor made BCM policy, aligned with the objectives of the organization. To create a BCM policy the following requirements must be taken into consideration:

1) Corporate policy (security, information, human resources, etc)

2) Specific policies (physical, operational, etc)

3) Standards (ISO, BS, etc)

4) Procedures (audit, crisis management, emergency, etc)

The organization should determine and provide the resources needed to establish, implement, operate and maintain the BCM and also have to assign and document the roles, responsibilities, competencies and authorities of the BCM.

3.1.3 Disclosure and presentation

As a final step of the first phase of a BCM project, the level and type of information that should be shared and updated with the top management of an infrastructure must be decided. The main objective here is to make the direction aware of the reasons and benefits of the project, that will guaranty their support in the implementation phase.

Once the support by the top management is obtained, it is necessary to do something similar (e.g. through a meeting) with the people that will participate in the project directly or indirectly, letting them know the expectations, their tasks and involvement in the implementation phase.

3.2 Business Impact Analysis Methodology

Under the Business Continuity Management Cycle, the objective of the Business Impact Analysis is to identify critical services, involved processes, resources, and suppliers needed to support those services.

A Business Impact Analysis is[1] "a process of analyzing business functions and the effect that a business disruption might have upon them".

The main objective of a Business Impact Analysis is to identify:

- Critical services and business processes.
- The activities that support those critical services.
- The impacts activity disruption has on critical services and how they vary over time.
- The maximum assumable interruption time for each activity
- The maximum time to recover the activity since an interruption occurs
- The maximum time to resume normal operating levels
- Categories of activities according to their criticality and recover priority
- Dependencies for each activity, including suppliers and subcontractors
- The necessary resources to resume critical activities

[1] Definition based on Good Practice Guidelines 2010 © Business Continuity Institute and BS25999 Parts 1 and 2 © British Standards Institution BS25999

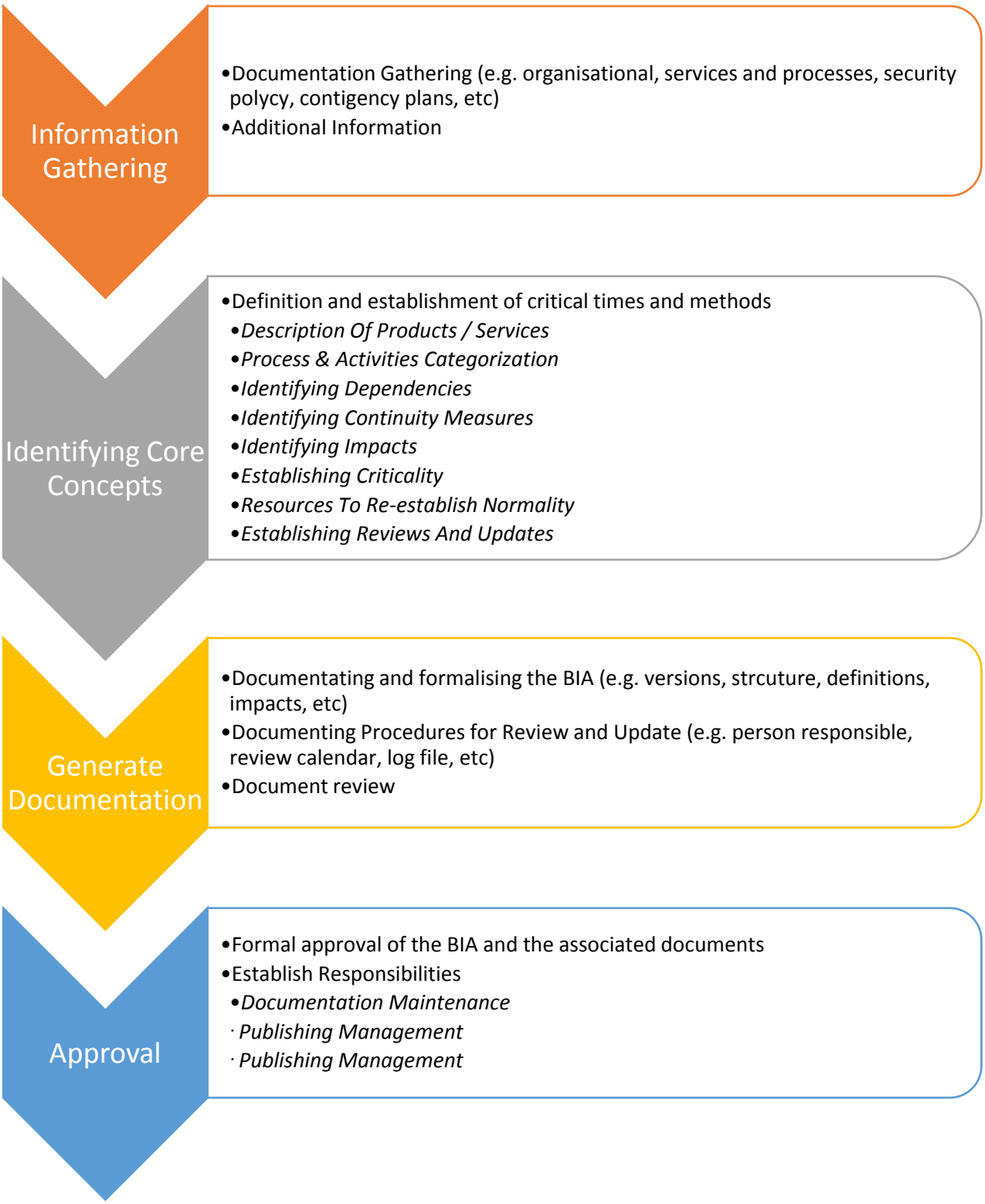

Figure 5 BIA Methodology

3.3 Risk Management Methodology

As in the previous section for BIA, the CI operator/owner should have a Risk Management (RM) methodology, in order to identify and manage the principal risks that services are exposed. The same steps are followed, as depicted in Figure 4 below.

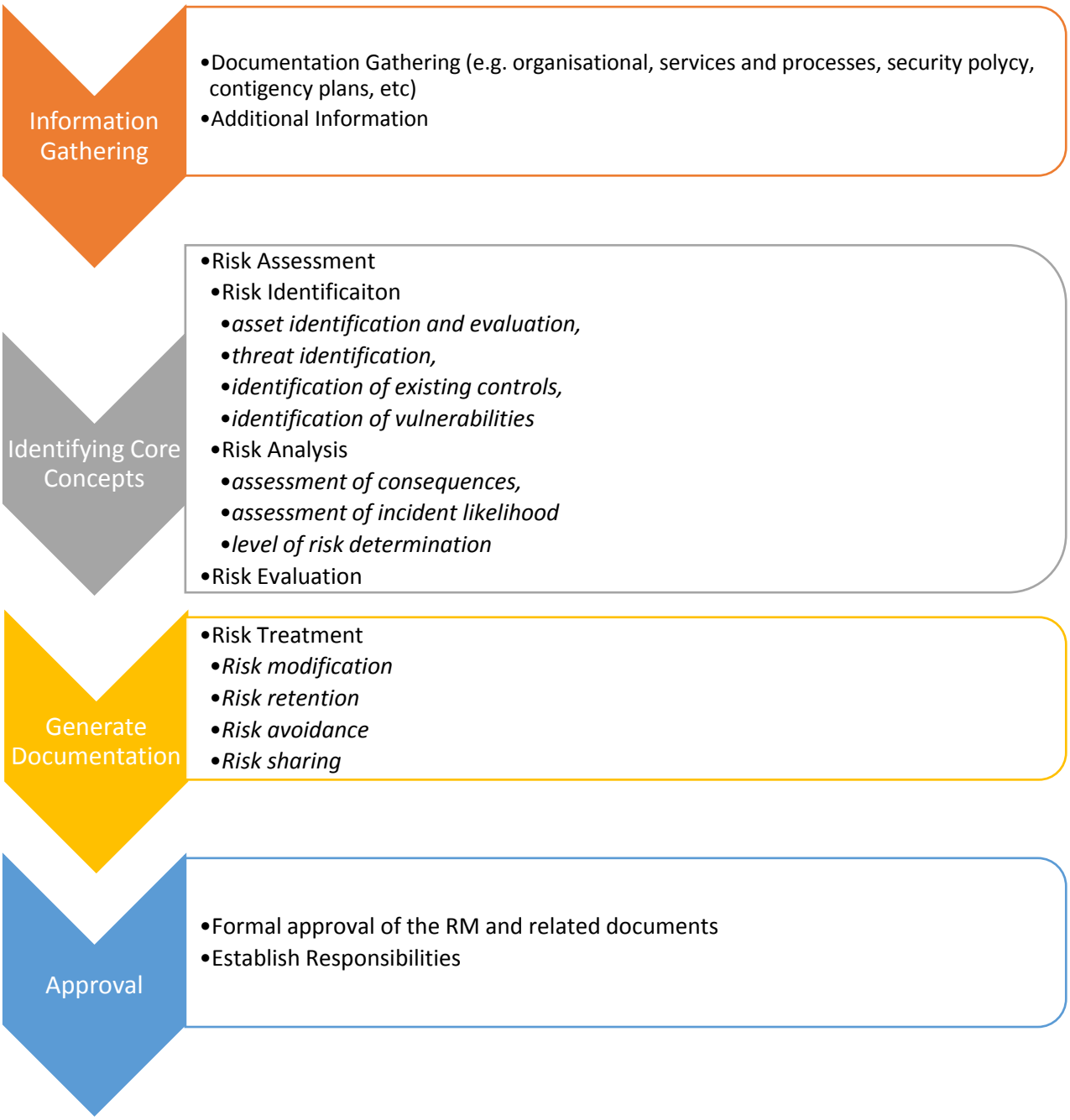

Figure 6 Generic Risk Management Methodology

The RM process aids decision making by taking into account uncertainty and the possibility of future events or circumstances (intended or unintended) and their effects on agreed objectives. The RM process flow is depicted in the Figure 5 below.

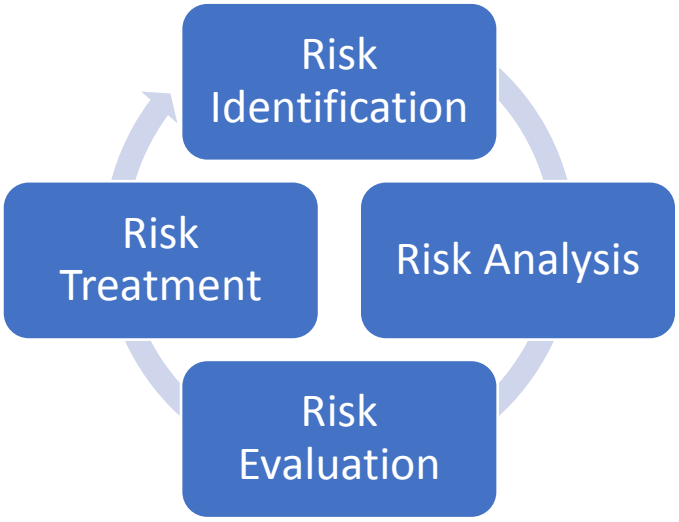

Figure 7 Risk Management process flow (based on ISO 27005:2011)

Once the context (reasons to perform the RM process, scope, organization, methodology and assessment criteria) is known, the Risk Assessment phase (consisting of Risk Identification, Analysis and Evaluation steps) may be carried out based on the chosen methodology. This phase provides those risks threatening the Information Systems (IS) and sets the basis for the development of the best suited Risk Treatment strategy, that management should ratify and support.

Risk Analysis is the consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of Critical Infrastructure. Risk Analysis could be made in parallel with the BIA or separately and should consider the following aspects:

- Assets
- Threats
- Vulnerabilities
- Impact
- Likelihood
- Risk / Residual Risk
- Controls

3.4 Business Continuity Strategy

The main objective of the Business Continuity Strategy is to define alternatives and strategies to follow in case of an interruption in the critical services to enable:

- Implement the appropriate measures to reduce the possibility of an incident or the potential effects of such incidents.

- Identify the necessary resources to restore the critical services in the established time.
- Implement effective solutions to restore as soon as possible within the recovery time objective defined for the critical services.

Also, the Business Continuity Strategy takes into account the mitigation measures already implemented by the organization and the services identified as no critical, but due to its dependencies with other critical services must be considered in the adoption of continuity strategies.

The Business Continuity Strategies should consider:

- The conclusions of the BIA and the Risk Analysis
- The maximum tolerable periods of the critical services
- The cost of the strategy implementation
- The consequences of non-implementation of any business continuity strategy

The Business Continuity Strategy Methodology is depicted in steps in Figure 6

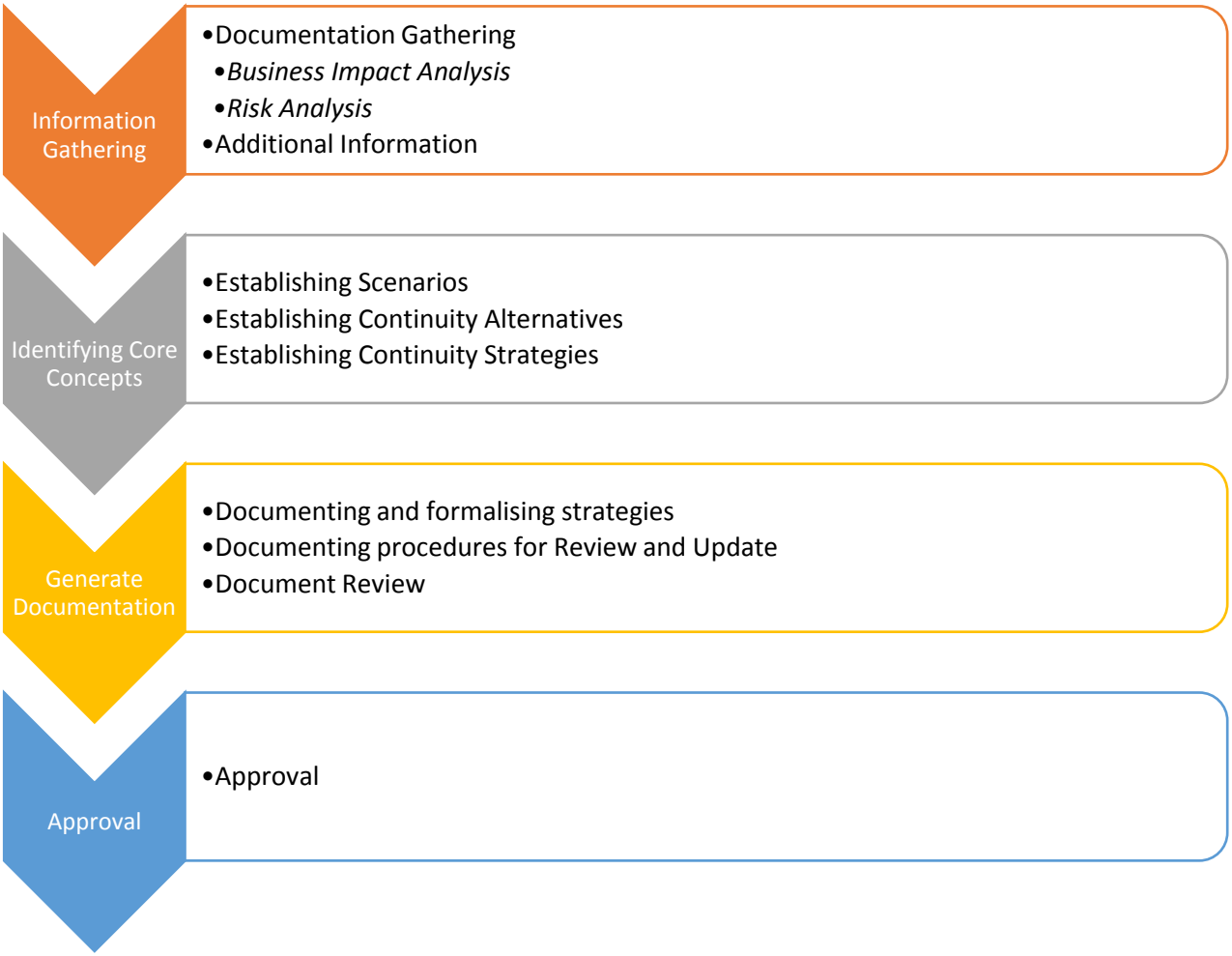

Figure 8 Business Continuity Strategy Methodology

The second and core concept of the above methodology, is to define continuity scenarios, alternatives and strategies, which are further analysed in the following sections. In order to group the results, the following categories of unavailability should be used:

- Unavailability of locations
- Unavailability of Human Resources
- Unavailability of Information Technology
- Unavailability of data
- Unavailability of supplies

3.4.1 Establishing Scenarios

To establish the strategies, the first step is to identify unavailability scenarios to study, which are selected depending on the resources and interests of the organisation. The identification of scenarios has to be done with the BC managers and must respond to the contingency assumptions that have been assumed. Examples of scenarios to be considered are presented in the following table.

Unavailability scenarios for BC	
Unavailability of Locations	• Main building • Alternative building • Offices • Data centre
Unavailability of Human Resources	• Personal • Continuity of Operations • Knowledge
Unavailability of Information Technology	• Applications • Computer platforms • Communications • Telephony
Unavailability of Data	• Data (total or partial loss)
Unavailability of Supplies	• Suppliers

3.4.2 Establishing Continuity Alternatives

The next step is to determine what alternatives are available for each of the scenarios considered above. In each case, the following recovery alternative items should be considered:

Alternatives for Continuity	
Infrastructure	• Alternative buildings • Collaboration with other companies • Estate Agreements • Alternative CPD • Hot site • Cold site • Warm site • Mobile site • Telecommuting

Alternatives for Continuity	
Logistics	• Transportation • Material • Suppliers
Recovery Equipment	• Designed Personnel • Alternative Personnel • Collaboration with other companies
Technologies Implemented	• Systems • Cluster • Virtualization • RAID • SAN • NAS • Data Replication • Replication • Cloud-computing • Telephony and Communications • Redundancy cabling and systems • Redundancy suppliers • Bandwidth and capacity
Unavailability of Supplies	• Suppliers

3.4.3 Establishing Continuity Strategies

Once the continuity scenarios and the available resources are determined, the strategies to follow for each continuity scenario should be established. The following aspects should be considered for each continuity strategy:

- **Purpose:** The purpose of the solution.
- **Description:** Details about the solution
- **Resources:** Whether it can be implement internally or help from third parties is necessary

The Continuity Strategies should be based on the resources and facilities of the organisation. In some cases, there may be a lack of them. For this reason, the services and assets that must recover should be identified and reflected through a plan defining the objective, duration, effort, cost and implementation phases (immediate, short, medium, long).

Finally, with the establishment of continuity strategies, the core task of Business Continuity Strategy has been finalized, followed by documenting and formalizing the strategies, documenting the procedures for reviews and updates and finally approving the strategies, documents and responsibilities.

3.5 Introduction to Plans and Operational Procedures

The main objective of this phase is to establish the operational plans and procedures that configure the Business Continuity Plan. These plans and procedures will establish the way to operate under a contingency or a crisis situation.

The activities of this phase cover the following aspects:

- **Prevention**: Implementation of security measures to avoid improper dealing of security incidents.
- **Response**: Phase of implementation of contingency detection and decision making.
- **Recovery**: Manage critical situations to work with an operational capacity with minimal impact and dimensioned
- **Restoration**: Return to the normal way of operating.

The methodology for Plans and Operational Procedures consist of the following steps:

1. Information/Documentation Gathering
2. Identify Requirements for Plans and Procedures
    a. Prevention Requirements
    b. Response Requirements
    c. Recovery Requirements
    d. Restoration Requirements
3. Generating Plans and Procedures
4. Plans and Procedures Approval

Below the tasks of the second step for identification of requirements for plans and procedures, are presented in detail.

3.5.1 Prevention Requirements

The objective of this phase is to implement security measures to avoid improper dealing of security incidents as far as possible, which would cause a need to activate the Business Continuity Plan (BCP).

Based on the results of the BIA and Risk Analysis, the organization should identify and implement controls or security measures:

- Reduce the likelihood of critical activities suffering interruptions
- Reduce the time of a possible interruption
- Limit the impact a shutdown of critical activities can have on the organisation
- Increase the strength of the business by eliminating single points of failure

The organisation must develop a plan of action that includes the actions the company intends to take to prevent and avoid as far as possible the risks that impact the availability of operations.

Besides, the fact of implementing these preventive security measures can become a cost saving, by reducing the possibility of having to face greater evils that would mean an extra expense.

The process of identifying and implementing security measures should be based on a balance between the following factors:

- Risk mitigation
- Cost of implementing the security measures
- Benefits of implementation

Instead of waiting for a disaster to affect the organisation to see how it recovers, preventive measures should be applied in order to increase the strength of its activities against possible impact previously identified in the BIA.

Examples of preventive measures are:

- Use of robust construction materials.
- Redundancy of computer systems and communication lines.
- Contracting insurance with different degrees of coverage.
- Backup information that supports a critical activity of the organisation.
- Enhanced fire detection and fire fighting.
- Intrusion prevention and access control systems.
- Alarm and monitoring.

3.5.2 Response Requirements

The objective of this phase is to implement the plan taking into consideration contingency detection and decision making. The response phase occurs when a system disturbance or interruption is detected or appears to be imminent. This in turn consists of two activities:

a) Notification procedures, which should be documented in the plan for both intended and unintended actions. Procedures should also be securely stored in different formats (e.g. electronic, paper) and locations to ensure being able to access them when needed. Reporting methods to be used are those that the company can provide in each case. Possible means may be by phone, pager, email, messaging, etc. Automated information systems may require an initial investment and training for people who will use it, but they normally ensure quick and accurate delivery.

b) Plan activation, which should be triggered by indicators such as

   i. Extent of damage to systems (e.g. physical, operational or cost) precludes continued operations

   ii. The criticality of the system to the organisation's mission

   iii. Deviations from the planned RTO

   iv. Safety of personnel is at stake

Upon completion of the response phase, the BCP personnel should be ready for carrying out the recovery of the system functions. Personnel to be notified in each case should be clearly identified and referred in the plan. In some cases, notifications can be sent to external organisations or other members, which could be affected.

Furthermore, the information relayed to those being notified should be documented in the plan. Based on the detail and the recipient, different information may be included, such as the nature of the incident, estimated break out time, actions, procedures, etc.

Finally, the incident evaluation report should be completed, determine the impact to the system, in order to notify the appropriate personnel to proceed with recovery.

3.5.3 Recovery Requirements

The objective of this phase is to achieve a situation in which the processes have been identified as critical and to work with an operational capacity in order to enable business continuity with minimal impact and dimensioned.

At this stage, formal recovery operations should have been enabled, the evaluation of the consequences of the incident completed, the staff notified, and appropriate teams mobilised.

The recovery phase activities focus on implementing recovery strategies to restore system capabilities, repair damage and resume operational capability in the original or alternate location, according to the definition in the BCP.

At the end of the recovery phase, the information system should be able to perform the functions specified in the plan. It is likely that only the system resources identified as high priority in the BIA were recovered at this stage.

3.5.4 Restoration Requirements

The objective of this task is to return to the normal way of operating, if possible.

This task defines the actions to be taken to test and validate system capability and functionality. During this task, recovery activities are completed and normal system operations are resumed.

If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to meet system processing requirements.

This phase consists of two major activities: the validation of a successful recovery and the deactivation of the plan.

The validation of recovery typically includes these steps:

- Concurrent Processing. Concurrent processing is the process of running a system at two separate locations concurrently until there is a level of assurance that the recovered system is operating correctly and securely.
- Data Testing Validation. Data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely and are current to the last available backup.
- Functionality Testing Validation. Functionality testing is a process for verifying that all system functionality has been tested and the system is ready to return to normal operations

At the successful completion of the testing validation, personnel in charge of BCP will be prepared to declare that restoration efforts are complete and that the system is operating normally.

Deactivation of the plan is the process of returning the system to normal operations and finalising restoration activities to prepare the system against another incident. Restoration activities include:

- Notifications. Upon return to normal operations, users should be notified by the person in charge of the BCP using predefined notification procedures.
- Cleaning. Cleaning is the process of cleaning the workspace or the dismantling of the temporary recovery locations, returning manuals or other documentation to their original locations.
- Offsite Data Storage. If storing data offsite is used, procedures for returning backups or recovery of the installation media to location offsite data storage should be documented.
- Data Backup. As soon as reasonable following restoration, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup should be stored with other system backups and comply with applicable security controls.

- Event Documentation. All recovery and restoration events should be well documented, including actions taken and problems encountered during the recovery and restoration efforts

Once all processes have been completed and documentation has been updated, the BCP can be formally deactivated. The announcement of the deactivation should be sent to all those involved directly or indirectly with the BCP for its information.

3.6 Exercising the Business Continuity Plan

Previously to the exercise of the BCP, it is necessary to compile and analyze each of the components that will be affected during the test.

As a result of good analysis in the previous phases, it will be obtained a series of exercises that will test the validity of the Business Continuity Plan.

The following items describe different aspects to review before an exercise:

- Review and evaluation of the Plans, that will be part of the test in order to define the objectives and motivators for conducting the test
- Scenario definition
- Identification of critical Services, based on the type of scenario defined previously
- Analysis of procedures and recovery actions, that participants will use during the test
- Identification of stakeholders, that are required to carry out the plans and procedures

Also, the development of the following actions is needed before the exercise:

- Identification of type of exercise, depending on the scope (e.g. unit, modular or global) and the method used (e.g. hypothetical, procedural, operational or integral)
- Development of a schedule, with meetings to consolidate concepts and interdependencies betwwen plans, procedures and services
- Definition of Test directive
- Organisation of the design and evaluation team
- Development of an incident Check list, providing indicators to compare with previous tests
- Identification of expected actions, arising from the review and analysis of previous plans and procedures
- Identifying points for improvement

Following the above, the next step is the test execution which intends to implement the aspects analyzed and reviewed in the analysis phase. This step consists of two blocks,

a) one of submission and opening of the trial in which the objectives to be achieved are explained, aim to ensure that all participants report the completion of the same and distribute the plans and procedures.

b) and a second one of support to actions taken and gathering of related evidence (e.g. time, status, location, action, person, action, comments)

Once the test is completed, there will be a review of it on which to evaluate the achievement of the objectives and goals set out in the definition of the test.

Teams will meet after the test to discuss general comments, ideas, suggestions to be made and specific changes to be introduced.

Evaluating the performance of the equipment to respond to the crisis, identifying ways to improve the plan and the level of preparedness of the team, is necessary. This will involve meetings with individual team leaders to discuss concrete proposals and changes that improve the environment and plan future tests.

The documentation obtained with the results of the test and other documentation changed as consequence of these results, must be finally approved.

3.7 Maintain and Review

The maintenance program is used to ensure that the plan is still valid despite the possible changes that could be made in the business process. Maintenance is a process of updating plans based on changes happened within the organization, whether internal or external.

Preventive and corrective actions should be differentiated:

- Corrective actions can come from an audit or an opened non-compliance.
- Preventive actions come from the maintenance process or an audit.

3.8 Diffusion and Dissemination

Finally, a diffusion and dissemination framework should be established to ensure that recipients are aware of the existence of the documents and instructed on their contents. This framework consists of the following actions:

a) Publish the results with appropriate restrictions to those persons involved (e.g. responsible for ICT, services, physical security, etc.)

b) Dissemination of the contents to involved personnel, through educational and training material

c) Closing the BC project, after all steps and phases completed, goals have been met, deliverables released and reviewed.

4 Adaptation to Climate Change using Business Continuity Management

Adapting to climate change presents BC managers with some new challenges, which mean that traditional approaches may need to be reviewed [5,9], such as the following:

1. Some aspects of adapting to climate change sit outside the traditional scope of BCM, such as:
    a. As well as causing disruption, weather can also affect a business in more subtle ways such as reduced efficiency (in terms of either process or manpower).
    b. Some sectors are vulnerable to changes in climate averages (e.g. monthly or seasonal rainfall or mean daily maximum temperature averaged over a season or month) as well as weather events, such as the water supply industry.
    c. Some companies face significant business opportunities as our climate changes. These can arise from being ahead of the game in preparing for threats but they can also arise from beneficial effects of weather and climate, such as by accessing the growing market for adaptation and resilience to climate change products and services.
2. Climate change by definition means that threats are changing. Assessment of climate risks and reaction to them may not have kept pace with these changes. In other words, the likelihood of severe weather events may be greater than an assessment based on past experience and things that have not happened could now be possibilities.
3. Climate change is a long term and dynamic phenomenon and therefore requires a response that takes into account future and changing threats and how these interact with business timescales. BCM, however, tends to be focussed on short timescales and does not generally engage with long-term drivers.

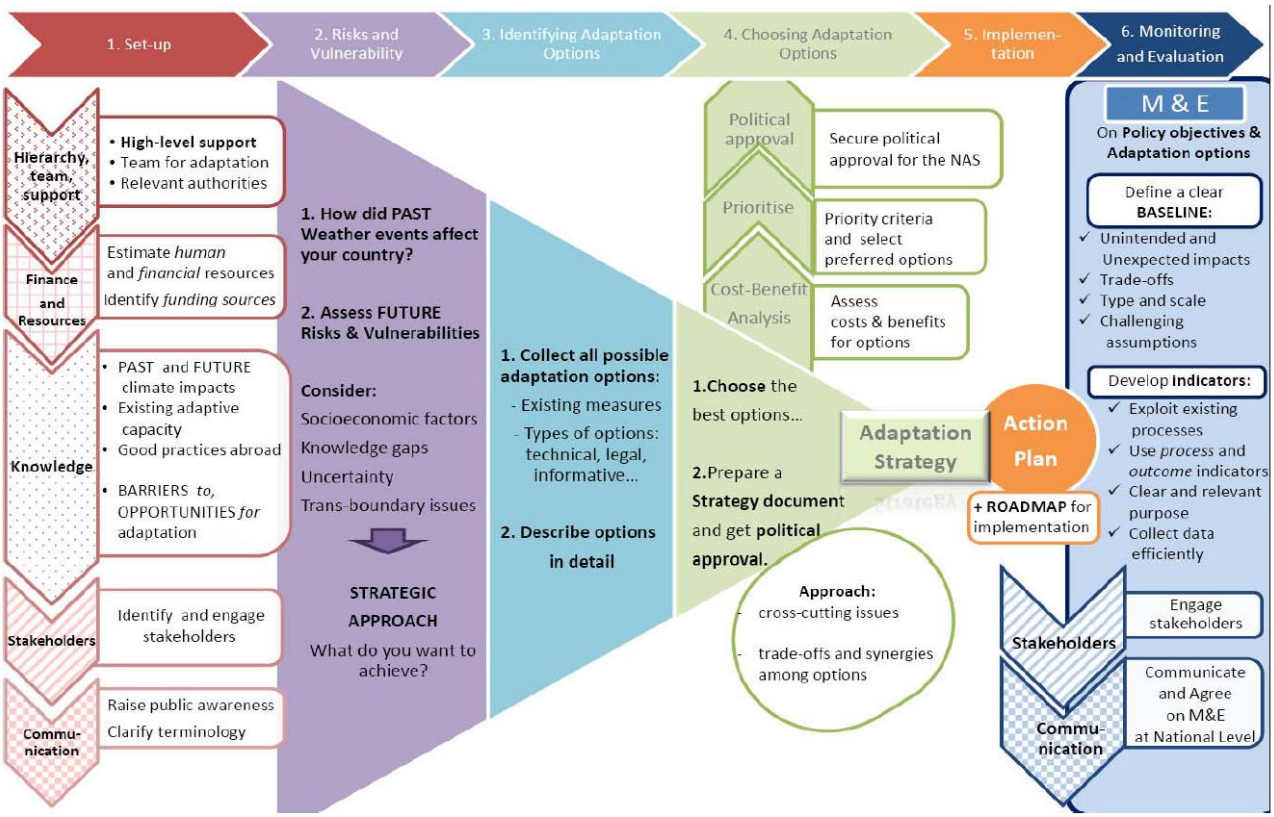

Figure 9 EC Guidelines on developing climate change adaptation strategies

The guidelines on developing adaptation strategies related to climate change are depicted in the above diagram. Such processes, that could be followed in order to adapt a BCM (as set it out in ISO 22301 and ISO 22313), are described hereafter.

4.1 Reviewing the Context of the Organization

In light of the desire to adapt to climate change, a review of the context of the CI should be implemented, divided in three proposed tasks:

4.1.1 Identify climate influenced external and internal factors

Climate change can be seen as an external factor that affects the organization either directly or through its influence on other external factors. It should be noted that interconnections with suppliers and providers are also important, especially where the relationship involves a shared risk. In this direction, climate trends in regions that the CI's relationships are located should be considered.

Regarding internal factors, activities, services, products or supplies, that involve long planning horizons, particularly vulnerable locations or a high degree of sensitivity to weather, climate or indoor temperature, should be considered.

4.1.2 Identify any new interested parties and requirements

There are several groups and individuals with an interest in climate change, from whom new requirements may arise (based on ISO 22313), such as the following:

- Government
- Pressure Groups/investors
- Staff
- Customers
- Trade groups
- Suppliers/neighbours/regulator

4.1.3 Review and amend the scope of your BCMS

The scope of a CI's BCM should be amended to cover:

1) Long-term considerations, will help avoiding decisions that embed vulnerability and identifying where it may be cost effective to implement measures early on in a process
2) Non-disruptive impacts, should be left out of the scope.

4.2 Developing Leadership

As with any new initiative, strong leadership will be important for the success of adaptation planning as it will secure the required commitment and resources from across the business. This section outlines three tasks that will help put this leadership in place:

4.2.1 Make the case to top management

Top management need to be committed both to adapting to climate change and to do so as part of the BCMS. This can be achieved by presenting a) examples of how weather has affected the Ci in the past and any related costs, b) a list of internal and external factors, c) a brief explanation of how adapting to climate change goes beyond normal BCM and d) examples of actions taken by others.

4.2.2 Review and amend the BC policy

In order to make sure it is clear that the impacts of climate change are covered by the BCM, the BC policy should be amended, so that it explicitly makes reference to climate change and/ or new and changing risks. This may or may not refer to adaptation as a separate activity. Alternatively, this commitment could be included in the environmental policy and linked as an internal factor affecting the BCM.

4.2.3 Define any new roles, responsibilities and authorities

Since adapting to climate change uses a current BCM system, roles and responsibilities should be assigned, depending on the expertise and profile that current managers/leaders have, or some other new roles and responsibilities may need to be allocated across a number of different functions.

4.3 Understanding the Key Issues

As described also in the previous chapter and In general in this deliverable, Business Impact Analysis (BIA) and risk assessment (RA) form the backbone of BC planning. Climate change considerations can be factored into these processes, making sure that the future is recognized as being different from the current situation, which in turn is different from the past. This may require new sources of information and ways of thinking.

There are different views on the relative importance of BIA and RA within the BC community. Both processes have features that offer some advantages over the other in the context of adapting to climate change as follows:

- Advantages of BIA:
    - By focussing on the business impact regardless of the source, BIA takes away the need to estimate the likelihood of an event or disruption. This can make assessments quicker and easier in the absence of robust information, which is often the case with regards to the effects of future weather events or climate change
    - The immediate focus on critical products and services and the activities and resources that support them also offers a practical way of prioritizing in order to allocate resources without the need for lengthy assessment processes based on very incomplete and complex information
- Advantages of RA:
    - Risk assessment offers a more complete picture and therefore will pick up a wider range of threats and benefits
    - Similarly, an understanding of risks is more likely to lead to creative thinking around solutions. This may be important as climate change begins to affect us in ways we haven't experienced before.

4.3.1 Review and amend your Business Impact Analyses

Despite the fact that BIA does not focus on the hazard but on the impact, a review may be required to take account of any change in scope and any ways in which the size of the potential business impact or the way that it plays out may be affected by climate change.

4.3.2 Climate risk assessment

ISO 22301 requires that a risk assessment is conducted for prioritized activities. Carrying out this task will make sure that climate related threats and benefits to these activities are taken into account within the risk assessment. The first step is to identify climate related threats and benefits, thinking out of the box and without limiting to previous experience, but focusing on things that could happen based on the list of key internal and external factors that have been defined in the first task of this chapter.

For the threats and benefits that have been identifier, a risk assessment should be carried out, adding in the methodology the following considerations:

- Understand the timescales of relevant decisions
- Use information about the future rather than the past.

4.4 Preparing for Climate Change

This process involves identifying actions to address climate risks and implementing these through your BC plans and procedures or within other business functions where appropriate. It is divided into the following tasks:

4.4.1 Identify adaptation options

Referring to the risks of the previous task, adaptation options can be considered, with a range of large-scale infrastructure project to simple low-tech solutions. They include measures to reduce likelihood of the

threat or increase likelihood of the benefit. These measures can be used in BC plans to shorten the period of disruption or limiting the its impact. Also, management of risks can be achieved through mandating or indicating the suppliers to manage their risks.

4.4.2 Review and amend BC strategy

One thing to consider is that the main impact of climate change may arise from the increasing frequency of disruption. Therefore, a definition of a maximum tolerable frequency of disruption within a period, which would be unacceptable to the business, should be considered.

Another significant impact on the choice of BC strategy is that climate change effects may be widespread and therefore may require a different approach. Strategy options that provide alternative means of operating when a localized disruption occurs may not be available if the incident is affecting a larger area.

4.4.3 Select and implement preferred adaptation options

Referring to the BC strategy, for each climate risk, preferred adaptation options should be identified. This may lead to an amendment of the BC plan and procedures, which may require support for actions. Unfortunately, it is very difficult to estimate the cost of future climate change impacts. This means that it is difficult to assess the effectiveness of different options or to identify the pay-back times or Return on Investment (RoI).

4.5 Performance Evaluation

By definition, adapting to climate change involves responding to a continually changing world. This process involves making sure that any new information, methods or priorities are accounted for by monitoring, measuring, analysis and evaluation in order have feedback for the evaluation report. Therefore this final process is divided into the following tasks:

4.5.1 Monitoring, measurement, analysis and evaluation

Monitoring the business impact of weather events is necessary, including details of the length of disruption, any associated costs and the effectiveness of any adaptation actions or BC procedures. Analysing the output from monitoring activities, can help to identify any implications in during BIA, RA, preferred adaptation actions or BC plans and procedures.

4.5.2 Management review

The management review of a BCM system may be the point at which issues that are not adequately addressed are flagged. Output of the monitoring activities above are used to ensure the continuing suitability, adequacy and effectiveness of this element of the BCM system.

5 BCM in EU-CIRCLE

5.1 Analysis of BCM Questionnaires

For the purposes of this deliverable, a questionnaire (see Annex) has been designed distributed to several CIs through the partners. The questionnaire was divided in two sections, the first regarding the BCM system in general and the second regarding the climate adaptation of the BCM system. The feedback collected consists of nine (9) responses which have been analyzed and presented hereafter.

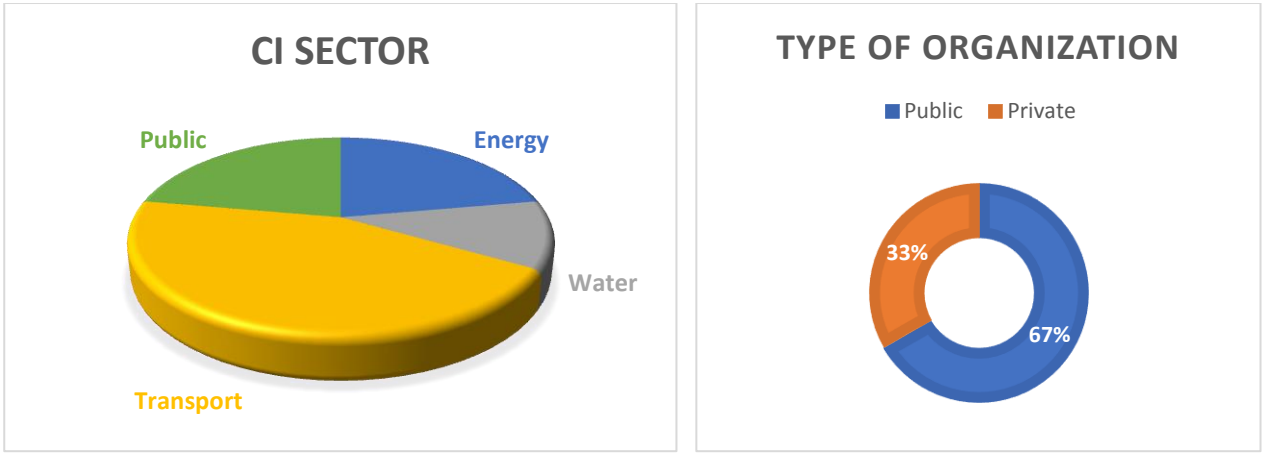

Figure 10 Sector (left) and type (right) of the CI

As depicted in Figure 8 above, most of the CIs comes from the public sector and are providing Transport services (including Railway, Urban, Road and inland water sectors). Responses came from EU countries including Germany, France, UK and Poland.

5.1.1 Part I: Business Continuity Management System Questions

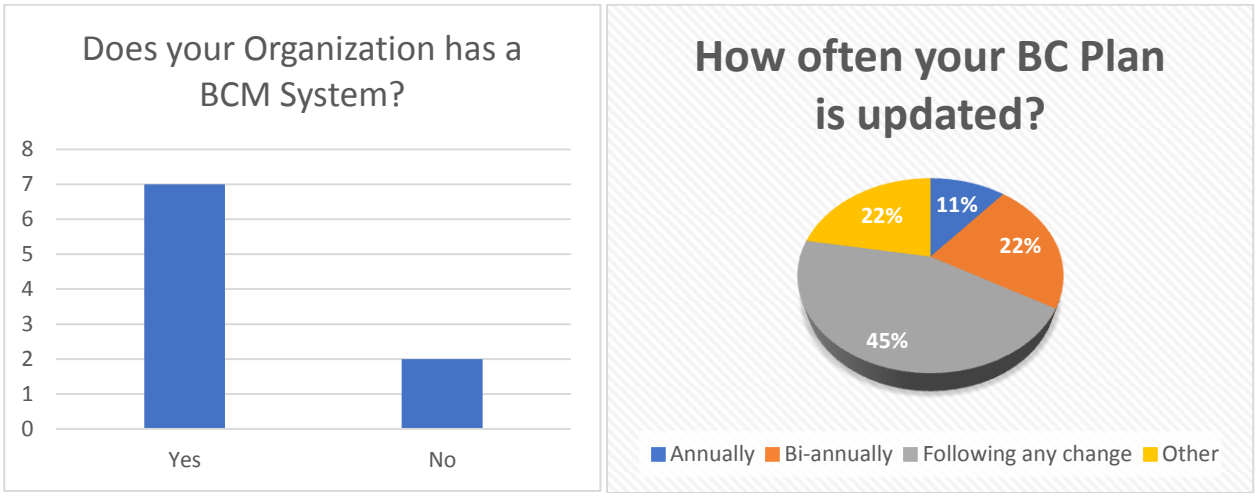

Figure 11 Availability of BCM system and frequency of update

Based on the responses, over 75% of the CIs have a BCM system in their organisation. Those two that do not have comes from the public Transport sector, and one of them, despite the fact that they do not have an organised BCM system, they do have defined procedures for some cases.

From those that do have a BCM system, follow the regular procedures and proposed guidelines (also described previously in this deliverable), updating the BC plan after each change and/or biannually (as a second option). There is also one CI that updates the BC plan after an organisational update and another one as soon as new knowledge is available, approximately 2-3 times in a year.

In the following table, examples of business processes that are considered as critical for the services provided, are presented

Critical business services examples	
Transport Sector (Urban, Bus, Rail, Inland water)	• Computer based operation management system • Communication between drivers and control centre • Telecommunication services • Fuel supplies • Financial services
Energy sector (Oil transport and Energy provider)	• Loading/unloading products • Transport of products • Purchase of electricity to the producers and injection to the network • Network control • Distribution of electricity to the clients • Maintenance
Water	• Provision of essential water and sewerage services
Public sector (EMS and SaR)	• People safeguarding • Emergency Accomondation • Various response functions • Search and Rescue services • Pollution response

In Figure 10, the most common triggering incidents that could lead to a disruption of services and activate the BC plan of an organization, are depicted. Based on the figure, loss of electric power, communications and supplies are of great importance, followed closely by loss of personnel and equipment.

Further to the above, a disruption to financial system and a cyber-attack, is referred as a triggering incident.

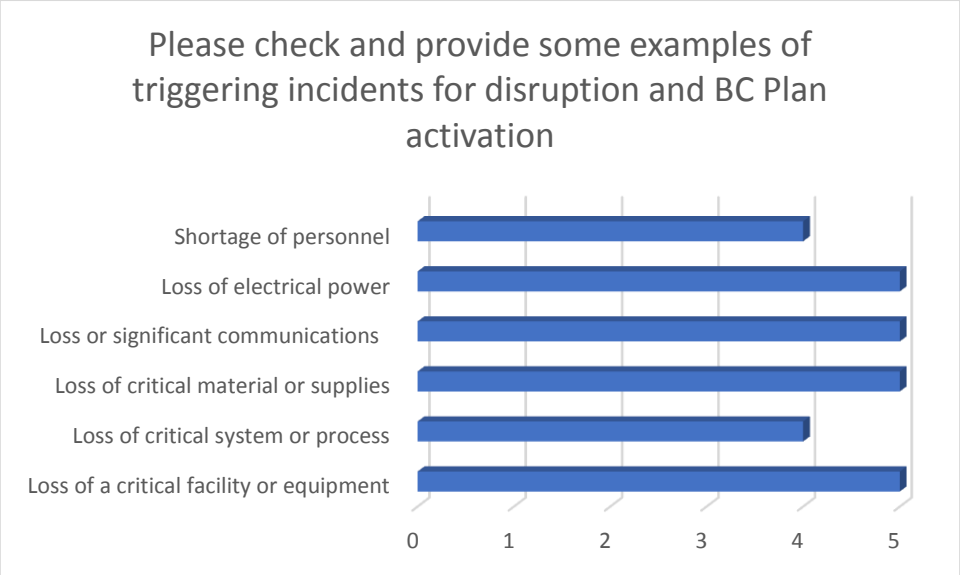

Figure 12 Triggering incidents for disruption and BC plan activation

Following a disruption and a BC plan activation, the key potential impacts identified by the responders of the questionnaires are those of contractual and regulatory compliance, and financial viability. Property protection and consumer confidence, are also considered. Ranking and other potential impacts are presented in Figure 11.

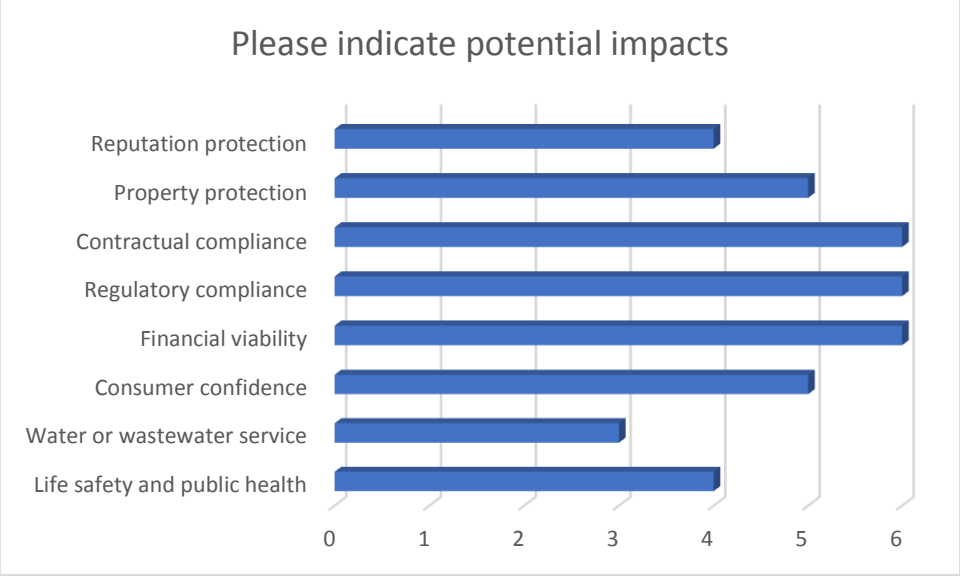

Figure 13 Potential impact of a disruption

In the following table, examples of target times that are set for recovery of business activities after a disruption, within some of the CIs interviewed, are presented. Based on the responses, a variety on RTOs is objected, depending on the process disrupted. Information systems though, are identified to concern most.

Please indicate Recovery Time Objectives (RTO) and possible disruptions				
CI sector	RTO	Department/Process	Essential Operations	Disruptions/Incidents
Transport	varies	Asset management	Maintain drainage systems	Lower line speeds
	No specifications on RTO are made			The typical restoration time depends from category of interruption. In case of “usual” road accidents, typically after 1-3 days operations are in a normal way.
	Weekdays: Until the next morning (4:00 a.m.) whenbus operations starts again	Bus	Bus operatoins	Computer-based operations management system
	120 minutes	IT department	Maintain communications equipment	Loss of communication
	24 hours	Financial and accounting department	Provide additional financing sources	Inability to finance shipping services
	24 hours	Purchasing department	Provide additional supplies	Inability to operate vessel
	12 hours	Logistic department	Provide additional services	Inability to load/ unload vessel
Energy	15 minutes	Maintenance traffic	Maintain operational process	Loss of electrical power
	3 hours	Technical	Loading/Unloading oil products	Pumping unit damage
	6 hours	HR	Provide additional personnel	Physical and intellectual fatigue of personnel during long time response

Please indicate Recovery Time Objectives (RTO) and possible disruptions				
CI sector	RTO	Department/Process	Essential Operations	Disruptions/Incidents
	Supply must be restored to 90% of the final clients that have been cut in maximum 5 days	Network control	Maintain supply	Supply to distribution networks
	Depending on each contract (confidential)	Network control	Maintain supply	Supply to industrial clients
	12 hours between the alert and the beginning of the intervention	Maintenance	Maintain supply or control by critical equipment availability	
Public	15 minutes	IT	Maintain communications equipment	Loss of communication

Regarding alternative facilities or redundant systems, most of the Cis have the following in order to continue their vital operations:

- Alternative or redundant telecommunication systems
- Alternative or redundant power supply (generators, UPS, etc)
- Alternative Buildings/Facilities/Coordination centers or distance control/management

As best practices in Business Continuity, that are very related and similar to the above, the following have been indicated:

- Relocation and Remote Working
- Generators and batteries used as back-up
- Portable communication means and temporary equipment
- Continuous update of the procedures
- Communication with the customers

5.1.2 Part II: Questions related to adaptation of BCM to climate change

In the following table, responses (where available) related to adaptation of BCM to climate change are presented. This question is applicable only to the participants (7) that answered in the first part, that they do have a BCM in their organisation. Based on the responses in almost all of the cases, organisations declared that have not conducted any action related to climate change adaptation.

Questions related to adaptation of BCM to climate change		
Question	Yes	No
Have your Organization defined key external and internal factors relating to climate threats?	28,57%	**71,43%**
Have your Organization identified any interested parties and requirements?	**57,14%**	28,57%
Have your Organization reviewed and amended the scope of its BCMS	14,29%	**85,71%**
Have your Organization reviewed and amended its BC policy	14,29%	**85,71%**
Have your Organization defined any new roles, responsibilities and authorities	14,29%	**85,71%**
Have your Organization reviewed and amended their Business Impact Analyses	0,00%	**85,71%**
Have your Organization implemented any Climate risk assessment	0,00%	**85,71%**
Have your Organization identified any adaptation options	14,29%	**71,43%**
Have your Organization defined a Maximum Tolerable Frequency of Disruption	0,00%	**85,71%**
Have your Organization selected and implemented any climate change adaptation options	14,29%	**71,43%**
Have your Organization changed the way of performance evaluation	14,29%	**85,71%**
Does your organization monitor the impact of weather events to your business (length of disruption, cost, adaptation actions …)?	28,57%	**71,43%**

The next question regarded examples of climate-driven disruptions, which are the following:

- Event
  - Heavy storm
  - Strong wind
  - Heavy rain
  - Snow and ice
  - Extreme hard sea
  - Cyclone Kyrill (2010)
  - Storms and flash floods
  - Floods
- Impact
  - Blocked roads
  - Tram and track damage
  - Harbour closing
  - Transformer/Distribution facilities flooded
  - Electric lines and pylons out of order

In the next question regarding, regarding indicators used in BCM systems of the organisations related to climate threats, none of the responders declared having something.

Finally, in the following table some critical climate thresholds (where applicable) are indicated, as well as some climate patterns.

Ccritical thresholds of weather/climate variables that have significant impact to a critical process			
Variable	Threshold	Impact	Response
Weather	Flooding above track	Lower line speeds or trains on stop	Flood water recedes, assess situation etc
Wind	No for SaR		Wind over 15 m/s stops mechanical recovery
Sea state	No for SaR		Sea state over 5 stops mechanical recovery
Sea state	No for SaR		Sea state over 6 stops all crane operations
Snow	Three steps are defined on snow height		Different intensity to clear the pedestrian areas at the stops
Storm	Not specified		
Snow	Not specified		
Rain	Not specified		

climate patterns that have significant impact to a critical process				
Variable1	Variable2	Variable3	Timeframe	Impact
Weather	Lack of maintenance	Damage to asset	Variable	Slower speeds. Train delays, financial impacts etc
Wind	Sea state	Visibility	12 hours	Personnel fatigue, response effectiveness, lack of aerial support

5.2 EU-CIRCLE Business Continuity Model

As indicated previously in D4.1, a number of steps were followed in the development of the resilience framework. The first step was to define the term resilience from the EU-CIRCLE point of view. The main approach used for this purpose was to analyse several existing definitions for of resilience, most of which have been gathered from the EU-CIRCLE taxonomy (D1.1). The key terms were identified within each definition and have been combined under four main classifications. The terminologies associated with resilience and their interconnections were also reviewed.

The next step, in D4.1, was to review existing resilience frameworks. The factors influencing critical infrastructure were thus identified. Both the resilience framework analysis together with the factors

influencing critical infrastructure helped to develop the necessary components for the EU-CIRCLE resilience framework presented in D4.1.

Following this, integration of D4.1 and subsequent feedback from discussions with other WP leaders and members is presented in D4.3, as well as crucial contributions from the deliverables completed during this period. Based on D4.3, the resilience triangle in Figure 14, the EU-CIRCLE BCM focus on the part of the curve that refers to resilience loss, aiming to evaluate different BC strategies that will reduce the recovery time, and secondly the part of adaptation, through various measures comparison.

Figure 14 Conceptual resilience triangle proposed in [4] adapted for EU CIRCLE definition

Business continuity strategy essentially means the development of options and the selection of the most appropriate strategies that allow the organization to align with requirements [16]. To align with the requirements outlined in Clause 8.3 of ISO 22301, a step process will be followed:

1. Identify possible business continuity strategies that will reduce the risk identified in the BIA and risk assessment to acceptable level. Three categories of business continuity strategy may be addressed:

   - Risk Mitigation

     Identify opportunities to reduce the likelihood of a disruption, as well as strategies to limit the impact should a disruption occur. For example, consider implementing back up power generation to address the concern about a loss of commercial power at a critical facility.

   - Incident Response
   - Recovery of Activities and Resources

     Identify alternate sources of resources or alternate methods of performing required activities in order to meet downtime tolerances and obligations (alternate facilities, personnel, equipment, information technologies, and even third-parties, as well as manual workarounds if resources such as applications are unavailable).

2. Assess the cost and benefits of identified alternatives and select the best contingency strategy for each core business process, asset or CI, in terms of resilience as described hereafter, but also in D4.3 and D4.5. From a CI's point of view, there are three important factors in the selection process:

   - functionality: the degree to which the replacement functionality supports the production of a minimum acceptable level of output for a given core business process,
   - deployment schedule: the time needed to acquire, test, and implement, and

- cost: life-cycle cost, including acquisition, testing, training, and maintenance.

3. Identify and document contingency plans and implementation modes

Based on the above steps, the following table is proposed as a general template that should be filled, in order to identify and describe BC activities.

Phase	Time Frame	Activity
Phase I- Activation and Relocation	Approx. 0-12 Hours	• **Alert and Notification**. The agency has established specific procedures to alert and notify the [executive director/general manager], senior management staff, and members of the advance team, operations team, support teams and contingency teams that BC activation is imminent. [*Briefly describe procedure or refer to procedure or checklist in appendix*.] • **Initial Actions**. The agency has identified specific actions to be taken to terminate primary operations and activate BC team, communications links, and the alternate facility. [*Briefly describe actions or refer to list of actions in appendix*.] • **Activation Procedures Duty Hours**. The agency has established procedures for an efficient and complete transition of direction and control from the primary facility to the alternate facility, and includes measures for security at both sites. These procedures complement the transportation agency's evacuation plans and emergency response plans. [*Briefly describe procedure or refer to procedure or checklist in appendix*.] • **Activation Procedures Non-Duty Hours**. Procedures for the notification of key staff when not at primary site have been developed. [*Briefly describe procedure or refer to procedure or checklist in appendix*.] • **Deployment and Departure Procedures (Time-Phased Operations)**. Allowances have been made for partial pre-deployment of any essential functions that are critical to operations; determination will be based on the level of threat. [*Briefly describe procedure or refer to procedure or checklist in appendix*.] • **Transition to Alternate Operations**. The transportation agency has established minimum standards for communication, direction, and control to be maintained until the alternate facility is operational. [*Briefly describe procedure or refer to procedure or checklist in appendix*.] • **Site-Support Responsibilities**. The transportation agency has developed a checklist to guide activation of the alternate facility; procedures include provision for notification to alternate facility manager to ready site for operations. [*Briefly describe procedure or refer to procedure or checklist in appendix*.]
Phase II- Alternate Facility/Work Site Operations	Approx. 12 Hours to Termination of Emergency	• **Execution of Essential Functions**. The transportation agency will perform any essential functions determined to be critical to operations from the alternate facility or using temporary work orders or procedures. [*Briefly describe procedure or refer to procedure or checklist in appendix*.]

		• **Establishment of Communications**. The transportation agency will re-establish normal lines of communication within the agency, to external agencies, and to the public. [*Briefly describe procedure or refer to procedure or checklist in appendix*.] • **Support and Contingency Team Responsibilities**. Responsibilities will be assigned to transportation personnel to perform essential functions. [*Briefly describe procedure or refer to procedure or checklist in appendix*.] • **Augmentation of Staff**. As the situation comes under control, additional staff will be activated to provide other services and functions, as necessary. [*Briefly describe procedure or refer to procedure or checklist in appendix*.] • **Amplification of Guidance to Support and Contingency Teams**. Additional guidance will be provided to all transportation personnel in regards to duration of alternate operations and include pertinent information on payroll, time and attendance, duty assignments, etc. [*Briefly describe procedure or refer to procedure or checklist in appendix*.] • **Development of Plans and Schedules for Reconstitution and Termination**. As soon as feasible, the operations team will begin preparation of communication, vital records and databases, and other activities to transfer operations back to primary facility. Circumstances may dictate that a new primary facility is designated and subsequently occupied. [*Briefly describe procedure or refer to procedure or checklist in appendix*.]
Phase III-Reconstitution	Termination of Emergency	• **Reconstitution Process**. The transportation agency will develop general guidance and policy on ending alternate operations and returning to a non-emergency status at the designated primary facility. [*Briefly describe procedure or refer to procedure or checklist in appendix*.] • **Reconstitution Procedures**. The transportation agency will establish specific actions to ensure a timely and efficient transition of communications, direction and control, and transfer of vital records and databases to primary facility. [*Briefly describe procedure or refer to procedure or checklist in appendix*.] • **After-Action Review and Remedial Action Plans**. The transportation agency will develop a task force to assess all phases and elements of the alternate operations and provide specific solutions to correct any areas of concern. [*Briefly describe procedure or refer to procedure or checklist in appendix*.]

5.3 CIRP and Case Studies

As described in the previous section, through the BC model, strategies will be identified and evaluated. This will be conducted for each test case in EU-CIRCLE, with the help, instructions and feedback collected by the respective CI stakeholders/owners that are involved.

The strategy identification and selection effort will involve three activities:

1. Identify available strategy options
2. Perform cost-benefit analysis on each available option
3. Present best choice(s) for selection and implement selected strategy

These strategies will be identified, based on the impacts that have been presented (and any other indicated by involved CI experts/stakeholders) in D1.5. These impacts are presented below for each test case.

Case study 1: Extreme drought and very large forest fires in South France

		Critical infrastructure impacts				
Cause and response	**Impact driver**	**Transportation**	**Energy**	**Telecom**	**Health**	**Emergency services**
Large scale forest fire	smoke, fire, panic	Low visibility, fallen tree, blockage	Controlled outage, transformer fire, poles burning	Network overload/failure, trunk network node fire	Respiratory problems, intoxication, burnings, fatal injuries	Scarce resources
Firefighting	Increased use of firefigthing means (trucks, ambulances, water carriers..)	Priority, low speed ..			Injured firemen	
Aerial Firefighting	Water bombing		Power lines cut-off, Brown-outs; difficulty to use helicopters to ispect the lines	Telecomunicatio n links lost		
Evacuation	Mass movement	Traffic overload, jams				
Road closure, low border point closure, airport closure	loss of nodes and links of CI networks	Traffic overload, jams	Difficulty to reach the assets by car			

		Critical infrastructure impacts				
Cause and response	**Impact driver**	**Transportation**	**Energy**	**Telecom**	**Health**	**Emergency services**
International cooperation	standards, language, cross-border agreements	Radio (RVA) messages in 3 languages	Electricity purchase (Italy)			

Case study 2: Storm and Sea Surge in the Baltic Sea Port of Gdynia, Poland

Port Oil Piping Critical Infrastructure (CI)				Other CIs affected (cascading effects)
CI Assets	Operating areas	Climate-weather Data Parameters (Impacts)	Potential consequences to oil pipeline CI	
Cargo loading/unloading systems Port internal transport infrastructure Internal transport service Docks and quays Port approach channels Roadstead Port protection infrastructure Search and Rescue system	Underwater	Sea water wave height Wind speed	Mechanical damage of a pipeline (increased corrosion, the rapture of a pipeline, wave impact) Resonance and increased tension of a pipeline	Port CI Network Oil Pipelines CI Network Ship Traffic and Port Operation Information CI Network Shipping CI Network
	Land	Air temperature Soil temperature	Mechanical damage of a pipeline (thermal expansion of the material, increased pressure)	

Chemical Spill Caused by Critical Infrastructure Accident (CI)			CIs affected (cascading effects)
Environment Domains	Climate-weather Data Parameters (Impacts)	Potential consequences to the Environment	
Air	Wind speed, wind direction	the increase of air / water surface / water column / bottom / shoreline temperature	Port CI Network Oil Pipelines CI

Water surface	Wind speed, wind direction, Sea water wave height	in the accident area, the decrease of oxygen concentration in the air / water surface / water column / bottom / shoreline in the accident area, the disturbance of the air / water surface / water column / bottom / shoreline pH regime in the accident area, the aesthetic nuisance of air / water surface / water column / bottom / shoreline (caused by smells, fume, discoloration etc.) in the accident area, the pollution of air / water surface / water column / bottom / shoreline in the accident area.	Network Ship Traffic and Port Operation Information CI Network Shipping CI Network
Water column	Wind speed, sea water wave height		
Sea floor	Wind speed, sea water wave height		
Coast (shoreline)	Wind speed, sea water wave height		

Case Study 3: Coastal flood in Torbay (UK)

				Critical infrastructure impacts			
Cause /scenario	**Impact driver**	**Response**	**Transportation**	**Energy (Gas/ Electricity)**	**Telecom**	**Health**	**Emergency services**
Coastal flooding Scenario 1: Overtopping of sea wall due to storm surge combined with spring tide	Water depth and extent, duration of event(i.e. duration of tide event)	Pumping of sea water, Evacuation, , temporary flood defences (e.g. sandbags), Flood warnings, Instigate major incident plan.	Flooded coastal roads, flooded properties, sea port damages, railway disruption, safety of people traveling close behind the defence structure	Gas main failure, electricity failure (mainly substations)	Network overload/failure	Injured people	Problems with reaching the flooded area, apply evacuation plan, additional resources
Coastal flooding- Scenario 2: Breaching of sea wall due to storm surge combined with spring tide	Water depth and extent, velocity of incoming water, duration (i.e. duration of event until	Pumping of sea water, evacuation, temporary defences	Flooded coastal roads, flooded properties, sea port damages (depending on the location of	Gas main failure, electricity failure (mainly substations)		Injured people	Problems with reaching the flooded area, apply evacuation plan, additional resources (e.g.

				Critical infrastructure impacts			
Cause /scenario	**Impact driver**	**Response**	**Transportation**	**Energy (Gas/ Electricity)**	**Telecom**	**Health**	**Emergency services**
	repairing)		the breach), railway disruption, safety of people traveling close behind the defence structure				equipment)
Combined flooding. Scenario 3: Pluvial flooding (urban-sewers) combined with coastal flooding scenario 1	Water depth and extent, runoff, duration of event (I.e. duration of storm-runoff). Combined Sewer Overflow (CSO) restricted discharge to coastal waters.	Pumping of mixed water (sea water, waste water), evacuation, temporary flood defences (e.g. sandbags), Flood warnings	Flooded roads, flooded properties, sea port damages, railway disruption, safety of people traveling.	Gas main failure, electricity failure (mainly substations)	Network overload/failure	Injured people, polluted water, sewage debris, clean water supply contamination, dysfunction of hospitals, clean up after event	Blocked resources (fire brigade access to assets restricted), scarce resources, problems with reaching the flooded area, apply evacuation plan, additional resources
Combined flooding. Scenario 4: River flooding combined with coastal flooding scenario 1	Water depth and extent, runoff, duration of event (I.e. duration of storm-runoff).. Combined Sewer Overflow (CSO) restricted discharge to coastal waters.	Pumping of mixed water (sea water, waste water, muddy water) Debris to remove, evacuation, controlled flooding areas (detention areas) Flood warnings	Flooded roads, flooded properties, sea port damages, railway disruption, safety of people traveling.	Gas main failure, electricity failure (mainly substations)	Network overload/failure	Injured people, polluted water, sewage debris, clean water supply contamination, dysfunction of hospitals, clean up after event	Blocked resources (fire brigade access to assets restricted), scarce resources, problems with reaching the flooded area, apply evacuation plan, additional resources

				Critical infrastructure impacts			
Cause /scenario	**Impact driver**	**Response**	**Transportation**	**Energy (Gas/ Electricity)**	**Telecom**	**Health**	**Emergency services**
Combined flooding. Scenario 5: Pluvial flooding (urban-sewers) and river flooding, combined with coastal flooding scenario 1	Water depth and extent, runoff, duration of event (I.e. duration of storm-runoff).. Combined Sewer Overflow (CSO) restricted discharge to coastal waters.	Pumping of mixed water (sea water, waste water, muddy water) Debris to remove, evacuation, controlled flooding areas (detention areas), , temporary flood defences (e.g. sandbags) Flood warnings	Flooded roads, flooded properties, sea port damages, railway disruption, safety of people traveling.	Gas main failure, electricity failure (mainly substations)	Network overload/failure	Injured people, polluted water, sewage debris, clean water supply contamination, dysfunction of hospitals, clean up after event	Blocked resources (fire brigade access to assets restricted), scarce resources, problems with reaching the flooded area, apply evacuation plan, additional resources

Case study 4: International Event

Cause / Scenario	**Impact driver**	**Response**	**Energy (Electricity; Coal power plant)**	**Transportation (Roads, Bridges)**	**ICT (telephones, mobile)**	**Water**	**Public**
Scenario 1: Cyclonic Pressure affecting the city of Khulna directly	1. Rainfall (depth duration, extent) 2. Wind (speed, duration, extent)	1. Evacuation of people, & buildings, flood defences 2. Embankment structure to protect housing 3. Recovery	Coal power plant newly built in the vicinity of the city, Grid substations and distribution lines. Trains are not electrified	Roads, rail and bridges Consideration of adaptation options	Failure of Telephones, internet sevices and mobile networks	waste water, water distribution, water for agriculture, water for industrial use and contamination. Consideration of adaptation options	Emergency services will be cut off due to bad roads and communication immediately after an event. Long term effects due to disruption of hospitals, schools Considerati

Cause / Scenario	Impact driver	Response	Energy (Electricity; Coal power plant)	Transportation (Roads, Bridges)	ICT (telephones, mobile)	Water	Public
		measures (short and long term)					on of adaptation options Welfare of people
Scenario 2: Cyclonic Pressure destroying the surrounding industries of the city	1. Rainfall (depth duration, extent) 2. Wind (speed, duration, extent)	1. Evacuation of people, & buildings, flood defences 2. Embankment structure to protect industries Recovery measures (short and long term)	Coal power plant newly built in the vicinity of the city, Grid substations and distribution lines. Trains are not electrified	Roads, rail and bridges Consideration of adaptation options	Failure of Telephones, internet sevices and mobile networks	waste water, water distribution, water for agriculture, water for industrial use and contamination, Consideration of adaptation options	Emergency services will be cut off due to bad roads and communication immediately after an event. Long term effects due to disruption of hospitals, schools Consideration of adaptation options, Welfare of people
Scenario 3: Tidal surge resulting from the cyclone along the river to Khulna city)	1. Rainfall (depth duration, extent) 2. Wind (speed, duration, extent) 3 Tidal waves (height, duration, extent)	1. Moving embankment structure 2. Recovery measures	Grid substations and distribution lines. Trains are not electrified	Roads, rail and bridges Consideration of adaptation options	Telephones, internet services and mobile networks	waste water, water distribution, water for agriculture, water for industrial use and contamination, Consideration of adaptation options	Emergency services will be cut off due to bad roads and communication immediately after an event. Long term effects due to disruption of hospitals, schools Consideration of adaptation options and longer-term effects,

Cause / Scenario	Impact driver	Response	Energy (Electricity; Coal power plant)	Transportation (Roads, Bridges)	ICT (telephones, mobile)	Water	Public
							Welfare of people

Case Study 5: Floods around Dresden, Germany

		Critical infrastructure impacts				
Cause and response	**Impact driver**	**Transportation**	**Energy**	**Telecom**	**Health**	**Emergency services**
River flood, groundwater	Water depth and extent of inundated area, runoff, duration	Non accessible roads, Blocked roads, rails	Electrical grid must be switched of partly	Energy cut	Evacuation of main hospitals could be needed due to inundation	Reduced accessibility of inundated areas
Energy cut	E-network topology, inundated area	(Tram network shut down)		Public phone network overload/shut-down due to energy cut	Evacuation due to energy cut	
Evacuation	Number of people	Additional transport demand		Higher demand for communication		
Drinking water	Quantity of water, energy cuts at pumps				Evacuation due to disrupted water provision	
Sewage system failure	Runoff, duration				Infection diseases	

In all test cases, the network of CI's that is assessed, including the assets identified and being involved will be designed and inserted in CIRP (see D5.6). Based on the hazard, the impact will be assessed through network analysis. After business impact and risk assessment being assessed, the involved stakeholders in cooperation with EU-CIRCLE partners and CIRP will implement (through simulation) for further analysis the BC strategies that are usually followed as best practices by their organization, or any other strategy proposed by the EU-CIRCLE experts. For example, in test case 4, a rerouting strategy will be assessed for the part of network that is flooded.

In more details, and based on the previous table of section 5.2, the following activities will be implemented in CIRP:

Activity	CIRP Implementation
Phase I- Activation and Relocation	
Activation Procedures Duty Hours.	Establish a set of predefined scenarios for network operation (either a single network or network of networks) under major disruptions.
Deployment and Departure Procedures (Time-Phased Operations).	Depending on BC response there is potentially the need to reach impacted location provided that transportation network is not available. This would require that transportation network analysis will be needed to estimate 1/ optimal routing & 2/ time needed between starting point of responders & impacted location
Transition to Alternate Operations.	1/ add or modify assets to a network (e.g. generators for electricity failure) to support operation & solve network 2/ provide alternative solution to network operation (without impacted assets) and determine if and how much network service is impacted (using indicators from D4.5)
Site-Support Responsibilities.	1/ determine that impacted assets are accessible by support teams 2/ determine that impacted assets have auxiliary services (e.g. access to telecoms, electricity, water) provided by other CI
Phase II- Alternate Facility/Work Site Operations	
Execution of Essential Functions	1/ add or modify assets to a network (e.g. generators) to support operation & resolve network 2/ provide alternative solution to network operation (without impacted assets) and determine if and how much network service is impacted (using indicators from D4.5)
Support and Contingency Team Responsibilities.	1/ determine that impacted assets are accessible by teams providing supplies / maintenance materials
Phase III- Reconstitution	
Reconstitution Process	Restoration of basic network (before impact on services). Solving of network with suitable analysis tools

6 Conclusion

BCM is not just about reacting to an incident. It's not just about disaster recovery, crisis management, risk management control or technology recovery. And it's not just a professional specialist discipline. BCM is a business owned and driven activity that can provide the strategic and operational framework to review the way that a Critical Infrastructure provides its products and services and increase its resilience to disruption, interruption or loss.

The key to recovery is time. Following an unplanned event, the CI which recovers in the shortest possible time will mitigate their losses to an optimum level. It should be viewed as a cornerstone to good corporate practice, embracing risk, security, insurance, legal, operational and safety issues.

In this deliverable, the Business Continuity Management framework is analysed, presenting also the relation with climate change and its adaptation. Further to that EU-CIRCLE BC model is presented and its relation with CIRP and test cases. In a nutshell, through BCM, appropriate strategies for recovery will be assessed through the following activities:

1. Identify available strategy options
2. Perform cost-benefit analysis on each available option
3. Present best choice(s) for selection and implement selected strategy

Evaluation of the strategies will be implemented through CIRP for each test case. This method will allow CI's owners/stakeholders/managers to identify and then select the best, most cost-effective methods to manage the risk and impact associated with the disruptive incident.

7 Bibliography

[1] Adapting the ICT Sector to the Impacts of Climate Change– Summary Report AEA/ED49926/Issue

[2] Baba, Hitoshi., Taisuke Watanabe, Masafumi Nagaishi, and Hideaki Matsumoto, Area Business Continuity Management, a new opportunity for building economic resilience, 4th International Conference on Building Resilience, Building Resilience 2014, Salford Quays, United kingdom, 8-10 September 2014

[3] Baba, Hitoshi., Itsu Adachi, Hiroshi Takabayashi, Noriaki Nagatomo, Shiro Nakasone, Hideaki Matsumoto, and Toshiyuki Shimano, Introductory study on Disaster Risk Assessment and Area Business Continuity Planning in industry agglomerated areas in the ASEAN, Journal of Integrated Disaster Management (IDRiM Journal) Vol.3 No.2, Dec. 2013, pp.184-195.

[4] Bruneau, M., et al. (2003). "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities." Earthquake Spectra 19(4): 733-752

[5] BSI Group, Adapting to Climate Change using your Business Continuity Management System

[6] Cabinet Office, Summary of the 2016 Sector Security and Resilience Plans, 2013.

[7] CLIMATE CHANGE IMPACT ON THE INFRASTRUCTURE SECTOR, https://climate.copernicus.eu/resources/information-service/climate-change-impact-infrastructure-sector

[8] European Commission, Energy Efficiency and its contribution to energy security and the 2030 Framework for climate and energy policy, 2014

[9] European Commission, Guidelines on developing adaptation strategies, 2013

[10] European Commission, WHITE PAPER Adapting to climate change: Towards a European framework for action, 2009

[11] European Commission, Impacts of Climate Change on Human Health in Europe. PESETA-human health study, JRC Scientific and Technical Report, 2009.

[12] European Environment Agency, Adaptation of transport to climate change in Europe - Challenges and options across transport modes and stakeholders, 2014.

[13] European Environment Agency, European Environment Agency – Energy, 2013.

[14] ICM COMPUTER GROUP, Beginners Guide to Business Continuity

[15] World Health Organisation – Europe, Protecting Health in Europe from Climate Change, 2008

[16] Zawada Brian, IMPLEMENTING ISO 22301: THE BUSINESS CONTINUITY MANAGEMENT SYSTEM STANDARD, Avalution Consulting

Annex

Annex I: EU-CIRCLE QUESTIONNAIRE for Business Continuity Management (BCM)

QUESTIONNAIRE for Business Continuity Management (BCM)

In the framework of D4.4-CI climate related business continuity model

EU-CIRCLE Partner:						
Stakeholder Title:						
CI Sector:	Energy ☐	ICT ☐	Water ☐	Transport ☐	Chemical ☐	Public ☐
Type of Organization:	Public ☐		Private ☐		Other ☐	
Country:						

PART I

The following table is related to Business Continuity Management (BCM) System in general. Please share as much information as you can, providing inputs and examples relevant to the questions. The questionnaire is intended to be filled in cooperation with the EU-CIRCLE partners. If there are confidential information or issues, please discuss confidentiality issues with the EU-CIRCLE contact person and define how this info might be used in EU-CIRCLE. No information is required at specific infrastructure/asset level, only generic information regarding processes/procedures/sequence of actions in case of service disruption.

Table 1 Business Continuity Management System Questions

Question	Answer
Does your Organization has a BCM System?	☐ Yes ☐ No
How often your BC Plan is updated?	☐ Annually ☐ Bi-annually ☐ Following any change ☐ Other ☐ ……
Provide examples of business processes that are considered critical for the service that you provide *(critical are meant processes that must be restored immediately after a disruption to satisfy mandatory regulations and requirements)*	☐ …… ☐ …….. ☐ …… ☐ ……..
Please check and provide some examples of triggering incidents for disruption and BC Plan activation	☐ Loss of a critical facility or equipment ☐ Loss of critical system or process ☐ Loss of critical material or supplies ☐ Loss or significant communications ☐ Loss of electrical power ☐ Shortage of personnel ☐ …… ☐ ……..
Please indicate potential impacts (BIA)	☐ Life safety and public health ☐ Water or wastewater service ☐ Consumer confidence ☐ Financial viability ☐ Regulatory compliance ☐ Contractual compliance ☐ Property protection ☐ Reputation protection ☐ …… ☐ ……..

Please indicate Recovery Time Objectives (RTO)[2] and possible disruptions			
RTO	**Department/Process**	**Essential Operations**	**Disruptions/Incidents**
Eg. 30 minutes	*Eg. IT*	*Eg. Maintain communications equipment*	*Eg. Loss of electrical power, loss of equipment, lack of access to equipment*
Does your Organization have Alternative facilities or redundant systems to continue Vital Operations? Please indicate		☐ …… ☐ ……	
Please indicate best practices for Business Continuity in your Organization (eg in case of Electric power loss, a generator is used as backup)		☐ …… ☐ …… ☐ ……	

[2] target time set for the recovery of business activities after a disruption

PART II

The following table is focusing on Climate Adaptation of BCM.
The same rules and guidelines, as in the previous part, are applied.

Table 2 Questions related to adaptation of BCM to climate change

Question	Answer
Have your Organization defined key external (heavy rain, strong wind, drought...) **and internal** (long planning horizons, site exposure, supply chain…) **factors relating to climate threats?**	☐ Yes ☐ No Your input: …….. ……..
Have your Organization identified any interested parties (Regulators, Government, Investors, Customers, Associations …) **and requirements?**	☐ Yes ☐ No Your input: …….. ……..
Have your Organization reviewed and amended the scope of its BCMS (e.g. including long-term considerations linked to climate change or non-disruptive events such reduced efficiency due to thermal discomfort during heatwaves**)?**	☐ Yes ☐ No Your input: …….. ……..
Have your Organization reviewed and amended its BC policy (e.g. deliver key business functions within the context of Climate extremes and Climate Change**)?**	☐ Yes ☐ No Your input: …….. ……..
Have your Organization defined any new roles, responsibilities and authorities (e.g. hazard expert, meteorologist …**)?**	☐ Yes ☐ No Your input: …….. ……..
Have your Organization reviewed and amended their Business Impact Analyses (e.g. identified business impacts that involve climate influenced factors**)?**	☐ Yes ☐ No Your input: …….. ……..
Have your Organization implemented any Climate risk assessment (identified climate threats/process, (climate) risk rate your key suppliers/vendors and your major customers in the RA…)**?**	☐ Yes ☐ No Your input: …….. ……..

Have your Organization identified any adaptation options (options concerning material, processes, technology etc. to address climate threats included in the BCMS e.g. reduce heat generation or alter cooling method to address potential change to temperature extremes…)**?**	☐ Yes ☐ No Your input: …….. ……..
Have your Organization defined a Maximum Tolerable Frequency of Disruption (number of disruptive events within a time period), **which can be influenced by climate change?**	☐ Yes ☐ No Your input: …….. ……..
Have your Organization selected and implemented any climate change adaptation options (maintenance, design etc.**)?**	☐ Yes ☐ No Your input: …….. ……..
Have your Organization changed the way of performance evaluation (monitoring, measurement, analysis and evaluation**)?**	☐ Yes ☐ No Your input: …….. ……..
Does your organization monitor the impact of weather events to your business (length of disruption, cost, adaptation actions …)?	☐ Yes ☐ No Your input: …….. ……..
Provide up to 3 examples of climate-driven disruptions recorded in your organization (or sector) in terms of event, disruption, damages, consequences, recovery & restoration	Example1: …….. …….. Example2: …….. …….. Example3: …….. ……..
Which are the standard indicators (quantitative) used in your BCMS related to climate threats and their respective thresholds?	Your input: …….. ……..

Please provide critical thresholds of weather/climate variables (or weather events) above (or below) which the impact to a critical process of your business become significant			
Variable	**Threshold**	**Impact**	**Response**

Please provide climate patterns (combination of weather variable values for specific time period) which may have significant impact to a critical process of your business				
Variable1	**Variable2**	**Variable3**	**Timeframe**	**Impact**