Standard Operation Procedures	SOP 65
Effective Date: 08/04/2026	**Public**

Business Continuity Plan

Special Requirements	This procedure is a controlled document maintained by Quality Management. It may not be deleted without comparable controls. Please note that this document becomes uncontrolled once printed. Make sure by always referring only to the Repository that you have the right version in use. The procedure should be updated when there are changes in EFSA with respect to what is stated in the document (e.g., Relevant Standards, legislation, and documents, change in procedure, etc.). The person responsible for maintaining this procedure up to date is the Lead author with the support of the QM.

Process Responsibility	Process owners are accountable of this procedure being adhered to their process or respective unit. All relevant staff is responsible for the correct implementation of the procedure. Responsibilities for performing specific steps are outlined in the document.

SCOPE AND OBJECTIVES

This document aims to define the provisions to be implemented to ensure the continuity of EFSA's operations. This Business Continuity Plan (BCP) is applicable as a response to disruptive event causing a major incident / emergency or crisis. In particular, the purpose of the BCP and related documents is to ensure the resumption of EFSA's critical processes / products within the Recovery Time Objective (RTO).

Annex to the present BCP formalize also relevant methodological BCMS related elements driving design, implementation and maintenance of the BCMS itself.

Scope of BCMS: Development and provision of independent scientific advice, information and risk communication in the areas of food, feed and emerging risks according to the European Parliament and Council Regulation No. 178/2002 and its supporting functions. Activities are related to IAF Sector 36.

Inclusion and Exclusion
Below is indicated what is included and what is excluded from the scope of the BCMS.

- All EPA Processes / Products
- EFSA site (the only one in Parma) is included in the scope of the BCMS. This includes the Data Centre located in its premises.
- All IT applications supporting critical process / products as per BIA results are included in the scope of the BCMS. All IT applications are either native cloud-based SaaS managed with contract SLAs or managed on on-premises infrastructure or IaaS / PaaS.
- All personnel and suppliers supporting critical processes / products as per BIA results.

Please refer to the Business Continuity Procedure for details regarding:

- EFSA Critical Processes / Products resulting from BIA and Recovery requirements (RTO);
- Critical personnel for which the organization has in place business continuity strategies;
- Critical suppliers for which the organization has in place business continuity strategies.

The complete list of Critical Applications in scope of the BCMS can be found at the following link.

What is not explicitly mentioned as in scope of the BCMS should be considered excluded.

RELEVANT STANDARDS, LEGISLATION AND DOCUMENTS

- ISO 22301:2019 Business Continuity Management System – Requirements
- ED Decision Health, Safety, Environment and Security Policy, Roles and Responsibilities
- Ann19_02 Security Emergency Plan
- SOP_064_Emergency / Incident and crisis management
- WIN_SOP065_01 Alternate Site Management
- WIN_SOP065_02 Business Continuity Procedure
- Disaster Recovery (DR) Manual
- Operations and Maintenance Manuals
- WIN_SOP049/02 Management of Information Security Incidents
- WIN_SOP 032_01 Internal ISO Audits Link

ABBREVIATIONS AND DEFINITION

ASC	Agency Security Committee
AST	Assistant

BC	Business Continuity
BCO	Business Continuity Officer
BCP	Business Continuity Plan
BIA	Business Impact Analysis
EPA	EFSA Process Architecture
IC	Incident Commander
ISO	Information Security Officer
LC	Lead Communicator
MS	Management System
MTPD	Maximum Tolerable Period of Disruption
PDCA	Plan, Do, Check, Act
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SM	Site Manager

PROCEDURE

The continuity of EFSA's operations is ensured by the adoption of ad-hoc response plans in line with the following **strategies**:

- **Short / Mid-term** (activities expected to be resumed within 60 days) – The response plan of short / mid-term strategy is this BCP document and related ones. The procedure described in this plan covers different major effects caused by a disruptive event:
  - EFSA site unavailability, in this case WIN_SOP065_01 on Alternate Site Management applies – DMS Link.
  - IT Unavailability, in this case the Disaster Recovery Manual applies – DMS Link
  - Critical personnel and supplier unavailability, in this case the "WIN_SOP065_02 BC procedure" applies – DMS Link
- **Long term** (activities not resumed within 60 days) – Response plan on the long-term course will be assessed on ad-hoc basis by the BC Team.

Roles, responsibilities and procedures to manage a major incident / emergency or crisis are described in detail in SOP_064_Emergency / Incident and crisis management (DMS Link).

This section aims at summarising the fundamental concepts for:

- Activating the BCP;
- Managing a crisis;
- Manage back to normal.

Within the Business Continuity (BC) the following high-level responsibilities are identified:

- Incident Commander (IC) – Lead the Strategic Group of the Security Emergencies / Incidents and Crises Management Team and is responsible for the endorsement of any strategic BC initiative;
- Lead Communicator (LC) – Support the Strategic Group of the Security Emergencies / Incidents and Crises Management Team by spreading to all appropriate interested parties the information deemed appropriate.
- Business Continuity Officer (BCO) – Lead the Tactical Group of the Security Emergencies / Incidents and Crises Management Team with regards of Business Continuity and is responsible for coordinating the activities deemed appropriate to achieve the strategic objectives in this area endorsed by the IC.

<table>
<tr><td colspan="2">

Duty Officer – Ensure management of the security emergency / incident and crisis along its lifecycle also supporting when needed the BCO. The role can be covered by the BCO, ISO or PSO, according to the event type.
Site Manager (SM) – Give specialist support to the Tactical Group of the Security Emergencies / Incidents and Crises Management Team.
Information Security Officer (ISO) – Give specialist support to the Tactical Group of the Security Emergencies / Incidents and Crises Management Team.
Process / Product Leader – Responsible for executing core response actions on Business Continuity in the scenario of loss of critical personnel / critical supplier unavailability.

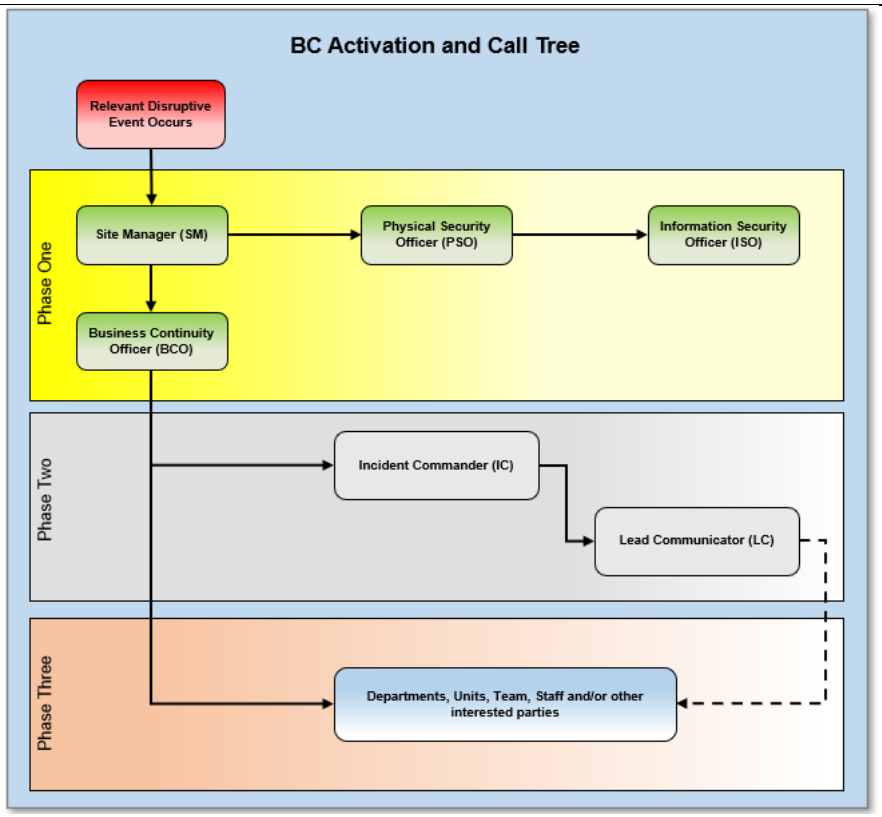
The type of disruptive events[1] that may trigger a major incident / emergency and crisis are the for example:

In the business continuity area: (i) fire in the building, (ii) flooding in the building, (iii) earthquake, (iv) gasoline or dangerous liquid spills in the building, (v) epidemic / pandemic, (vi) travel related incidents, (vii) supplier IT failure, (viii) supplier personnel unavailability, (ix) supplier not expected default;
In the physical security area – (i) site occupation, (ii) receiving a suspect parcel, (iii) discovery a suspect item, (iv) presence of suspect vehicles, (v) presence of armed individual;
In the information security area – (i) cyberattack, (ii) virus affection, (iii) physical or hardware problems.

</td></tr>
<tr><td>Step 1</td><td>ACTIVATING THE BCP</td></tr>
<tr><td>Incident Commander and Business Continuity Officer</td><td>The following picture illustrates the communication workflow used in case a disruptive event affects EFSA.

After consultation with the SM, PSO and ISO (Phase One) and approval by the Incident Commander (Phase Two) the BCO activates the BCP. The BCO contacts all parties deemed necessary to operationally achieve the goals endorsed by the Strategic Group. LC broadcast general information to all relevant EFSA community (Phase Three).</td></tr>
</table>

[1] The list of the events that were considered in the context of this BCP may be further refined in future Plan, Do, Check, Act (PDCA) iterations.

	
Step 2	IDENTIFY A CRISIS ROOM
Business Continuity Officer	BCO is responsible for identifying the most suitable location to use as Crisis Room. The room must: - Have space to host the BC Team members for their coordination meetings; - Be segregated from other working spaces to ensure an adequate level of confidentiality. When the appropriate room to manage the crisis is identified, any planned or on-going meetings in that room is cancelled/suspended. BCO is responsible for recording the coordination meetings held in the Crisis Room by the Security Emergencies / Incidents and Crises Management Team with the most appropriate mean. It is possible also to organized virtual crisis rooms (e.g., through dedicated Teams meetings) or mixed (i.e., some of required team members are physically on premise, others are connected remotely).
Step 3	MANAGING A MAJOR INCIDENT/EMERGENCY/CRISIS
Business Continuity Officer *Strategic Group* *Tactical Group*	In line with the Emergency / Incident and Crisis Procedure, the event is managed either by the Strategic Group or the Tactical Group, according to the event type. In all cases, the objective is to implement recovery procedures for all impacted resources and processes.

All Departments, Units and Teams must cooperate with BCO to achieve any objective assigned within the context of the BCP.

The following paragraphs illustrate the response actions to implement in order to manage the different types of event effects that EFSA has considered.

The BCO is accountable for the achievement of the set objectives and to periodically report to Incident Commander the status of objectives' achievement.

EFSA Site Unavailability

EFSA has a dedicated Working Instruction (WIN_SOP065_01 – DMS Link) to relocate operations in a suitable location or allow staff to work remotely, when a disruptive event cause partial or total site unavailability.
The following table summarises operational responsibilities and resources needed to implement relocation procedures.

Strategy	Operational Responsibility	Needed resources
Remote Working	BCO	-
Florence Site Relocation	SM	Coordination with EUI SM and availability of EUI SM collaborators (1 resource). Financial resources for personnel mission.
Hotel Relocation	CORSER-AST (identified by BCO)	Agreement (contract) with hotel and financial resources

IT Unavailability

EFSA has procedures (DR Manual) and detailed operational instruction (Operational and Maintenance Manual) to manage an adequate response and restoration of services to IT unavailability.

Strategy	Operating Instruction	Operational Responsibility	Needed resources
IT recovery (Tactical Level)	DR Manual Link	ISO	DW Team support (minimum 2 resources);
IT recovery (Operational Level)	Operational and Maintenance Manual Link	ISO	Service Provider (minimum 4 resources).

Critical Personnel Unavailability

EFSA has a dedicated Working Instruction (BC Procedure - WIN_SOP065_02 – DMS Link) detailing the activities to be executed in case of an unavailability of critical personnel scenario for any of the process / product[2] in scope as well as the responsible role for their execution. The abovementioned Working Instruction also details the critical personnel needed for each critical process / product emerged from BIA over time, and their respective backups. The Process / Product Leader has a core responsibility in responding to the personnel unavailability scenario by activating backup resources within defined timeframes and by keeping the BCO informed.

The following table summarises operational responsibilities and resources needed.

Strategy	Operational Responsibility	Needed resources
Replacement of the absent resource(s) with defined backup(s)	Process / Product Leader	Backup resources for each critical personnel unavailable

Critical Supplier Unavailability

EFSA has a dedicated Working Instruction (BC Procedure - WIN_SOP065_02 – DMS Link) detailing the activities to be executed in case of an unavailability of critical supplier scenario for any of the process / product in scope as well as the responsible role for their execution. The abovementioned Working Instruction also details the selected business continuity strategy for each critical supplier emerged from BIA. The Process / Product Leader has a core responsibility in responding to the critical supplier unavailability scenario by executing the defined continuity strategy and by keeping the BCO informed.

The following table summarises operational responsibilities and resources needed.

Strategy	Operational Responsibility	Needed resources
Activate / interact with internal personnel to ensure insource of specific activities executed from supplier	Process / Product Leader	Internal personnel able to insource supplier activities
Activate cascade contracts	Process / Product Leader	Cascade contract

[2] Please note that recovery activities have been divided, depending on the specific process situation, by process, in some case by sub-process and in other cases by product or group of products. The wording "process / product" should be intended as a short way to refer to all those cases as a whole.

	Identify and engage alternative suppliers in the market among the multiple available ones	Process / Product Leader	Alternative supplier
	Identify and engage alternative experts in the market among the multiple available ones	Process / Product Leader	Alternative experts
Step 4	MANAGE BACK TO BUSINESS AS USUAL		
Duty Officer *Business Continuity Officer (BCO)* *Incident Commander*	The Duty Officer and the BCO are responsible to conduct a post event review to define whether the disruptive incident is closed. In case of crisis, the Incident Commander is consulted but nonetheless informed. For the activities to be carried out in order to close the process, refer to SOP 64 - Emergency / Incident and Crisis Management, which contain the provisions to manage the Back to Business as Usual phase.		

RECORDS

Reference	Title	Source or Link/Location
Step 2	Minutes of coordination meetings	DMS
Step 3	Periodic reports to Incident Commander	DMS
Step 4	Post event review	DMS

ANNEX A - CONTEXT OF THE ORGANIZATION

EFSA was established in 2002, following a series of food-related crises during the late 1990s, as an independent actor for scientific consulting and communication concerning the risks concerning the food chain. The agency was formally established by the European Union (EU) as per the norms of Regulation (EC) 178/2002[3], laying down the general principles and requirements of food law amended by the "New Transparency Regulation" Regulation (EU) 2019/1381 Link.

In particular the aim and scope of the Regulation is described as follow:

> *1. This Regulation provides the basis for the assurance of a high level of protection of human health and consumers' interest in relation to food, taking into account in particular the diversity in the supply of food including traditional products, whilst ensuring the effective functioning of the internal market. It establishes common principles and responsibilities, the means to provide a strong science base, efficient organisational arrangements and procedures to underpin decision-making in matters of food and feed safety.*
>
> *2. For the purposes of paragraph 1, this Regulation lays down the general principles governing food and feed in general, and food and feed safety in particular, at Community and national level.*
>
> *It establishes the European Food Safety Authority.*
>
> *It lays down procedures for matters with a direct or indirect impact on food and feed safety.*
>
> *3. This Regulation shall apply to all stages of production, processing and distribution of food and feed. It shall not apply to primary production for private domestic use or to the domestic preparation, handling or storage of food for private domestic consumption.*

The EU general food law created a Europe-wide system of food safety within which the responsibility to evaluate risks and that of managing them are kept separate.

The majority of the activities the EFSA undertakes arise from scientific consultancy requests by the European Commission, the European Parliament and by EU Member States.

EFSA is also able to carry out scientific work on its own initiative. Such a process is known as "self-tasking".

EFSA sets out its work program - be it annual or multiannual- based on the priorities agreed upon with the European Commission and other partners, taking the available resources into account.
Scientific consultancy by EFSA is mostly provided by its Panels of scientific experts and by its Scientific Committee, whose members are appointed by public selection procedures.

[3] Regulation (EC) no. 178/2002 (link) laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety.

The staff of the Agency can produce scientific documents on its behalf, such as for example peer reviews on pesticides and their active substances or answering urgent consultancy requests. The staff of EFSA is able to monitor and analyse information and data on biological danger, chemical contaminants, food consumption and emerging risks.

Furthermore, EFSA complies with several principles and procedures in order to warrant the excellence of its activities. Such principles include:

- A commitment towards opening and transparency;
- Developing a corpus of good practices about risk management, under the guidance of our Scientific Committee and Panel experts;
- A Quality Management System able to constantly monitor and enhance the quality of EFSA's scientific work. This includes self-review and customer feedback systems ensuring that scientific processes are developed consistently and continuously improved. Such a structure includes a self-review system warranting that the whole of the scientific production is uniformly developed by the Panel experts and EFSA personnel;
- A careful review and control activity carried out by an internal auditor under the supervision of EFSA's Management Board's Audit Committee, advising the senior management on possible improvements to work practices in turn;
- External evaluation: the EU regulation establishing EFSA orders the Authority to commission independent external evaluations of its work and working practices. Based on these evaluations, the Management Board makes recommendations on EFSA's future management plans and strategies.

Considering that food security issues respect no boundaries, EFSA does not work alone, but cooperates strongly with partners and stakeholders across the whole of Europe, sharing scientific competences, data, and knowledge.

Furthermore, the agency actively involves its (external) stakeholders in transparency and dialogue, as per the seven main categories below:

- EU Institutions
- Consumers' associations;
- NGOs and pressure groups;
- Food enterprises and companies;
- Suppliers and HORECA (Hotel/Restaurant/Café) professionals;
- Associations of health professionals;
- Academia;
- Farmers and producers.

Regarding the legal and regulatory requirements, EFSA is subject only to EU Regulations and to those specific norms applying to European institutions and other agencies.

However, since the lack of compliance with Laws and Regulations may affect the risk levels and operational continuity and in order to facilitate and/or allow those activities assessing the compliance EFSA has with laws in force, usually carried out by dedicated Certification Organisms, EFSA has chosen to comply, similarly to Guidelines, with the Italian law, international standards and best practices, in the fields of Environment, Health and Safety at Work, Information Security and overall Security.

Therefore, EFSA shall reserve the right to evaluate, on a case-by-case and a point-by-point basis, the application of the relevant laws and norms.

The document marked as WIN SOP 032_06 contains the main procedures by means of which the applicable norms are managed by EFSA.

In particular the Law n. 17 of 10th January 2006 which is the ratification of the Seat Agreement between the Italian Republic and the European Food Safety Authority. It was published on the Gazzetta Ufficiale della Repubblica Italiana[4] on the 10th of January 2006 (link).

The aim of this law is mainly to agree on the conditions of the establishment of EFSA on the Italian territory.

The Italian Republic:

- Helps EFSA to settle and maintain in good condition of functionality his premises in Italy;
- Makes sure that the Italian competent authorities provide an appropriate protection to the surrounding areas of EFSA premises;
- Provides an appropriate school education to the children of EFSA staff guaranteeing a school system coherent with the European Schools system.

EFSA's privileges and immunities are regulated by the "Protocol on the privileges and immunities of the European Communities" of 8 APRIL 1965.

Finally, the following EU Regulations directly apply to EFSA.

- Financial Regulation (Link): This Regulation lays down the rules for the establishment and the implementation of the general budget of the European Union and the presentation and auditing of the accounts. This Regulation shall apply to the implementation of the budget for the Euratom Supply Agency.
- Staff Regulations (Link): Staff Regulations set up the rules, principles, standards and working conditions of European civil service.

PRODUCTS AND SERVICES

According to the Article 23 of the Founding Regulation EFSA's tasks are the following:

- Provide scientific and technical support in the areas within its mission
- Provide scientific and technical assistance in the fields within its mission
- Provide scientific opinions in all cases provided for by Community legislation and on any
- question within its mission
- Promote and coordinate the development of uniform risk assessment methodologies in
- the fields falling within its mission
- Commission scientific studies necessary for the accomplishment of its mission
- Search for, collect, collate, analyse and summarise scientific and technical data in the
- fields within its mission
- Undertake action to identify and characterise emerging risks, in the fields within its
- mission
- Establish a system of networks of organisations operating in the fields within its mission and be responsible for their operation
- Ensure that the public and interested parties receive rapid, reliable, objective and
- comprehensible information in the fields within its mission

[4] Trans. *Official Gazette of the Italian Republic*

ACTIVITIES

EFSA's activities are identified in the EFSA Process Architecture (EPA) and the structure of this can be found at this link.

EPA was analysed in the Business Impact Analysis (BIA) and the Maximum Tolerable Period of Disruption (MTPD) and Recovery Time Objective (RTO) have been identified for each process.

BIA identified a set of critical processes[5].

PARTNERS[6] AND NETWORKS

- EU Member States
- EU institutions and agencies
  - European Commission
  - European Parliament
  - European Medicines Agency
  - European Chemicals Agency
  - European Centre for Disease Prevention and Control
  - Joint Research Centre
- Competent organisations in Member States
  - A complete and regularly updated list can be found at this link.
- International organisations
  - Food and Agriculture Organization (FAO)
  - World Health Organization (WHO)
  - Codex Alimentarius Commission
  - International Plant Protection Convention
  - European and Mediterranean Plant Protection Organization
  - Organisation for Economic Co-operation and Development
  - World Organisation for Animal Health
- Stakeholders
  - A complete list of the stakeholders can be found at this link.

SUPPLY CHAIN

Core Business

Scientific Data delivered by:

- EU National Competent authorities
- Universities, Research Centres
- Laboratories
- Industries and stakeholders' organisations (industry associations)

Support

A list of in force contracts grants and ISA contracts is in place and maintained up to date by Procurement[7].

[5] For the MTPD and RTO results and the list of critical processes, see the Business Continuity Procedure (link)
[6] Complete list of Partners and networks (link)
[7] List is published and available on the DMS (link)

ANNEX B – BUSINESS IMPACT ANALYSIS METHODOLOGY

BIA PROCESS

The purpose of the Business Impact Analysis (BIA) process is to prioritize the different organizational components, so that product and service delivery can be resumed in a predetermined order, following a disruptive incident to the satisfaction of interested parties.

The products and services are prioritized first. This sets the time and service level parameters for process prioritization to deliver.

The integrity of the BCMS depends on the data obtained during the BIA and on the conclusions drawn from it. Each part of the BIA must be completed consistently, carefully, and thoroughly.

The prioritization is attributed by determining the impact of losing the availability of any resources to an organization. The BIA establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and supporting systems.

Compared to previous years, significant efforts have been made to improve the maturity of EFSA's Business Continuity Management System (BCMS) and adopt a holistic approach to Business Continuity with a more detailed process-oriented BIA that considers all aspects identified in BIA (e.g., people, building, IT systems and suppliers).

This will allow the collection of necessary information to develop the appropriate recovery strategies based on business continuity requirements and define plans for responding to a disruptive incident.

The following diagram displays the BIA lifecycle together with prerequisites and its relationship to strategy identification.

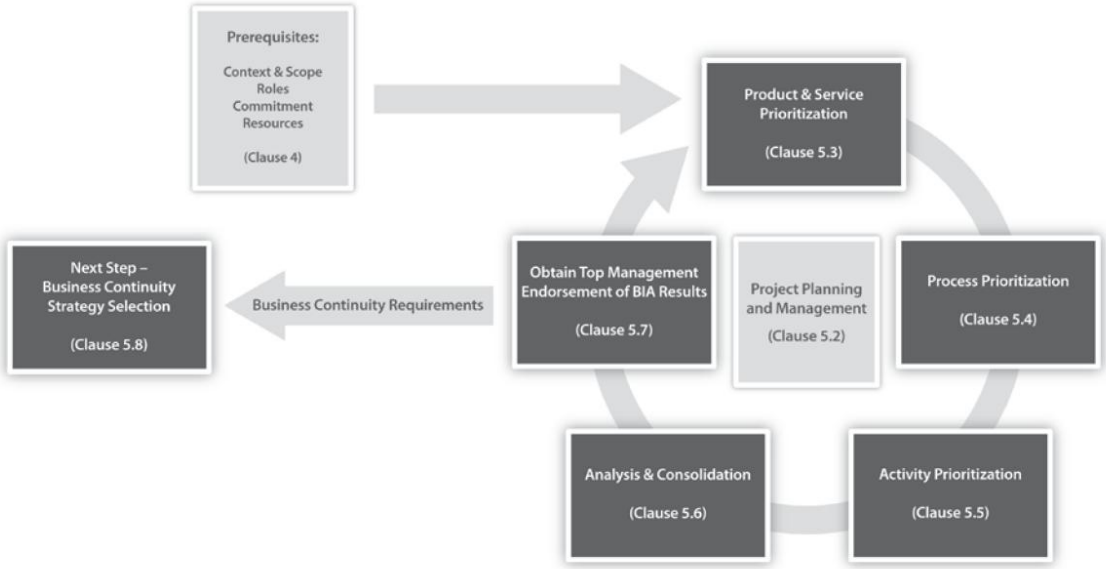


FIGURE 1 - BUSINESS IMPACT ANALYSIS LIFECYCLE WITH REFERENCES TO ISO 22317 CLAUSES

A combination of quantitative and qualitative methods is used to perform the BIA.
In particular, interviews are performed with key stakeholders and processes owners to gather insights into critical business processes, and to discuss resources need, obligations, and possible impacts if a disruptive incident were to affect the capability to deliver processes, products, or services.

Narrative scenarios of potential disruptions are evaluated using the worst-case approach, and different impact categories (e.g., financial, reputational, legal and regulatory) are discussed in qualitative terms, describing how disruptions might affect each area. Where possible, quantitative data is incorporated to quantify the potential financial impacts of disruptions.
Finally, cross checks are performed to ensure consistency and accuracy of findings.

The main sources of information for the BIA 2025 are:

- Document Review (former BIA 2024, EPA process charters and relevant operating procedures or documents available on DMS);
- Interview with the process owners / leaders;
- Relevant Regulations, Decisions of the Management Board.

BIA METHODOLOGY

The objectives of the Business Impact Analysis are:

- Identify EFSA's critical business processes / products;
- Identify the Maximum Tolerable Period of Disruption (MTPD) for each process, which indicates the time it would take for the adverse impacts of not providing a product/service or performing an activity to become unacceptable;
- Identify the Recovery Time Objective (RTO) for each process, which indicates the period of time following an incident within which a product, service or an activity must be resumed;
- Identify the key resources that support critical processes / products;

The execution of the BIA includes the macro-phases described in the following figure.

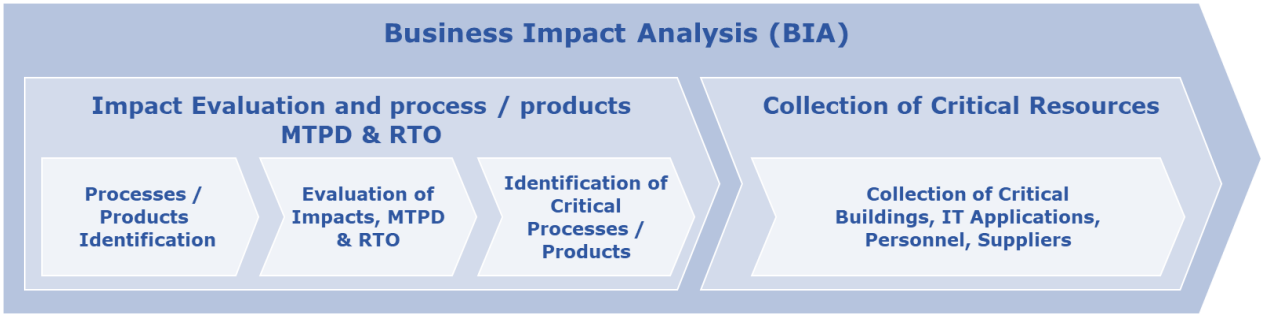


FIGURE 2 - BUSINESS IMPACT ANALYSIS PHASES

Impact Evaluation and Process MTPD & RTO

The business impact evaluation and the process Maximum Tolerable Period of Disruption (MTPD) and Recovery Time Objective (RTO) is the first phase of the BIA, and it involves interviews with the Process Owners or their delegates (e.g., process leaders) who typically have full understanding of the business elements / needs of their processes' continuity.

The main activities included in this phase are:

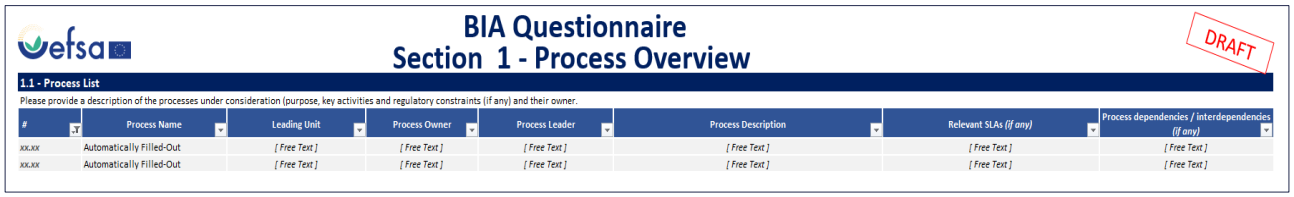
- Identification of the processes in scope of the BIA;
- Evaluation of the business impacts when a catastrophic event occurs and causes an interruption of the processes;
- Identification of the critical processes for the business continuity.

Before executing the BIA, the perimeter of analysis must be defined.

The target scope of the BIA 2025 is to assess the impact of the unavailability of each process identified by the EPA 3. Therefore, it is the basis for the implementation and improvement of EFSA's business continuity management system that has the scope to manage scientific advice and scientific and technical support for the European Community's legislation and policies in all fields which have a direct or indirect impact on food and feed safety.

For this activity, the updated list of EFSA's EPA processes and related process charters were gathered from the GPS Unit and considered when executing the new BIA.

In certain cases, processes were also divided into multiple parts, products or groups of products that could have different impact evaluations over time.


efsa

BIA Questionnaire
Section 1 - Process Overview

DRAFT

1.1 - Process List

Please provide a description of the processes under consideration (purpose, key activities and regulatory constraints (if any) and their owner.

#	Process Name	Leading Unit	Process Owner	Process Leader	Process Description	Relevant SLAs *(if any)*	Process dependencies / interdependencies *(if any)*
xx.xx	Automatically Filled-Out	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Free Text]
xx.xx	Automatically Filled-Out	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Free Text]

FIGURE 3 - BIA QUESTIONNARE: SECTION 1 – PROCESS OVERVIEW

After identifying the processes in scope, BIA interviews should be conducted to evaluate the impacts over time in case of process interruption, and identify for each process:

- the Maximum Tolerable Period of Disruption (MTPD) (i.e., the maximum amount of time after which the impact of a disruption to the processes would become unacceptable for the organization);
- the Recovery Time Objective (RTO) (i.e., the timeframe within which a process should be restored after an incident or disruption to avoid unacceptable impacts on the organization).

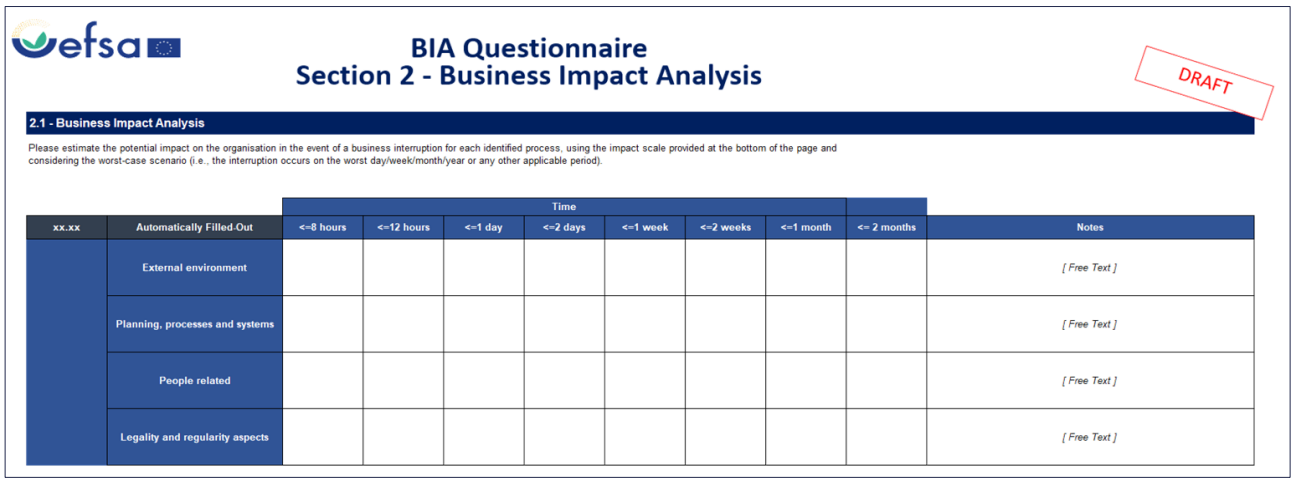
For the BIA 2025, impacts were evaluated over a timeframe ranging from 8 hours to 2 months, using the impact types and levels defined in the Impact Matrix provided by the European Commission (Figure 5).

In particular, the impact areas are:

- **External Environment**: considering the nature of EFSA business and entity, one of the most critical areas that could be affected and damaged in case of ineffective management of critical circumstances is the reputation. In fact, a negative reputation of the European institutions would produce a very consistent damage for all the activities carried out from the Agencies and from the Commission, with social and political potential consequences.
- **Planning, processes and systems**: due to the nature of EFSA's business, the unavailability of a process could lead to degradation of provided services, interruption or delay in the activities performed or could cause an increase of costs needed to produce deliverables as planned.

- **People related**: any effects that a disruption could have on people's health and safety, staff productivity or morale.
- **Legal and regularity aspects:** since EFSA is committed to provide a timely information and evaluation, reaching the legal deadlines agreed for the provision of a scientific advice is a focal point. Not respecting this kind of contractual terms could lead to litigations and legal exposure that could potentially affect the business activities, directly or indirectly (reflecting on a reputational level).

The tolerance threshold was set to level 2, indicating the maximum acceptable impact.



efsa

BIA Questionnaire
Section 2 - Business Impact Analysis

DRAFT

2.1 - Business Impact Analysis

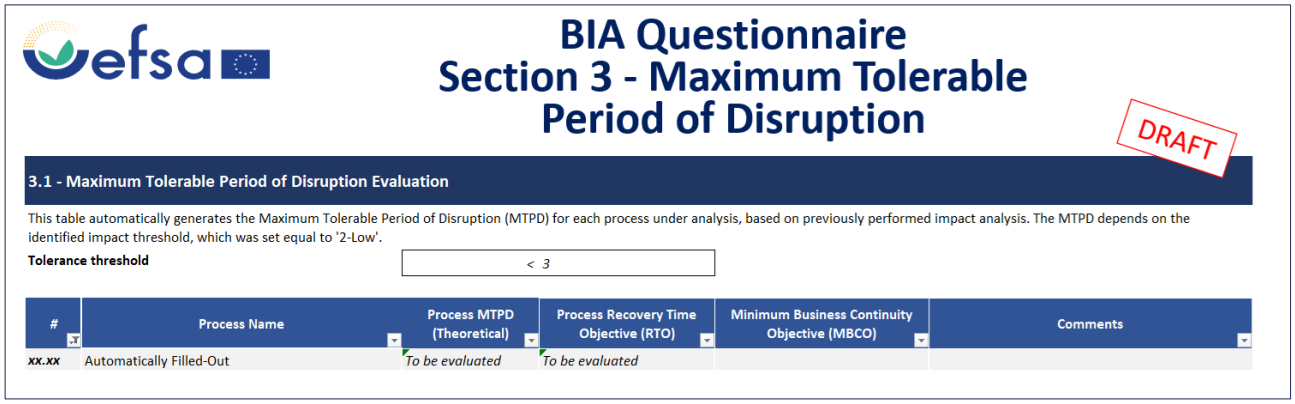
Please estimate the potential impact on the organisation in the event of a business interruption for each identified process, using the impact scale provided at the bottom of the page and considering the worst-case scenario (i.e., the interruption occurs on the worst day/week/month/year or any other applicable period).

		Time								
xx.xx	Automatically Filled-Out	<=8 hours	<=12 hours	<=1 day	<=2 days	<=1 week	<=2 weeks	<=1 month	<= 2 months	Notes
	External environment									[Free Text]
	Planning, processes and systems									[Free Text]
	People related									[Free Text]
	Legality and regularity aspects									[Free Text]

FIGURE 4 - BIA QUESTIONNAIRE: SECTION 2 – BUSINESS IMPACT ANALYSIS

Business impact types	Measurement criteria	Impact levels				
		1 - Very Low	2 - Low	3 - Medium	4 - High	5 - Major
External environment						
Damage to political relations	Extent of damage	Negligible or no damage	Moderate damages	Consequential damages	Significant damages, adversely affect(s)	From serious to exceptionally grave damages; Raise tension or formal protest
Impaired political decision/execution	Extent of delay (time)	**delay**: One week or negligible **Financial impact**: Less than 0,01%	**delay:** One month or moderate **Financial Impact** 0,01% to 0,1%	Three to five months or consequential delay Financial Impact 0,1% to 2%	Six months or significant delay Financial Impact: 2 to 5% budget	From one year or serious delay to exceptionally grave delay, or abandoned execution Financial Impact : More than 5%
Damage to Commission's partner	Extent of damage	damage : Negligible or no damage Financial impact: Less than 0,01% of budget	damage : Moderate Financial impact: 0,01% to 0,1% of budget	damage : Consequential Financial impact: 0,1% to 2% of budget	damage : Significant, adversely effects Financial impact: 2 to 5% of budget	Serious to Exceptionally grave damage Financial impact:more than 5% of budget
Damage to reputation/image	Extent of negative publicity	Extent of negative publicity: Negligible or no damage	Extent of negative publicity: Moderate/ local negative publicity	Extent of negative publicity: Consequential or limited to 3 EU countries	Extent of negative publicity: Significant or limited to 5 EU countries	Extent of negative publicity: More than serious, Europe wide or worldwide negative publicity
Damage to public order	Extent of damage	Negligible or no protest	Limited or very localised protest	Consequential, region wide protest, lightly injured people	Demonstrations national effects or injured people	Threaten stability, widespread effects/ individual or loss of life
Planning, processes and systems						
Impaired management control	Extent of problem	Negligible or no damage **Financial impact** less than 0,01%	Moderate damages **Financial Impact**: 0,01% to 0,1% of budget	**damages** consequential, affect executions **Financial Impact**: 0,1% to 2% of budget	**Damages:** Significant or impede important executions **Financial Impact**: 2 to 5% of budget	**Damages**: from serious to exceptionally grave, or from disrupt to abort critical execution(s) **Financial Impact**: More than 5% of budget
Degraded service	Extent of damage	Damages: Negligible or no damage Financial Impact : Less than 0,01% Delay : 1 day or less	Damages: Moderate Financial Impact : 0,01% to 0,1% Delay: 1 week or moderate (<10%)	Damages: Consequential Fincancial Impact: 0,1% to 2% Delay: 1 month or consequential (<25%)	Damages: Significant and adversely affect(s) Financial Impact: 2% to 5% Delay: 2 months or significant(<50%)	Damages: Serious to exceptionally grave Financial Impact : More than 5% Delay: 1 year or more or serious delay (>50%)
Unforeseen or additional costs	Financial (% of budget)	Financial Impact: Less than 0,01%	Financial Impact : 0,01% to 0,1%	Financial Impact: 0,1% to 2%	Financial Impact: 2% to 5%	Financial Impact: More than 5%
Loss of tangible assets	Financial (% of budget)	Financial Impact: Less than 0,01%	Financial Impact : 0,01% to 0,1%	Financial Impact: 0,1% to 2%	Financial Impact: 2% to 5%	Financial Impact: More than 5%
Budget overrun	Financial (% of budget)	Damages: Negligible or no damage Financial Impact : Less than 0,01%	Damages: Moderate Financial Impact : 0,01% to 0,1%	Damages: Consequential Fincancial Impact: 0,1% to 2%	Damages: Significant and adversely affect(s) Financial Impact: 2% to 5%	Damages: Serious to exceptionally grave Financial Impact : More than 5%
People related						
Health and safety	Number of incidents & extent of harm	No injuries	Minor injury(ies)	More than minor injury(ies)	Life of individual(s) threatened	From death of one individual to widespread loss of life
Damage staff morale/productivity	Extent of loss of morale	Negligible or no damage	Moderate damages	Consequential damages	Significant damages, adversely affect(s)	From serious to complete loss
Abuse of personal data	Extent of damage	Negligible or no damage	Moderate damages	Consequential damages	Significant damages, adversely affect(s)	From serious to exceptionally grave damages; Raise tension or formal protest
Legality and regularity aspects						
Impede law/rules enforcement	Extent of damage	Negligible or no damage	Moderate damages	Consequential damages	Significant damages, adversely affect(s)	From serious to exceptionally grave damages; Raise tension or formal protest
Penalties and legal liabilities	Financial (% of budget)	Damages: Negligible or no damage Financial Impact : Less than 0,01%	Damages: Moderate Financial Impact : 0,01% to 0,1%	Damages: Consequential Fincancial Impact: 0,1% to 2%	Damages: Significant and adversely affect(s) Financial Impact: 2% to 5%	Damages: Serious to exceptionally grave Financial Impact : More than 5%

FIGURE 5 - BIA QUESTIONNAIRE – IMPACT MATRIX



BIA Questionnaire
Section 3 - Maximum Tolerable Period of Disruption

DRAFT

3.1 - Maximum Tolerable Period of Disruption Evaluation

This table automatically generates the Maximum Tolerable Period of Disruption (MTPD) for each process under analysis, based on previously performed impact analysis. The MTPD depends on the identified impact threshold, which was set equal to '2-Low'.

Tolerance threshold < 3

#	Process Name	Process MTPD (Theoretical)	Process Recovery Time Objective (RTO)	Minimum Business Continuity Objective (MBCO)	Comments
xx.xx	Automatically Filled-Out	To be evaluated	To be evaluated		

FIGURE 6 – BIA QUESTIONNAIRE: SECTION 3 – MAXIMUM TOLERABLE PERIOD OF DISRUPTION

The results obtained during the BIA's first phase are analysed in order to identify the critical processes products.

A process is considered critical from a Business Continuity standpoint if its disruption / unavailability for up to 2 months could lead to unacceptable impacts on the organization (i.e., impacts equal to or higher than level 3).

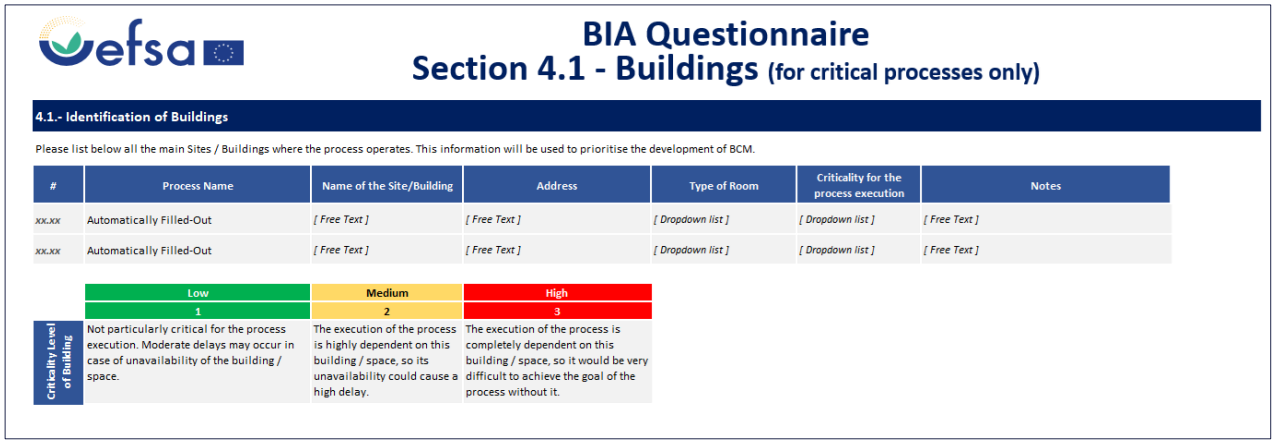
Collection of Critical Resources

This phase aims at collecting for each identified critical process the critical resources that will need to be in place to guarantee BC.

Information must be collected with the process owners / leaders or their delegates regarding the minimum necessary resources required to ensure continuity of critical processes at a minimum accepted service level after a disruptive event.

Such resources belong to the following categories:

- **Buildings:** for any site or building where the critical process operates, the dependency of the process execution is assessed on a scale from 1 (not dependent) to 3 (highly dependent).
- **IT Applications**: IT applications are mapped to critical processes and the dependency of the process execution on the IT application is estimated on a scale from 1 (not dependent) to 3 (highly dependent).
- **Personnel:** starting from the FTE plan shared by GPS, the minimum number of staff (headcounts) required to support the critical process in case of an emergency is estimated for each time period.
  In addition, information is collected about any critical staff and existing people-related Business Continuity Strategies (e.g., backup staff).
- **Suppliers**: information about any supplier supporting a critical process is collected and the dependency of the process execution on the supplier is estimated on a scale from 1 (not dependent) to 3 (highly dependent).
  Where present, existing supplier-related Business Continuity Strategies are gathered (e.g., existence of alternative suppliers, ability to insource activities) for critical suppliers.



BIA Questionnaire
Section 4.1 - Buildings (for critical processes only)

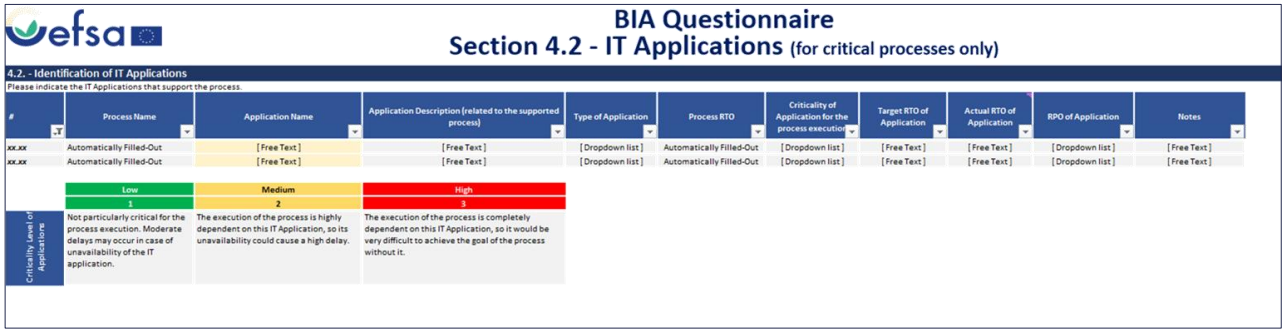
4.1.- Identification of Buildings

Please list below all the main Sites / Buildings where the process operates. This information will be used to prioritise the development of BCM.

#	Process Name	Name of the Site/Building	Address	Type of Room	Criticality for the process execution	Notes
xx.xx	Automatically Filled-Out	[Free Text]	[Free Text]	[Dropdown list]	[Dropdown list]	[Free Text]
xx.xx	Automatically Filled-Out	[Free Text]	[Free Text]	[Dropdown list]	[Dropdown list]	[Free Text]

Criticality Level of Building	Low	Medium	High
	1	2	3
	Not particularly critical for the process execution. Moderate delays may occur in case of unavailability of the building / space.	The execution of the process is highly dependent on this building / space, so its unavailability could cause a high delay.	The execution of the process is completely dependent on this building / space, so it would be very difficult to achieve the goal of the process without it.

FIGURE 7– BIA QUESTIONNAIRE: SECTION 4.1 – BUILDINGS



BIA Questionnaire
Section 4.2 - IT Applications (for critical processes only)

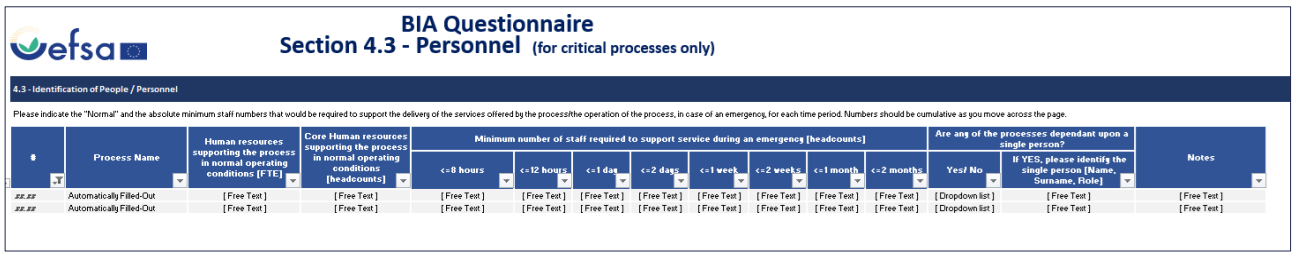
4.2. - Identification of IT Applications

Please indicate the IT Applications that support the process.

#	Process Name	Application Name	Application Description (related to the supported process)	Type of Application	Process RTO	Criticality of Application for the process execution	Target RTO of Application	Actual RTO of Application	RPO of Application	Notes
xx.xx	Automatically Filled-Out	[Free Text]	[Free Text]	[Dropdown list]	Automatically Filled-Out	[Dropdown list]	[Free Text]	[Free Text]	[Dropdown list]	[Free Text]
xx.xx	Automatically Filled-Out	[Free Text]	[Free Text]	[Dropdown list]	Automatically Filled-Out	[Dropdown list]	[Free Text]	[Free Text]	[Dropdown list]	[Free Text]

Criticality Level of Applications	Low	Medium	High
	1	2	3
	Not particularly critical for the process execution. Moderate delays may occur in case of unavailability of the IT application.	The execution of the process is highly dependent on this IT Application, so its unavailability could cause a high delay.	The execution of the process is completely dependent on this IT Application, so it would be very difficult to achieve the goal of the process without it.

FIGURE 8– BIA QUESTIONNAIRE: SECTION 4.2 – IT APPLICATIONS



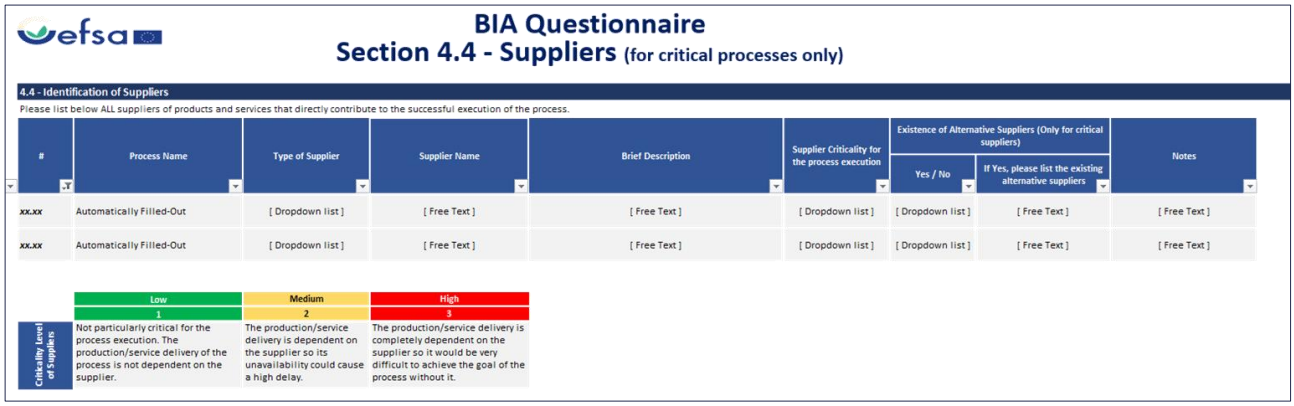
BIA Questionnaire
Section 4.3 - Personnel (for critical processes only)

4.3 - Identification of People / Personnel

Please indicate the "Normal" and the absolute minimum staff numbers that would be required to support the delivery of the services offered by the processithe operation of the process, in case of an emergency, for each time period. Numbers should be cumulative as you move across the page.

#	Process Name	Human resources supporting the process in normal operating conditions [FTE]	Core Human resources supporting the process in normal operating conditions [headcounts]	Minimum number of staff required to support service during an emergency [headcounts]								Are any of the processes dependant upon a single person?		Notes
				<=8 hours	<=12 hours	<=1 day	<=2 days	<=1 week	<=2 weeks	<=1 month	<=2 months	Yes/ No	If YES, please identify the single person [Name, Surname, Role]	
zz.zz	Automatically Filled-Out	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Dropdown list]	[Free Text]	[Free Text]
zz.zz	Automatically Filled-Out	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Free Text]	[Dropdown list]	[Free Text]	[Free Text]

FIGURE 9– BIA QUESTIONNAIRE: SECTION 4.3 - PERSONNEL



BIA Questionnaire
Section 4.4 - Suppliers (for critical processes only)

4.4 - Identification of Suppliers

Please list below ALL suppliers of products and services that directly contribute to the successful execution of the process.

#	Process Name	Type of Supplier	Supplier Name	Brief Description	Supplier Criticality for the process execution	Existence of Alternative Suppliers (Only for critical suppliers)		Notes
						Yes / No	If Yes, please list the existing alternative suppliers	
xx.xx	Automatically Filled-Out	[Dropdown list]	[Free Text]	[Free Text]	[Dropdown list]	[Dropdown list]	[Free Text]	[Free Text]
xx.xx	Automatically Filled-Out	[Dropdown list]	[Free Text]	[Free Text]	[Dropdown list]	[Dropdown list]	[Free Text]	[Free Text]

Criticality Level of Suppliers	Low	Medium	High
	1	2	3
	Not particularly critical for the process execution. The production/service delivery of the process is not dependent on the supplier.	The production/service delivery is dependent on the supplier so its unavailability could cause a high delay.	The production/service delivery is completely dependent on the supplier so it would be very difficult to achieve the goal of the process without it.

FIGURE 10– BIA QUESTIONNAIRE: SECTION 4.4 - SUPPLIERS

ANNEX C – BUSINESS CONTINUITY RISK MANAGEMENT METHODOLOGY

The risk management process is carried out periodically, at least annually, and facing any changes that may have possible impacts on the ISO 22301 BCMS and in general on the environment in which the business structure operates. Risk assessment results will be integrated within EFSA annual planning cycle and control activities.

The process involves the implementation of the following phases:

- **Phase 1: Scope and reference risks** aims to identify the business assets in scope of the process, the reference list of risks with potential business continuity impacts and the relevant norms and standard for EFSA.
- **Phase 2: Risk applicability** aims to identify for each risk with potential business continuity impacts the type of business assets to which apply (e.g., building, personnel).
- **Phase 3: Risk analysis** aims to assess the characteristics of the risks by determining their likelihood and potential consequences (impacts). Existing mitigation measures are also identified. Outcome of this phase is estimate of both an inherent and residual risks. The goal is to provide a solid basis for the subsequent evaluation and prioritization of risks.
- **Phase 4: Risk Evaluation** aim to calculate the current risk based on a matrix that combines the dimensions of likelihood and impact as assigned to each scenario. Risk evaluation involves comparing the results of the risk analysis with a set of established risk criteria to determine where additional action is required.
- **Phase 5: Risk treatment** consists in creating a summary of all the risks studied in order to define a risk treatment strategy.

The phases of the risk management process are shown in the following diagram:

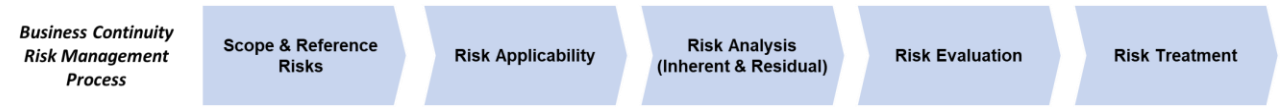


FIGURE 11 - PHASES OF THE BUSINESS CONTINUITY RISK MANAGEMENT PROCESS

SCOPE & REFERENCE RISKS

The purpose of this first phase is to identify the business assets in scope of the risk management process and the reference list of risks with potential business continuity impacts.

The **business assets** in scope of business continuity risk management are those resulting critical from the Business Impact Analysis. Not critical business assets are considered out of scope from the BC Risk Management process due to their limited impacts from a continuity standpoint. The business assets belong to three different categories, specifically building, personnel and suppliers. IT Infrastructure / IT Applications represent another category of critical business asset for EFSA, but the continuity risks (from a technological perspective) related to them are analysed as part of the Information Security Risk Management process (i.e., availability of information is one of the core scenarios analysed in there).

The single business assets emerging from BIA in scope of business continuity risk management process could also be consolidated whenever there is limited value added in analysing them separately. However, despite business assets are evaluated in a consolidated manner, mitigation

measures (existing and potential) could be considered with the adequate level of details (e.g., by process with regards of personnel and supplier).

Regarding **business continuity risks,** a reference list has been defined based on elements emerged from the analysis of external reports, past incidents experienced by the organization and BIA execution. The list includes a set of risks with related description belonging overall to three different macro risks coming from EFSA corporate risk approach, specifically: 1.1. Macro environmental risks, 2.2 Risks related to operational processes and 3.4 Risks related to the safety of staff, buildings, and equipment.

RISK APPLICABILITY

The purpose of this phase is to identify for each risk with potential business continuity impacts the type of business assets to which they apply (e.g., building, personnel).

Specifically, some risks (e.g., Terrorist Attack) have been considered applicable to one or more categories of assets (building and personnel), others to a single category of assets.

RISK ANALYSIS

The purpose of this phase is to assess the characteristics of the risks by determining their likelihood and potential consequences (impacts). Existing mitigation measures are also identified. Outcome of this phase is an estimation of both inherent and residual risks.

Specifically, first step is to evaluate the **inherent impact and likelihood** for the assets in scope and the related applicable risks:

- Inherent impact evaluations are based on impact evaluations coming from BIA related to the processes supported by the specific business asset under analysis (please note that BIA, Information Security Risk Assessment and BC Risk assessment are using the same impact matrix defined from European Commission, evaluating 4 different impact categories - External environment; Planning, processes, and systems; People related; Legality and regularity aspects - against 5 different severity levels - Very High, High, Medium, Low, or Very Low. See Figure 5 - BIA QUESTIONNAIRE – IMPACT MATRIX for details)
- Inherent likelihood evaluations are based on historical data and / or external reports, providing estimates of likelihood (the reference values adopted for likelihood are present in Table 1 - Risk Likelihood Level)

Risk Likelihood Level	**Nearly certain**	5	• The risk event has a very high likelihood of occurrence in a 5 years time horizon. • The risk event has occurred frequently in the last 2.5 years. • The risk event occurs in most of the cases • Probability 70 – 100 %
	Verv likely	4	• The risk event has a high likelihood of occurrence in a 5 years time horizon. • The risk event occurred in the last 2.5 years. • The risk event occurs in many cases • Probability 50 - 70 %
	Likely	3	• The risk event has a medium likelihood of occurrence in a 5 years time horizon. • The risk event has occurred several times in the last 5 years. • The risk event might occur in several cases • Probability 30 – 50 %
	Rather unlikely	2	• The risk event has a low likelihood of occurrence in a 5 years time horizon.

			• The risk event has occurred at least one time in the last 5 years. • The risk event is unlikely to occur • Probability 10 – 30 %
	Unlikely	1	• It is expected that the risk event will not occur in a 5 years time horizon. • The risk event has not occurred in the last 5 years. • The risk event occurs only in exceptional circumstances • Probability 0 – 10 %

TABLE 1 - RISK LIKELIHOOD LEVEL

The inherent impact and likelihood combined together provide the **inherent risk** for the specific business asset under analysis and related applicable threats.

The second step is to **collect the mitigation measures in place**, specifically:

- The existing measures can reduce both impact and / or likelihood;
- Existing Business Continuity measures should be included among the measures to be considered.

The final step is to evaluate, depending on the nature of the implemented mitigation measures and potential limitations regarding their effectiveness, the **residual impact, residual likelihood, and consequently residual risk.**

RISK EVALUATION

The **residual risk** is a function of the values of residual impact and likelihood and is evaluated on a business asset for a specific risk.

The calculation of the **current risk** is obtained using the following matrix that combines the dimensions of **likelihood** and **impact** as assigned to each risk and it is valued on a scale of 3 values: **Low**, **Moderate**, **High**.

Risk Heatmap

Likelihood	Likelihood rating						
	Nearly Certain	5					
	Very Likely	4					
	Likely	3					
	Rather Unlikely	2					
	Unlikely	1					
			1	2	3	4	5
		Impact Rating	Very Low	Low	Medium	High	Very High
		Impact					

LOW	**Acceptable AS IS** No action is to be undertaken
MODERATE	**Tolerable under control** A follow-up in terms of risk management is to be conducted and actions are to be set up in the framework of continuous improvement over the medium and long term (between 1 and 3 years)
HIGH	**Unacceptable** Measures for reducing the risk must absolutely be taken in the short term (< 1year)

FIGURE 12 - RISK MATRIX

The calculated current risk must be appropriately managed by implementing any additional security controls depending on whether or not the **risk acceptance level** is exceeded.

RISK TREATMENT

The purpose of this phase is to create a summary of the **risks and related business assets** identified and to define a **risk treatment strategy**.

For each risk, it is important to agree on **acceptance thresholds** of the risk level to be achieved in case of non-acceptance. The decision is to develop **treatment actions** for any risk that is **Moderate** or **High**.

LOW	Acceptable as Is. No action is to be undertaken
MODERATE	Tolerable under control. A follow-up in terms of risk management is to be conducted and actions are to be set up in the framework of continuous improvement over the medium and long term (between 1 and 3 years)
HIGH	Unacceptable. Measures for reducing the risk must absolutely be taken in the short term (< 1year).

Any risks raised would be registered in the **IMS tool**[8] (once available) to allow visibility and approval of the action plan.

The risk treatment phase aims to determine the calculated **risk treatment options**, for each risk in the risk analysis phase, and to identify the **treatment actions** to be implemented in order to reduce the value of the current risk to a level deemed acceptable (risk appetite).

The possible **treatment options** of the current risk, identified in this methodology, are the following:

- ***Transfer risk***: transfer the risk to a third party.
- ***Mitigate risk***: implement new control or improve existing ones in order to reduce the current risk to a level deemed acceptable.
- ***Accept risk***: maintain the same level of risk without implementing additional mitigating actions, where the current risk associated with the threat meets the established risk acceptance criteria.
- ***Avoid risk***: stop, modify, or avoid performing one or more activities that gave rise to the risk, so that the source of the threat is no longer active.

The choice of the most appropriate treatment option is made starting from the results of the risk analysis activity and on the basis of a cost-benefit analysis by the BCO with the support of involved Unit(s), e.g., jointly evaluating the cost of implementing the **treatment option** and the expected benefits. Treatment options are reviewed and approved by the Head of Unit, who is the process owner for the identified risk on the business asset and by Agency Security Committee, responsible for decisions in the context of security measures having impact on EFSA staff or stakeholders (as per Administrative Act 39).

The **actions** to be taken for the correct implementation of the chosen treatment option are reported in IMS tool in relation to the risk mitigated, the owner is identified and effective implementation by the established closure date is appropriately monitored.

[8] In the absence of the IMS tool, the risks will be registered on "F04_01 - Register of complaints, NC, CA, near misses"

INFORMATION SECURITY AND BUSINESS CONTINUITY RISK MANAGEMENT DEPLOYMENT TIMELINES

The Information Security and Business Continuity Risk Assessment must be updated / executed with a yearly frequency, preferably during the period January – August of the year. Assessments can be also started whenever a specific need / change in the context arise. Instead, management of identified risks (e.g., mitigate actions) can be performed continuously in line with specific risk management plans defined case by case.

ANNEX D – BUSINESS CONTINUITY EXERCISE MANAGEMENT

Agency Security Committee (ASC) Chair approves the security and BC exercise(s) annual planning.

Business Continuity Officer (BCO) is responsible for planning, conducting, and evaluating exercise activities.

BC Exercises are conducted under the responsibility of BCO. If deemed appropriate on the basis of the extent and complexity of the exercise, external qualified personnel may be addressed.

A Test is a particular kind of exercise, involving the expectation for an element to pass (or fail) within any given objective. It is usually employed when testing the trustworthiness and functionality of technologies and of IT procedures.

Exercise must be managed in line with ISO 22398 - Guidelines for Exercises.

Any given exercise program should begin simply and then gradually become more complex in line with the BC maturity of the organisation.

Any kind of exercise should be carefully planned in order to maximize its benefits, considering also the time spent in developing and performing it.

Exercises should be realistic and should minimally affect operations.

In order to deliver an exercise, the following three steps should be followed:

- Planning;
- Conducting;
- Evaluating and Reporting.

Exercise methods can be grouped into two categories:

- Discussion-based exercises - structured moments are set up, during which the participants peruse the relevant plans, analyse the relevant issues and highlight any and all flaws present, without being weighed down by operational pressure and stress.
- Operations-based exercises – they are carried out through simulations with the exercise activities conducted in real-life environments.

ANNEX E – PERFORMANCE EVALUATION

MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION

The BCO is in charge of how and what to assess, including the specific methods. Generally speaking, the assessments concern the following elements:

- the main objectives concerning the reduction of risks and the goals to be achieved;
- non-conformities and near misses;
- the specific results of exercises;
- the established reactions in case of a crisis;
- and/or simply monitoring events, in order to detect trends and/or signals, no matter how faint, liable to affect organisational resilience.

The regularity of such assessments is different according to the specific topics. Assessment results are formally analysed and verified during re-examination.

INTERNAL AUDITS

Those internal audits concerning the management system are programmed annually by the BCO, together with the relevant exercises; such activities are examined during the re-examination of the management system and are then reviewed by the CORSER HoU.

The audits have the following objectives:

- Verify that the activities to be carried out within the organisation comply with the management system;
- Verify that the activities to be carried out within the organisation comply with the ISO 22301 standard;
- Verify that the activities to be carried out within the organisation are then actually implemented and kept valid and up to date.

Internal audit may be carried out both by internal and external personnel, provided they are qualified. The qualification criteria needed are written on WIN_SOP 032_01 Internal ISO Audits, detailing the Internal Audit procedure.

The Lead Auditor entrusted with this task shall be completely independent from those areas and the activities that will be audited.

The Audit concerning the management system features the following phases:

- Planning the audit;
- Carrying out the audit, recording the relevant evidence;
- Archiving the documents arising from these activities.

Audits shall be carried out following the procedures detailed in WIN_SOP 032_01 Internal ISO Audits, examining the Internal Audit procedure.

MANAGEMENT REVIEW

The BCO shall review the performance and the correct implementation of the management system at least annually.

Such a review aims to:

- Provide ED with information on the status (including improvements) of the management system;
- Suggest ED the endorsement of those corrective or improvement actions deemed useful or necessary.

Management Reviews includes:

- Those actions and activities undertaken following the previous management reviews by the MS;
- The soundness of the Business Continuity policies undertaken by the organization;
- The opportunities for improvement;
- Audit results (be they internal or external on supply chain business continuity, whenever they are carried out;
- The output of exercises and tests;
- The Non-conformities having arisen during a specific period, as well as the status of the Corrective Actions;
- The effectiveness of the management system whenever the relevant conditions (be they internal or external) change;
- Any training activities carried out during the current year.

After verifying and discussing the aforementioned issues, the ED (or delegated person), in cooperation with the BCO shall confirm or modify the following, considering the output of the reviews and a framework of continuous improvement:

- The organisational policies on business continuity;
- Organizational performance and all related indexes;
- Objectives connected with risk reduction;
- The elements needing to be improved within the BCMS;
- The allocation of the relevant resources.

All the reviews of the management system are formal in nature and are documented through specific minutes.