

TECHNICAL SPECIFICATION

**ISO/TS
22317**

Second edition
2021-11

Security and resilience — Business continuity management systems — Guidelines for business impact analysis

*Sécurité et résilience — Systèmes de management de la continuité
d'activité — Lignes directrices pour l'analyse d'impact sur l'activité*



Reference number
ISO/TS 22317:2021(E)

© ISO 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Prerequisites	1
4.1 General	1
4.2 Context and scope	2
4.2.1 Context	2
4.2.2 Scope	2
4.3 Roles and responsibilities	2
4.3.1 General	2
4.3.2 BIA leader	2
4.3.3 Activity owners	3
4.4 Commitment	3
5 The BIA process	3
5.1 Fundamentals	3
5.2 Plan BIA	4
5.3 Agree approach for undertaking BIA process	4
5.3.1 Understand impacts	4
5.3.2 Define impact types and criteria	5
5.3.3 Define time frames	7
5.3.4 Define methodology	7
5.4 Determine products and services' priorities with top management	8
5.4.1 Overview	8
5.4.2 Inputs	8
5.4.3 Product and service priority determination	8
5.4.4 Outcomes	9
5.5 Determine the prioritized activities	9
5.5.1 Overview	9
5.5.2 Inputs	9
5.5.3 Identify activities	9
5.5.4 Set RTO for the activities	9
5.5.5 Define the prioritized activities	10
5.5.6 Results	10
5.6 Identify resources and other dependencies	10
5.6.1 Identify resource and other dependency requirements	10
5.6.2 Resource requirements	11
5.7 Analyse and consolidate BIA results	11
5.8 Obtain top management approval for BIA results	12
6 Review BIA	12
6.1 Review BIA process and methodology	12
6.2 Review BIA results	12
Annex A (informative) BIA within the BCMS of ISO 22301:2019	14
Annex B (informative) BIA information collection methods	15
Annex C (informative) Other uses for the BIA process	22
Annex D (informative) Examples for performing a BIA	25
Bibliography	36

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

This second edition cancels and replaces the first edition (ISO/TS 22317:2015), which has been technically revised. The main changes are as follows:

- the document has been updated to align with ISO 22301:2019;
- the document structure has been updated to improve the description of the business impact analysis (BIA) process;
- more focus has been placed on the BIA process and less on the business continuity programme;
- BIA and the BIA process have been clearly differentiated;
- BIA process roles have been consolidated to BIA leader and activity owners;
- the section “Initial BIA considerations” has been removed and the guidance redistributed;
- the section “Strategy selection” has been removed as it is part of ISO/TS 22331;
- the annex on terminology has been removed;
- the annex on BIA information collection methods has been enhanced;
- a new annex with examples for performing a BIA has been included.

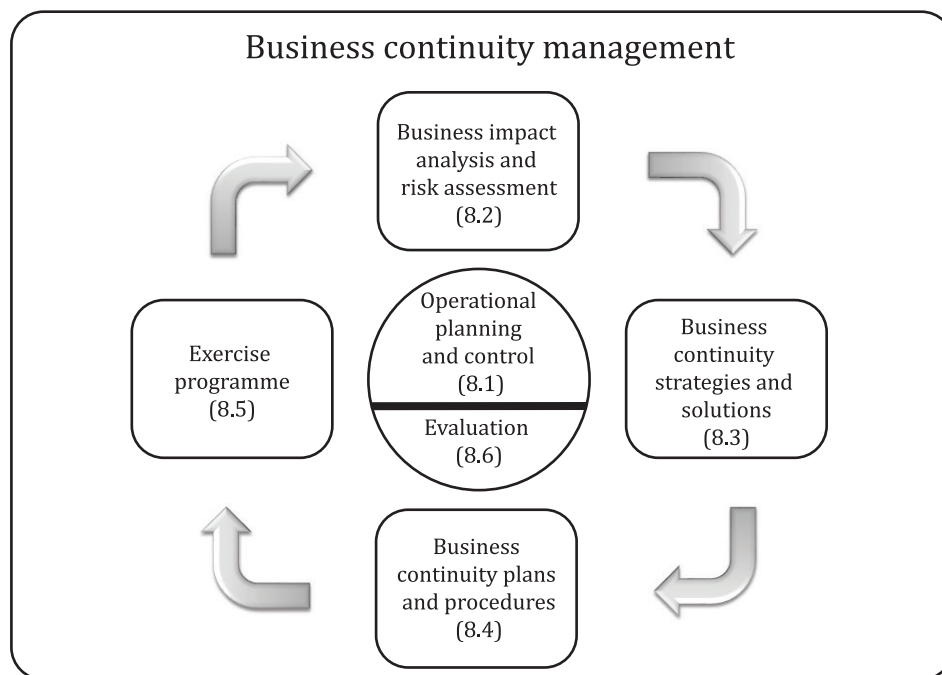
Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document provides detailed guidelines for implementing and maintaining a business impact analysis (BIA) process consistent with ISO 22301. This document is applicable to the performance of any BIA process.

The terminology used is consistent with ISO 22300 and ISO 22301, but an organization can use different terms provided they are clearly understood.

[Figure 1](#) notes the relationship of the BIA process to the business continuity management system (BCMS) as a whole. The organization should complete a cycle of the BIA process before business continuity strategies and solutions are selected.



NOTE Source: ISO 22313:2020, Figure 5.

Figure 1 — Elements of business continuity management

The BIA process analyses the effects of a disruption on the organization. The outcome is a statement and justification of business continuity priorities and requirements.

The first step in the BIA is the prioritization of products and services, which is followed by a number of process BIAs (optional) and activity BIAs. The scope of each of these BIAs can be limited, but together they should cover the entire BCMS scope. Organizations should review and perform the BIA process on a periodic basis (e.g. annually) and whenever there are significant changes within the organization or its context.

In this document, the terms “BIA” and “BIA process” are used as well as “result” and “outcome”. [Figure 2](#) depicts how these terms are used.

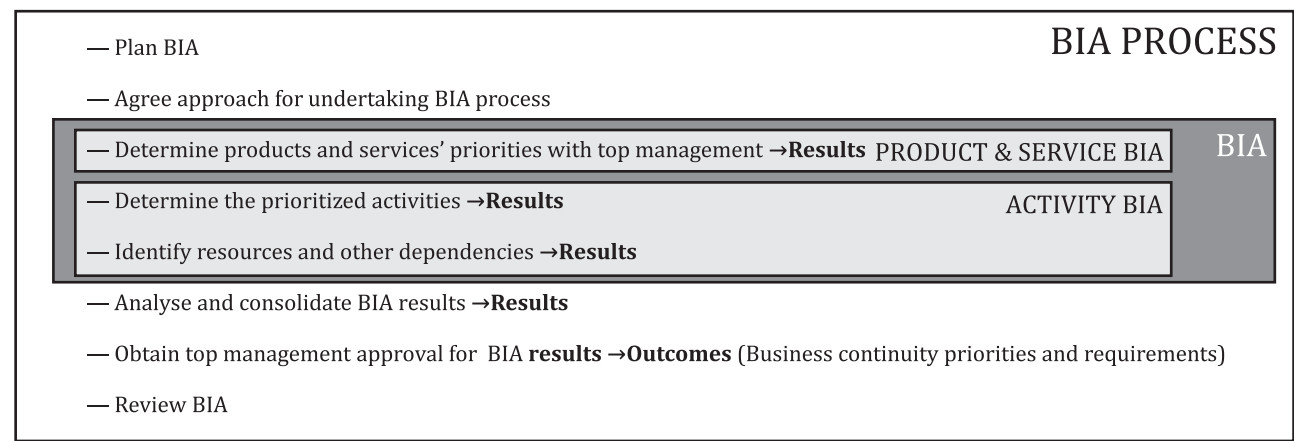


Figure 2 — Understanding BIA, BIA process, results and outcomes

The purpose of this document is to:

- provide a basis for implementing an effective BIA process within an organization;
- assist the organization with planning, conducting and reporting on the BIA process in a consistent manner.

This document provides examples for performing the BIA. It is important to note that these examples, individually or in combination, can help an organization achieve BIA outcomes. The selection of the most appropriate method will be influenced by the organization's size, sector, geography or context.

The outcomes of the BIA process include:

- endorsement or modification of the organization's BCMS scope;
- identification of legal, regulatory, and contractual requirements (obligations) and their effect on business continuity priorities and requirements;
- evaluation of the impact of a disruption over time on the organization, which serves as the justification for business continuity priorities and requirements;
- estimation of the time it would take for adverse impacts to products and services to become unacceptable [maximum tolerable period of disruption (MTPD)] following a disruption;
- identification of the requirements [MTPD and recovery time objective (RTO)] for the prioritized activities;
- identification of the resources needed to perform prioritized activities following a disruption, including their dependencies, and requirements, specifying RTOs and applicable recovery point objectives (RPOs);
- identification of dependencies including suppliers, partners and other interested parties;
- identification of the interdependencies of prioritized activities.

Figure 3 shows the BIA process, along with its prerequisites and its relationship to the selection of business continuity strategies and solutions. The clauses referred to in the diagram correspond to subclauses of this document.

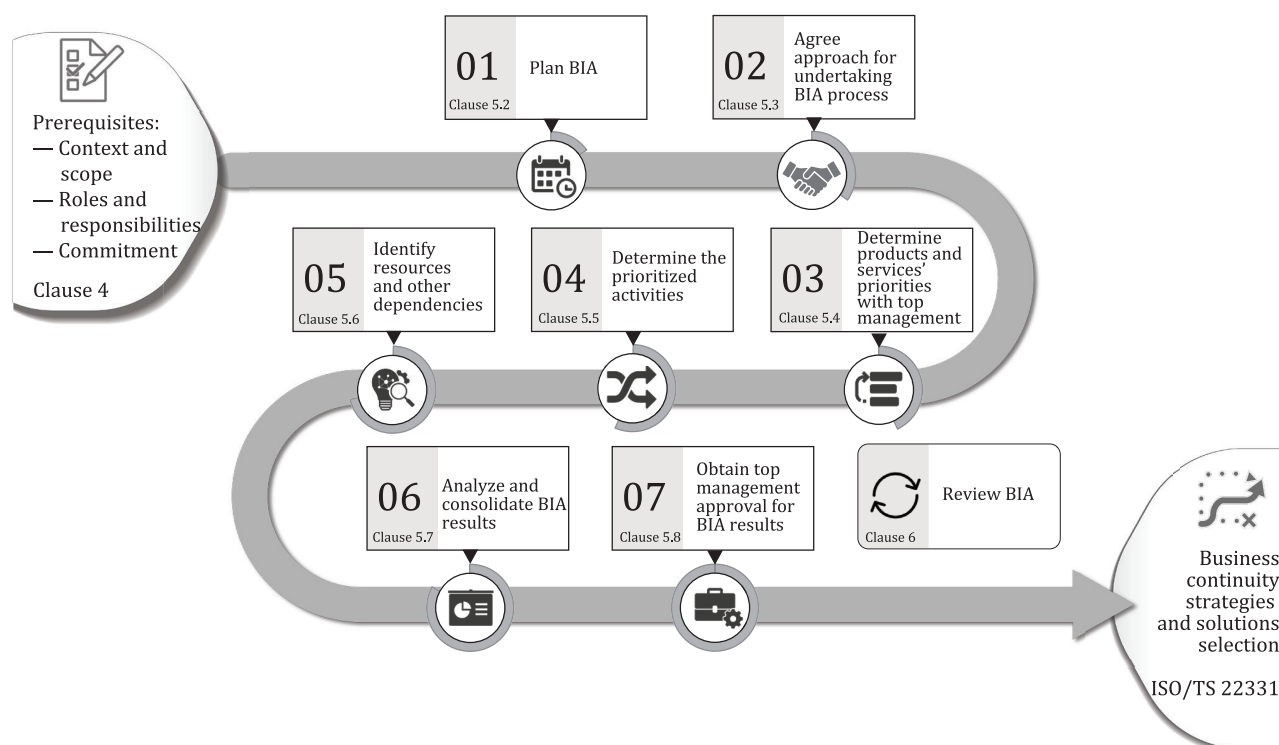


Figure 3 — BIA process

The organization should use the statement of business continuity priorities and requirements to select business continuity strategies and solutions.

The BIA can cause the organization to reconsider how it delivers its products and services.

The BIA depends on information being provided by many people across an organization who can have different perspectives on how the organization operates, what is time-critical or what impacts can occur following a disruption. Commonly, some overstate their requirements, while others understate theirs. This document seeks to define an approach that provides sufficient objectivity and minimizes these issues to produce effective outcomes.

Security and resilience — Business continuity management systems — Guidelines for business impact analysis

1 Scope

This document gives guidelines for an organization to implement and maintain a formal and documented business impact analysis (BIA) process appropriate to its needs. It does not prescribe a uniform process for performing a BIA.

This document is applicable to all organizations regardless of type, size and nature, whether in the private, public or not-for-profit sectors. The guidance can be adapted to the needs, objectives, resources and constraints of the organization.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22300, *Security and resilience — Vocabulary*

ISO 22301, *Security and resilience — Business continuity management systems — Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and ISO 22301 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

4 Prerequisites

4.1 General

While this document is consistent with the requirements of ISO 22301, it can be used to implement and review any BIA process.

Before commencing the BIA process, the organization should:

- define the context and scope of the BIA process (see [4.2](#));
- define and communicate roles and responsibilities (see [4.3](#));
- obtain leadership commitment and allocate adequate resources (see [4.4](#)).

NOTE See [Annex A](#) for a mapping of each clause to ISO 22301.

4.2 Context and scope

4.2.1 Context

The outcomes of the BIA process are dependent on the organization's understanding of the following, so that it can achieve its purpose by delivering its products and services to customers:

- the external environment (including suppliers, statutory and regulatory bodies) in which it operates;
- the internal operating environment, inclusive of business processes, activities and resources, as well as the potential impact caused by disruption to the delivery of products and services;

NOTE In organizations operating within a non-commercial environment, the "customer" can be the public or an overseeing authority, such as the government.

4.2.2 Scope

The BIA process should cover the whole of the BCMS scope. The organization should have defined and documented the scope of the BCMS in terms of its products and services. The outcomes of the BIA process can require the organization to reconsider the scope of the BCMS by adding or removing products and services.

The organization should first prioritize all products and services in scope which can include internal strategic services (see [5.4.3](#)). Those with higher priorities can be addressed first.

4.3 Roles and responsibilities

4.3.1 General

Top management should ensure:

- responsibilities and authorities for relevant roles are assigned and communicated within the organization;
- that persons leading the BIA process are competent;
- resources necessary to perform the BIA process are provided.

Top management should ensure that the following roles (other roles can be appropriate) to perform the BIA process are appointed:

- a) BIA leader (this can be the same person as the BCMS manager) (see [4.3.2](#));
- b) activity owners (see [4.3.3](#)).

4.3.2 BIA leader

The BIA leader is responsible for the BIA process and should:

- ensure people with the required competencies are available to enable the BIA process;
- prepare and deliver the BIA methodology;
- plan and manage the BIA process;
- make sure that the information provided by the activity owners is consistent throughout the organization;
- undertake consolidation and analysis of the information provided by the activity owners;
- present the outcomes to top management for approval.

4.3.3 Activity owners

Activity owners should:

- provide a detailed understanding of the activity for which they are responsible, including all of the resources that enable the activity to operate;
- provide information regarding existing workarounds, business processes and resources that influence the business continuity priorities and requirements;
- apply BIA methodology and provide the relevant information to the BIA leader.

4.4 Commitment

Top management commitment to the BIA process is necessary to ensure effective participation. They should:

- a) communicate the value of the BIA process;
- b) provide ongoing support for the BIA process;
- c) provide sufficient resources for the BIA process to:
 - 1) fulfil BIA process-specific roles and responsibilities, as well as training and awareness requirements, in adequate time;
 - 2) meet the changing requirements of the organization;
- d) agree on the BIA methods, priorities and time frames;
- e) ensure an environment that enables continual improvement within the organization;
- f) approve the outcomes of the BIA that ensure:
 - 1) business continuity priorities and requirements are aligned with organization's objectives and strategic direction;
 - 2) the organization meets its legal, contractual and customer requirements during a disruption;
 - 3) products and services, business processes, activities and resources are appropriately aligned;
- g) ensure that BIA outcomes are available when selecting business continuity strategies and solutions.

5 The BIA process

5.1 Fundamentals

The BIA process prioritizes activities and resources so that product and service delivery can be resumed in a predetermined time frame and at a predefined capacity following a disruption, to the satisfaction of interested parties. The outcomes are the business continuity priorities and requirements.

The quality of the BIA process and its outcomes is key to selecting appropriate business continuity strategies and solutions.

The timeliness of achieving quality BIA outcomes is key to minimizing impacts in case of a disruption. If some information is incomplete, unavailable, confidential or withheld, these challenges should not delay the progression and completion of the BIA process. A balance between quality and timeliness should be found.

5.2 Plan BIA

Planning tasks can include:

- a) allocating necessary resources, including competent people to lead and participate in the BIA process;
- b) grouping products and services together when they have similar characteristics, e.g. they can be grouped by type, by geographic area or by line of business;
- c) identifying the organization's structure and the teams or individuals that can provide information about products and services, activities and resources;
- d) communicating expectations to all participants in the BIA process;
- e) establishing the plan, including activities for:
 - 1) obtaining top management's agreement on the approach for undertaking the BIA process (see [5.3](#));
 - 2) organizing meeting(s) with top management to determine products and services' priorities (see [5.4](#));
 - 3) identifying and selecting the information collection methods (see [Annex B](#));
 - 4) defining a template or tool to record the information collected (see [5.5](#));
 - 5) gathering information from the activity owners (see [5.5](#) and [5.6](#));
 - 6) analysing and consolidating the information received (see [5.7](#));
 - 7) obtaining top management approval for the results (see [5.8](#));
- f) gaining approval of the planned BIA process.

5.3 Agree approach for undertaking BIA process

5.3.1 Understand impacts

The BIA process explores, in a consistent manner, the organizational impact resulting from the disruption to the delivery of products and services. Disruption can come from within, from the supply chain or from other external sources – all of which can result in a disruption to the delivery of one or more products and services to customers and other interested parties.

The impacts on the organization resulting from the reactions of interested parties can include the examples given in [Table 1](#).

Table 1 — Impacts due to interested parties

Interested party	Examples of the impact
Existing customers and clients	Loss of revenue and market share Increasing complaints Contract penalties or litigation
Community	Loss of confidence
Potential customers and clients	Loss of potential business opportunities
Partner organizations	Reduced willingness and ability to continue to cooperate
Media and society	Negative effect on reputation, brand value and public opinion
Shareholders	Negative effect on current share price and future investment

Table 1 (continued)

Interested party	Examples of the impact
Creditors	Negative effect on debt payments and future finance requirements
Competitors	Loss of market share as competitors take advantage of the situation
Staff	Loss of key personnel (temporary or permanent)
Regulators and government	Penalties and rule changes Loss of license to operate

5.3.2 Define impact types and criteria

The organization can experience different types of impacts such as damage to reputation or business objectives, financial losses and litigation. Impact types are not the same as consequence types or categories as used in risk management. Impact is the result of a disruption on the organization. To compare and assess impacts that are very different in a consistent manner, the organization should define impact types and criteria.

The organization should define impact types to understand the impact over time of a disruption to the delivery of products and services. Top management should approve the proposed impact types and criteria.

The choice of impact types and criteria are influenced by the organization's sector, context and the nature of its activities, as well as organizational culture. The selection of one or more impact types and criteria, including the need for quantitative and qualitative impact information and the level of detail collected, should be suitable for the organization to select or justify business continuity priorities and requirements.

Impact types to be considered can include:

- business objectives;
- environmental;
- financial;
- health and safety;
- legal, regulatory and contractual;
- market share;
- operational;
- reputational.

An organization can consolidate impact types, for example, to the following:

- business objectives;
- financial;
- legal, regulatory and contractual;
- reputational.

To assess different types of impacts and their effect on the business, the organization can choose to define thresholds when the impact becomes unacceptable (see the examples in [Table 2](#)) or to define an impact matrix with defined criteria for each impact level and type (see the examples in [Table 3](#)). The criteria should be as objective and measurable as possible.

NOTE [Table 3](#) shows five levels but the number of levels can be adapted to the organization's needs.

Table 2 — Examples of thresholds for impact types

Impact type	Description	MTPD threshold
Business objectives	Failure to deliver on objectives or take advantage of opportunities	Negative deviation by x % on business objectives
Financial	Financial losses due to fines, penalties, lost profits or diminished market share	Viability threatened by loss higher than USD x in revenue or cost
Legal and regulatory	Litigation liability and withdrawal of license to trade	Regulator suspends operating licence
Market share	Loss of clients moving to competitors	New orders drop x %
Reputational	Negative opinion or brand damage	Leading news story

Table 3 — Examples of impact level criteria

Level of impact						
Impact type	0	1	2	3	4	5
Financial	None	Loss of < USD x in revenue or expense	Loss of ≥ USD x and < USD y in revenue or expense	Loss of ≥ USD y and < USD z in revenue or expense	Loss of ≥ USD z and < USD t in revenue or expense	Loss of ≥ USD t in revenue or expense
Market share	None	Loss of < x % customers to opposition	Loss of ≥ x % and < y % customers to opposition	Loss of ≥ y % and < z % customers to opposition	Loss of ≥ z % and < t % customers to opposition	Business failure due to loss of ≥ t % customers to opposition
Customer (e.g. electricity supply company)	None	Loss of electricity supply to < x % customers	Loss of electricity supply to ≥ x % and < y % customers	Loss of electricity supply ≥ y % and < z % customers	Loss of electricity supply to ≥ z % and < t % customers	Business failure due to loss of electricity supply to x zone or ≥ t % customers
Liability (inclusive of legal costs)	None	Liability < USD x < x claims	Liability ≥ USD x and < USD y ≥ x and < y claims Class action lawsuit	Liability ≥ USD y and < USD z ≥ y and < z claims Multiple class action lawsuits	Liability ≥ USD z and < USD t ≥ z and < t claims Multiple class action lawsuits	Liability ≥ USD t ≥ t claims
Regulatory	None	Little interest from regulator Possible request for a summary report post disruption Possible warning issued to public	Regulator takes an interest requesting regular updates Public warning issued	Regulator on site requesting formal report Fines > USD x and ≤ USD y	Suspension of licence Fines ≥ USD y	Business failure due to loss of licence

Table 3 (continued)

Impact type	Level of impact					
	0	1	2	3	4	5
Reputational	None	Some negative attention in local press or in social media not requiring a response	Negative attention reported via traditional news channels not requiring a response Social media complaints requiring response	Temporary negative regional attention reported via news channels requiring response Social media complaints requiring dedicated response team	Negative national attention extensive enough to engage external communications experts for traditional and social media Requires top management to be included in the response Pushing response video of top management through social media channels	Consistent negative media attention from traditional and social media Business failure due to perceived incompetence or loss of faith in the organization
Business objectives	None	Negative deviation < x % on business objectives	Negative deviation ≥ x % and < y % on business objectives	Negative deviation ≥ y % and < z % on business objectives	Negative deviation ≥ z % and < t % on business objectives	Negative deviation ≥ t % on business objectives

5.3.3 Define time frames

Impacts almost always increase over time. However, impacts do not always increase at the same rate. For instance, financial impacts can arise as contract penalties are incurred or as customers are lost, while reputational damage can occur suddenly at a point during the disruption.

To assess the magnitude of the impact over time, the organization can choose a set number of time frames at which to consider the magnitude of the impact (e.g. at 1 hour, at 6 hours, at 24 hours, at 3 days, at 1 week) or a set number of time frames within which to consider the increasing magnitude of impact (e.g. 0 to 1 hour, 1 to 6 hours, 6 to 24 hours). The chosen ranges can vary between organizations depending on their context.

5.3.4 Define methodology

A methodology should be defined to ensure that the same principles and criteria are applied when assessing all products, services and activities, regardless of when the assessment is done or the team responsible for the assessment.

The methodology should include the following:

- How to assess impacts over time using the agreed impact types, criteria and time frames. When assessing impacts over time, the analysis should assume that the disruption occurs at the worst possible moment, e.g. the peak operating period, the end of the financial month or the busiest time of year. The worst case should be documented.
- Identification of the time frame when a disruption becomes unacceptable to the organization (e.g. when at least one of the thresholds in [Table 2](#), or an unacceptable level of impact in [Table 3](#), is reached). This can be referred to as the MTPD.

- c) A set time frame for recovery of disrupted activities with a specified minimum acceptable capacity. This time frame can be referred to as the RTO and cannot be longer than the MTPD.

The outcomes described in this methodology are the minimum required to be consistent with ISO 22301. The organization can add additional tasks to the BIA process, such as collecting additional information or identifying single points of failure, as part of the information gathering sessions (see [Annex C](#)).

NOTE Examples can be found in [Annex D](#).

5.4 Determine products and services' priorities with top management

5.4.1 Overview

Top management should determine the priorities of products and services that the organization provides to its customers. This prioritization can be done by discussion, although other sources of input can be available. For example, it is possible that product and service prioritization have been previously performed as part of enterprise risk management. In these situations, the BIA process can consider those conclusions.

It is top management's responsibility to prioritize products and services because they:

- a) set the objectives of the organization;
- b) have the ultimate responsibility for ensuring the continuity of the organization and the fulfilment of its objectives;
- c) have the widest view of the entire organization from which to assess priorities;
- d) can choose to override contractual and other obligations in setting priorities in exceptional circumstances;
- e) are aware of planned future changes and other factors which can affect the business continuity priorities and requirements.

5.4.2 Inputs

To make decisions, top management should consider the following information:

- a) mission, objectives and strategic direction of the organization;
- b) BCMS scope;
- c) assessment of product and service priorities from a previous top management review;
- d) legal and regulatory requirements to which the organization, or specific products and services, are subject (as well as an assessment of the impact of breaching each requirement);
- e) contractual requirements, including penalties for failure to deliver products and services;
- f) expectations of customers and other interested parties;
- g) assessment of impacts for failure to deliver (see impact types in [5.3.2](#));
- h) lessons learned from past disruptions and exercises.

5.4.3 Product and service priority determination

Based on the impact types and criteria (see [5.3.2](#)), the defined time frames (see [5.3.3](#)) and the agreed methodology (see [5.3.4](#)), top management should decide, for each group of products and services, the time after which continued failure to deliver them becomes unacceptable to the organization. This

determines the minimum acceptable capacity for initial recovery and how quickly it will need to return to full capacity.

When necessary, top management should also agree on the priority of internal services, such as payroll and other employee-facing services. Some organizations can choose to treat internal services similarly to externally facing products and services.

The organization should retain documented information describing the reasons why decisions have been made.

5.4.4 Outcomes

The outcomes should be a list of prioritized products and services and their continuity requirements which will be used in activity prioritization (see [5.5](#)).

The outcome of the product and service prioritization can result in the modification of the organization's BCMS scope.

5.5 Determine the prioritized activities

5.5.1 Overview

It is important to understand the relationship between products and services, business processes and activities before setting the RTOs of the activities.

The priority of products and services influences the priority of their related activities. In cases where an activity is part of a business process, it is possible that the activity needs to be analysed together with the remaining activities in the business process. This can result in changes to the RTOs of activities.

5.5.2 Inputs

The inputs required to undertake activity prioritization include:

- a) scope of the BIA process;
- b) impact types and criteria (see [5.3.2](#));
- c) priorities for the products and services defined by top management (see [5.4](#));
- d) known dependencies;
- e) legal, regulatory, and contractual requirements (obligations).

5.5.3 Identify activities

For each product and service within the scope of the BIA process, the related activities should be identified by their activity owners.

5.5.4 Set RTO for the activities

Based on the impact types and criteria (see [5.3.2](#)), the defined time frames (see [5.3.3](#)) and the agreed methodology (see [5.3.4](#)), activity owners should assess the impacts over time resulting from a disruption, identify the MTPD and set the RTO in combination with the minimum acceptable capacity for each activity. This capacity can be represented as a metric such as a percentage or ratio of a level of service, or quantity of product.

The information collection methods that have been identified during planning (see [5.2](#)) and the selected template or tool should be used to document the analysis.

Each activity should be analysed, taking into consideration:

- a) fluctuations in demand or peak operating periods;
- b) additional factors that can affect the determination of business continuity priorities and requirements (e.g. backlogs or legal and regulatory requirements);
- c) the interdependencies on other activities (internal or external).

A list of activities sorted in ascending RTO order should be created.

5.5.5 Define the prioritized activities

Based on the activities' RTO, an organization should create a list of prioritized activities. Prioritized activities will require strategies and solutions. This requires information about resources and dependencies to be collected.

Making this selection will reduce the information to be collected but can result in no recovery solutions being defined for non-prioritized activities. In subsequent iterations of the BIA, the list of prioritized activities can be expanded.

Top management should sign off on the selection of prioritized activities.

5.5.6 Results

The results should be:

- a) the approved list of prioritized activities;
- b) for each activity:
 - 1) identification of interdependencies and relationships between products and services, and activities;
 - 2) impacts over time;
 - 3) corresponding MTPD;
 - 4) corresponding RTO;
 - 5) minimum acceptable capacity.

5.6 Identify resources and other dependencies

5.6.1 Identify resource and other dependency requirements

After determining the prioritized activities, the organization should obtain a detailed understanding of day-to-day resource requirements, to identify the resources necessary to recover or maintain prioritized activities. These include, but are not limited to:

- a) people;
- b) information and data (including vital records);
- c) physical infrastructure such as buildings, workplaces or other facilities and associated utilities;
- d) equipment (e.g. office equipment, manufacturing equipment, special tools, spare parts and components) and consumables (e.g. raw materials);
- e) information and communication technology (ICT) systems (e.g. applications, cloud services, remote access);

- f) transportation and logistics;
- g) finance;
- h) partners and suppliers.

5.6.2 Resource requirements

For the resources identified, the following information should be collected:

- a) Quantity, i.e. the amount or number of resources needed over time, and based on the activity RTO, the activity owner can determine to start their activity with the following:
 - 1) a decrease in the quantity of resources, e.g. recognizing that the activity can recommence with a reduced capacity; the activity owner must then increase the quantity of resources over time so that the activity eventually returns to its business as usual;
 - 2) the business as usual quantity;
 - 3) an increase in the quantity of resources, e.g. to resolve the backlog accumulated over the period that the business activity was disrupted or to respond to an anticipated spike in demand; consideration should be given to estimate the period of time the supplemental quantity of resources is to be released to return the activity to its business as usual level;
- b) time frame(s) in which the resources need to be available;
- c) characteristics of the resource: the information to be gathered in this case depends on the type of resource, e.g.:
 - 1) for staff and contractors, the minimum acceptable level for required service, knowledge, skills, authority or qualifications required should be defined;
 - 2) specification of IT equipment;
 - 3) current location;
- d) maximum tolerable data loss for information resources (the RPOs should not be greater than the maximum tolerable data loss);
- e) dependencies on other resources;
- f) applicable legal or regulatory requirements.

NOTE This information gathering can be carried out when setting the RTO for the activities.

Limitations imposed on resources, e.g. by logistics, should be taken into account when defining requirements.

During the resources requirements analysis, single points of failure can be discovered and should be documented and reported appropriately.

5.7 Analyse and consolidate BIA results

While analysis occurs throughout the BIA process, the organization should perform a final analysis (or consolidation of analyses). This involves reviewing validated and approved information gathered from all levels of the BIA process and drawing conclusions that lead to business continuity priorities and requirements.

The organization should choose the appropriate quantitative and qualitative analytical approach(es), which can be influenced by the type, size or nature of the organization, as well as resource and skill constraints. The approach(es) selected will also depend on the type of information gathered.

Regardless of approach, the organization should challenge and check the information to ensure that it is:

- a) correct: sufficiently accurate and reliable;
- b) credible: reasonable and justifiable;
- c) consistent: comparable, clear and repeatable;
- d) current: up to date and available in a timely manner;
- e) complete: comprehensive.

The consolidation can reveal incompatible or inappropriate recovery objectives that need to be reviewed with the activity owner and resolved. Furthermore, it can be necessary to adjust the RTO of predecessor activities to ensure successor activities can meet their set RTOs.

The results of analysing and consolidating information are the business continuity priorities and requirements.

5.8 Obtain top management approval for BIA results

The BIA leader should seek management approval of BIA results, including the prioritization of products and services, business processes (if applicable), activities and resources.

The organization should provide the following key BIA results to top management for their review, amendment (if necessary) and approval before moving on to next steps:

- product and service prioritization;
- business process prioritization (if undertaken);
- activity prioritization;
- confirmation of the original, or endorsement of the modified, BIA scope.

The approval of the BIA results by top management should be documented. Some organizations can choose to seek approval via a report or presentation to top management. A presentation should be chosen if the organization would benefit from debating the BIA results before approving or proposing an alternate conclusion. A report can be appropriate as a pre-read to a presentation or as the primary method of seeking approval, if recommended business continuity priorities and requirements and their justification are straightforward and likely not to require discussion.

The BIA results are used to identify and select business continuity strategies and solutions.

6 Review BIA

6.1 Review BIA process and methodology

The BIA process and methodology should be reviewed to continually improve its quality. Different approaches over time can be considered, changing, for example, impact types, time frames, information collection methods or participants to improve the quality of the results.

6.2 Review BIA results

BIA results should be reviewed on a periodic basis (typically annually) and whenever there are significant changes within the organization or the context in which it operates that can affect the business continuity priorities and requirements, such as:

- a) mergers and acquisitions;

- b) strategic directional changes;
- c) product or service changes;
- d) regulatory changes;
- e) customer and/or contractual changes;
- f) operational changes, including new/change application/ICT, supply chain (insourcing/outourcing) and site/facility resources;
- g) changes to the organization's structure;
- h) lessons arising from business continuity exercises and disruptions.

The activity owners should monitor their activities and top management should consider strategic changes to identify these triggers.

In areas of the organization which have changed little since the last BIA, it can be sufficient to validate the previous BIA results rather than conduct a full BIA.

Annex A (informative)

BIA within the BCMS of ISO 22301:2019

Table A.1 — BIA within the BCMS of ISO 22301:2019

ISO 22301:2019	This document
8.2 Business impact analysis and risk assessment	Introduction
8.3 Business continuity strategies and solutions	
Clause 4 Context of the organization	4.2 Context and scope
5.3 Roles, responsibilities and authorities	4.3 Roles and responsibilities
7.2 Competence	
5.1 Leadership and commitment	4.4 Commitment
8.2.2 a) define impact types and criteria ^a	5.3.2 Define impact types and criteria
8.2.2 b) identify activities ^a	5.5.1 Overview 5.5.3 Identify activities
8.2.2 c) use impact types to assess impact ^a	5.5.4 Set RTO for the activities
8.2.2 d) identify MTPD ^a	
8.2.2 e) set RTO ^a	
8.2.2 f) prioritize activities ^a	
8.2.2 g) determine resources ^a	5.6 Identify resources and other dependencies
8.2.2 h) determine dependencies ^a	
8.2 Business impact analysis and risk assessment	Clause 5 The BIA process
8.6 Evaluation of business continuity documentation and capabilities	Clause 6 Review BIA
^a Abbreviated from the full list-item text.	

Annex B **(informative)**

BIA information collection methods

B.1 General

This annex summarizes common methods to collect information necessary to deliver BIA results. No matter how information is collected, it should be collected in a consistent manner so that the information can be compared across the organization.

The BIA leader should consider the following factors which can influence the selection of the BIA information collection method or methods:

- information required to perform the analysis is intended to be objective or subjective;
- the BIA is being performed for the first time in the organization;
- participants can be influenced by personal or other biases which can misrepresent the true or balanced needs of the organization;
- business continuity is an understood concept and its benefits are known among interested parties;
- activities and resources within the scope of the BIA process have interdependencies;
- the number of activities that fall within the scope of the BIA process;
- skills and experience of business continuity practitioners implementing the BIA process;
- physical location(s) of those representing activities and their time constraints;
- maturity of other management systems implemented in the organization and their documented information.

Common methods of BIA information collection are:

- documentation review;
- interviews;
- surveys/questionnaires;
- workshops.

To ensure consistent information, regardless of information collection method:

- provide training for those who are leading or participating;
- identify information requirements;
- provide oversight or quality assurance of outputs;
- determine whether it is necessary to perform a trial of the information collection method before implementing it.

B.2 Document review

The BIA leader can find it useful to review documentation as background in preparing for interviews, developing survey questions, and eventually performing analysis-related work, such as:

- annual reports;
- business performance metrics;
- business process documentation;
- contractual requirements;
- customer-related service level agreements;
- data backup regime;
- equipment and ICT lists;
- existing business continuity capabilities;
- horizon scanning information;
- insurance policies;
- marketing materials;
- organizational charts;
- post-incident reports;
- previous BIA information;
- relevant BCMS documentation;
- roles and responsibilities;
- standard operating procedures describing day-to-day task execution;
- strategy documents.

B.3 Interviews

The BIA leader or delegate can perform interviews to enable discussion regarding day-to-day operations, resource needs, obligations and possible impacts if a disruption were to affect the activity's capability to deliver products and services. This method is appropriate when qualitative assessment is required.

There are many topics to be discussed during an interview including:

- BIA process overview, objectives, desired outcomes and the relationship of the BIA process to the remaining business continuity planning process;
- BIA participant expectations;
- activity discussion including:
 - activity overview and relationship to products and services and business processes, with emphasis on key tasks and the time frames necessary to perform the activity as a whole or the subordinate tasks (including fluctuations in demand or peak operating periods);
 - resource dependencies and requirements (see [5.6](#)), including existing workarounds and how long they remain viable;

- known impact associated with activity downtime;
- known activity-specific obligations;
- experience of disruptions;
- lessons learned;
- next steps, including a review of the interview summary, comments and corrections, and approval.

Interview good practice includes the following:

- prepare adequately, which often includes an agenda with instructions for the interview participant on preparing for the interview;
- research on the activity, in order to inform interview questions;
- repeat key information to ensure it was heard accurately;
- document an interview summary, solicit feedback and obtain approval.

Examples of questions for BIA interviews can include the examples given in [Table B.1](#).

NOTE The example questions can be altered to engage different interviewees, e.g. engaging process owners rather than activity owners.

Table B.1 — Examples of questions for a BIA interview

Topics	Questions
Interested parties (e.g. customers)	<ol style="list-style-type: none"> 1. Who are your internal and external interested parties, e.g. customers? 2. Do you have any business continuity-related contractual requirements or service level agreements impacting business continuity? If so, please describe.
Products and services	<ol style="list-style-type: none"> 1. What are the products and services that you provide? 2. How do you deliver your products and services? 3. Are there peak periods when products and services are delivered? If so, please describe. 4. How long does it take to produce products and services (cycle time)?
Activities	<ol style="list-style-type: none"> 1. What activities are you responsible for? 2. Where are these activities performed? 3. How do they contribute to products and services? 4. How do you describe each activity, focusing on its purpose and the tasks performed? 5. What does the activity produce and who receives it? 6. What are the possible impacts in the event of a business disruption?

Table B.1 (continued)

Topics	Questions
Resources	<ol style="list-style-type: none"> 1. People: Which roles or responsibilities are required to perform each activity? How many people perform each role and how many are needed to do a minimum level of work? 2. Information, data and ICT: <ol style="list-style-type: none"> a. What applications and data support each activity? What communication technologies do you need? Are there manual procedures that are also used? b. Do you require access to any electronic or hard copy records or documentation to operate? If so, where are they stored? c. Do you require any special software, hardware, settings, permissions, licences, etc.? If so, please describe. 3. Vital records: What non-digital (e.g. paper based) information do you need? 4. Physical infrastructure: Where are these resources located (e.g. offices, data centres, warehouses)? Do they require any specific physical infrastructure? 5. Equipment: What equipment or tools are necessary to operate? 6. What other resources are needed to perform each activity? 7. With current capabilities, if the resource becomes unavailable, how long will it take to become available?
Partners and suppliers	<ol style="list-style-type: none"> 1. Which third parties does your business unit and its activities rely upon? 2. What do these suppliers provide to you, when and how often? 3. How soon does the activity stop if the suppliers' products or services are not delivered?
Other dependencies	<ol style="list-style-type: none"> 1. What are the dependencies and interdependencies of each activity? 2. Which activities, in other business units, must be operational to enable your activity to produce its outputs?

B.4 Surveys or questionnaires

The BIA leader or delegate can use surveys or questionnaires to effectively collect discrete information, i.e. information with a finite number of possibilities or information that can be quantified.

This method is appropriate:

- where objective information can be collected;
- when information can be numerical or ranked;
- when the number of respondents is high.

Surveys can be delivered as:

- hard-copy documents;
- electronic documents;
- online survey service.

It is important that the questions be clear in their intent and language. A contact should be provided to resolve questions that the interviewee can have.

Common survey content can include the following:

- description of the activity in terms of its purpose and outputs;

- list of the activity's customers (internal and external);
- description of service level agreements or contractual obligations to deliver products and services;
- description of the impacts of a disruption on the activity and how they change over time, referring to the impact types considered by the organization (see 5.3.2);
- list of the activity's resource dependencies (location, people, equipment, ICT and third parties);
- peak times (daily, weekly, monthly, quarterly, seasonally, annually);
- other quantitative information.

B.5 Workshops

Workshops with participants representing different activities or business processes can be used to explain the BIA process and collect information. It is recognized that workshops produce higher quality results because they provide a forum for discussion, socialization of concepts and greater understanding by the participants.

This method is appropriate when rapid results are required.

Topics discussed in a workshop can be similar to those used in surveys and interviews; however, they add value by:

- producing additional, more complete information;
- having multiple respondents providing input and possibly challenging each other's answers;
- resolving competing, possibly unrealistic expectations.

B.6 Comparison of collection methods

Tables B.2 to B.5 provide a list of advantages, disadvantages, opportunities and tips for collection methods.

Table B.2 — Document review

Advantages	Disadvantages
<ul style="list-style-type: none"> — Potentially detailed and thought through — Evidence already exists/does not require additional effort or verbal communications — Leverages previous efforts/promotes cooperation — Easy to access 	<ul style="list-style-type: none"> — Time consuming — Lack of explanation and context — Can be out-of-date or incorrect — Needed information can be difficult to locate due to volume
Opportunities	Tips
<ul style="list-style-type: none"> — Information can come from many sources — Can enable the compilation of draft questionnaires/interview questions — Can confirm information collected by other methods 	<ul style="list-style-type: none"> — Pair with a meeting to ensure the context is understood — Read available documentation in preparation for interviews and workshops — Combine with other methods

Table B.3 — Interviews

Advantages	Disadvantages
<ul style="list-style-type: none"> — Involves staff and raises awareness — Interviewer gains knowledge of people and functions — Explores the topic in more detail 	<ul style="list-style-type: none"> — Time consuming — Can use more staff time — Questionnaire draft still needed — Subjective response — Potential lack of consistency if more than one interviewer
Opportunities	Tips
<ul style="list-style-type: none"> — Use of senior participants — Increase awareness of the BIA process — Identification of risks — Discuss lessons learned from previous disruptions 	<ul style="list-style-type: none"> — Formalize interview structure — Interview in location — Take time to explain purpose of the BIA process

Table B.4 — Questionnaires and surveys

Advantages	Disadvantages
<ul style="list-style-type: none"> — Easy to analyse — Easier to standardize response — Produces “hard-copy” evidence — Can be automated 	<ul style="list-style-type: none"> — Questionnaire fatigue — Interpretation of questions — Need to cross-check — Possibility of error in questions nullifying results — Lack of involvement — Miss soft issues — Miss major issues through not challenging the responses
Opportunities	Tips
<ul style="list-style-type: none"> — Potentially create awareness in all staff 	<ul style="list-style-type: none"> — Use database or spreadsheets for graphs — Keep information requirements streamlined — Use automated survey tools — Verify information — Combine with other methods

Table B.5 — Workshops

Advantages	Disadvantages
<ul style="list-style-type: none"> — Cross-activity perspective — Brainstorming — Shows organization's commitment — Fewer distractions — More professional 	<ul style="list-style-type: none"> — Difficult to timetable — Difficult to deal with dissent and internal politics in a group — Facilitation skills required — Lots of preparation
Opportunities	Tips
<ul style="list-style-type: none"> — High level of commitment — Can also be used to raise awareness of business continuity 	<ul style="list-style-type: none"> — Sell to management based on cost savings — Prepare it well — only get one chance! — Retain focus on impacts, not causes

Annex C (informative)

Other uses for the BIA process

C.1 Collect additional information during the BIA process

The BIA process described in this document comprises only the information required to prioritize activities and resources. This then provides business continuity priorities and requirements necessary to identify and select appropriate business continuity strategies and solutions.

Conducting a BIA through any of the methods described can be an opportunity to collect additional information which can be useful for developing or reviewing strategies and solutions, for instance:

- a) at the top management level:
 - 1) the planned strategic direction of the organization, such as mergers, relocation or acquisitions which can affect business continuity strategy in the future and should be taken into account when selecting current strategies;
 - 2) exploration of business continuity strategy opportunities such as cooperation with other organizations (including competitors) to provide mutual aid;
- b) at the business process level:
 - 1) opportunities to buy-in a service to deliver elements or all of the process temporarily, or outsource elements or all of a business process permanently after a disruption;
- c) at the activity level:
 - 1) the documentation of workarounds for the absence of resources and their limitations of quality, extra resource needs, and for how long they are effective;
 - 2) feasibility of sourcing alternate supplies;
 - 3) characteristics of staff, including:
 - i) skills of individual members of staff (in current and past roles);
 - ii) contact details;
 - iii) their primary work location, home location and mode of transport to work;
 - iv) ability to work from home (including network capacity, equipment and desk location);
 - v) ability to work at an alternative location (including the need for transport);
 - vi) records and their location.

NOTE For more detail on strategies and solutions, see ISO/TS 22331.

C.2 Increasing the efficiency of the organization

The overview of the operation of an organization that emerges from the BIA process can enable participants in the process to identify changes that can improve its efficiency. These changes are not always apparent until the organization explores its web of interdependencies.

A better understanding of the time imperatives of product and service delivery can improve scheduling and prioritization when resources are temporarily limited.

Knowing the time imperatives of various parts of a manufacturing process can improve the optimization of stocks of raw materials or spare parts.

Understanding the interdependencies of activities can suggest changes in the organization's structure.

C.3 Exploring alternative strategic planning options

The organization can apply the BIA process to one or more future situations in order to understand the business continuity implications of planned changes.

This application of the BIA process can be useful if the organization is planning significant changes such as:

- rearrangement of workspace: a new site, site closure or consolidation;
- change in resource: staff increase or decrease;
- change in technology: automation, ICT hardware, etc.;
- product or service change: new contracts or change in business terms.

The application of a future-looking BIA process can explore various options to understand the business impact of each change as there can be significant differences within which disruption to products, services, business processes or activities remains acceptable. These conclusions can be used as an input into the decision-making process. For example:

- a call centre service delivered from two sites can provide an acceptable, if not degraded, service compared to downtime potential if a single site was used and became non-operational;
- the impact of a loss following the proposed change is unacceptable, so the organization abandons the proposed change;
- space freed by relocation can be considered as potential recovery space rather than disposed of;
- a change in staff numbers can affect the time taken to recover an activity;
- new ICTs can have different recovery time frames, and some can be feasible within the time available so this should be ascertained as part of the selection process;
- it should be verified that service levels and contractual obligations for recovery are achievable prior to agreement.

C.4 Assisting with longer-term strategy decision-making

The method of evaluating impacts over time can be applied at a strategic level to a number of strategic decisions other than recovery requirements.

Many long-term shifts in an organization's operations are driven by external factors such as:

- pending regulatory change;
- changes in the business environment;
- degradation of the environment;
- shifts in public opinion;
- market change.

The organization does not need to respond immediately to these changes, but top management can assess the growing impacts over time to reach a decision as to when, roughly, the reputational, financial or other impacts of not responding to the changing circumstances become unacceptable. This can then be a consideration in strategic planning.

C.5 Identifying risks

Although business continuity risk assessment and BIA are different processes, it is common to identify business continuity risks while conducting the BIA, especially when carried out through interviews. In addition, the identification of resources necessary to perform the prioritized activities also provides the organization with an important input for risk assessment, e.g. the risk of unavailability of any of those resources. Also, during a BIA interview or during the resource requirements analysis, the impact of single points of failure or unacceptable levels of risks can be revealed.

The identified risks should be analysed outside the BIA process and within the scope of the business continuity risk assessment.

Annex D (informative)

Examples for performing a BIA

D.1 Example 1 — Estimate product and service MTPD, then use it to estimate activity MTPD and set RTO

D.1.1 General

This example presents forms that can be used to record top management's decisions on the priorities for the delivery of products and services (see [Table D.1](#)). These are then used to prioritize the organization's activities and resources (see [Tables D.3](#) to [D.7](#)).

The steps are as follows:

- define the MTPD threshold for each impact type (see [5.3](#));
- document the products and services and estimate their respective MTPD (see [5.4](#));
- for each product and service, document the activities, identify their MTPD and set their RTO (see [5.5](#));
- for each activity, document the resources (see [5.6](#));
- consolidate resource requirements across all activities (see [5.7](#)).

D.1.2 Step 1 — Define MTPD threshold for each impact type

Complete an impact table (see [Table D.1](#)) with the description of impacts and the defined MTPD threshold as agreed by top management.

Table D.1 — MTPD impact table

Impact type	Description	MTPD threshold
Business objectives	Failure to deliver on objectives or take advantage of opportunities	Drop greater than 15 %
Financial	Financial losses due to fines, penalties, lost profits or diminished market share	Loss greater than USD 1 million
Legal and regulatory	Litigation liability and withdrawal of license to trade	Regulator suspends operating licence
Market share	Loss of clients moving to competitors	New orders drop greater than 25 %
Reputational	Negative opinion or brand damage	Negative attention extensive enough to engage external communications experts

D.1.3 Step 2 — Document products and services and estimate their respective MTPD

The product and service BIA form (see [Table D.2](#)) presents the organization's identified products and services. For each product and service, top management determines the threshold for the agreed impact types (see [Table D.1](#)) and selects the lowest MTPD value across the impact types.

Table D.2 — Product and service BIA form

Product or service	Impact type	MTPD threshold (see Table D.1)	Product or service MTPD
Customer service	Business objectives	48 hours	24 hours
	Financial	5 days	
	Legal and regulatory	Not applicable	
	Market share	Not applicable	
	Reputational	24 hours	
....
Insurance policy booklet	Business objectives	Not applicable	48 hours
	Financial	5 days	
	Legal and regulatory	48 hours	
	Market share	1 month	
	Reputational	1 week	

D.1.4 Step 3 — For each product and service, document the activities, identify their MTPD and set their RTO

The activity BIA form (see [Table D.3](#)) presents the activities required to deliver each product and service. The activity RTO should be set within the activity MTPD. This example assumes that, for this service, all three activities need to be resumed within the service MTPD.

Table D.3 — Activity BIA form

Product or service	Product or service MTPD	Activity	Activity MTPD	Activity RTO
Customer service	24 hours (from Table D.2)	Front line call handling	4 hours	1 hour
		Second line problem solving	8 hours	2 hours
		Document dispatching	24 hours	8 hours

D.1.5 Step 4 — For each activity, document the resources

The resource BIA form (see [Table D.4](#)) presents the resources required by each activity. There will be one table for each activity (which can be involved in delivering more than one product and service). The contents of this form will vary according to the nature of the organization's resource requirements.

Table D.4 — Resource BIA form

Activity	Front line call handling (from Table D.3 “Activity” column)
Activity RTO	1 hour (from Table D.3 “Activity RTO” column)
Product(s) and service(s) delivered	Customer service (from Table D.3 “Product or service MTPD” column)
Interdependencies	New pricing from consumer products department
Resources	Staff (see Table D.5) Equipment (not shown in this example) Applications (see Table D.6) Suppliers (see Table D.7)

[Tables D.5](#), [D.6](#) and [D.7](#) are examples of how to document some resource requirements.

D.1.6 Step 5 — Consolidate resource requirements across all activities

When identifying resource requirements, the earliest activity RTO is selected (see [Tables D.5](#), [D.6](#) and [D.7](#)). The resources can be accumulated across all activities. They can also be tabulated by business unit or location.

Table D.5 — Cumulative staff numbers required over time

Activity	Resource	BAU ^a	1 hour	< 2 hours	< 8 hours	< 1 week	< 1 month	> 1 month
Front line call handling	Supervisors	6	1	1	2	4	4	6
	Operators	100	5	15	40	80	80	100
Second line problem solving	Supervisors	4	0	1	1	2	2	4
	Software engineers	30	0	5	12	20	20	30
Document dispatching	Operators	5	0	1	1	1	3	5
Total		145	6	22	56	107	109	145
^a BAU: business as usual.								

Table D.6 — List of applications required with their RTO and RPOs

Application	Used by activity	RTO from activity	Application RTO	RPO from activity	Application RPO
Call register system	Front line call handling	1 hour	1 hour	2 hours	2 hours
	Second line problem solving	2 hours		12 hours	
Call handler system	Front line call handling	1 hour	1 hour	24 hours	24 hours
Document management repository	Document dispatching	24 hours	24 hours	24 hours	24 hours
...

Table D.7 — List of suppliers and their resource RTO

Supplier	Resource	Used by activity (from Table D.3)	Activity RTO (from Table D.3)	Resource RTO
Supplier A	External call operators	Front line call handling	1 hour	24 hours
	Software engineer	Second line problem solving	2 hours	5 days
Supplier B	Courier	Document dispatching	24 hours	48 hours
...

D.2 Example 2 — Identify MTPD and set RTO

D.2.1 General

The following example shows how criteria can be defined in advance and applied across the organization to ensure consistency when:

- top management estimates the MTPD for products and services;
- activity owners identify the MTPD and set the RTO for activities.

The steps are as follows:

- a) document and approve an impact matrix (see [5.3.2](#));
- b) define and approve time frames for assessing impacts (see [5.3.3](#));
- c) determine and approve criteria for product and service as well as activity MTPD (see [5.3.4](#)) and activity RTO;
- d) estimate and approve the MTPD for each group of products and services (see [5.4](#));
- e) identify the MTPD and set the RTO for each activity (see [5.5](#)).

D.2.2 Step 1 — Document and approve impact matrix

An impact matrix (see [Table D.8](#)) needs to be completed with the description of impacts and the criteria for each as agreed by top management.

Table D.8 — Impact level matrix approved by top management

Impact types	Levels of impact					
	0	1	2	3	4	5
Financial	None	Loss of < USD 10 000 in revenue or expense	Loss of ≥ USD 10 000 and < USD 50 000 in revenue or expense	Loss of ≥ USD 50 000 and < USD 250 000 in revenue or expense	Loss of ≥ USD 250 000 and < USD 1 000 000 in revenue or expense	Loss of ≥ USD 1 000 000 in revenue or expense
Regulatory	None	Little interest from regulator	Regulator requests updates	Regulator issues warning	Suspension of licence	Business failure due to loss of licence
Reputational	None	Some negative attention in media Response not required	Negative attention in media Requires response	Temporary negative regional attention reported via news channels Requires a dedicated response team	Negative national attention extensive enough to engage external communica- tions experts Requires top management to be included in response	Consistent negative media attention Business failure due to perceived incompetence or loss of faith in the organization

D.2.3 Step 2 — Define and approve time frames for assessing impacts

The time frames given in [Table D.9](#) have been defined for the purpose of this example.

Table D.9 — Worksheet with agreed time frames

Impact over time					
1 hour	8 hours	24 hours	72 hours	1 week	> 1 month

D.2.4 Step 3 — Determine and approve criteria for product and service as well as activity MTPD and activity RTO

Based on the information in [Table D.9](#), top management has agreed the following:

- the MTPD is when the impact level reaches 4;
- the RTO is set at a time when the impact level is not greater than 3.

D.2.5 Step 4 — Estimate and approve MTPD for each product and service

The BIA leader meets with top management and asks the following for each product and service:

- the interested parties who would be affected by the disruption and main concerns related to the delivery of products and services, as this can give an idea of the impacts to be discussed;
- the time of the day/month/year, peak periods or circumstances when the disruption will result in the greatest impact (worst case), as this worst case will be used for the following discussion;
- the impacts of disruption to the delivery of products and services for each of the agreed time frames, challenging the answers as needed;

- the planned changes related to the product and service that can influence these impacts in the short to medium term.

During the meeting, the worksheet (see [Table D.10](#)) is completed as follows:

- document the product or service name;
- document the worst case;
- start with the first impact type and for each “Impact over time” column record the impact level using the impact matrix (see [Table D.8](#));
- repeat for subsequent impact types;
- record the largest value of each column on the “Product or service impact” row;
- record the time frame at which the product and service impact reaches the MTPD at the bottom of the worksheet to define the result.

Table D.10 — Completed product and service worksheet

Product or service name	Online sale of children’s clothes					
Worst case	Peak period Black Friday					
Impact types	Impact over time					
	1 hour	8 hours	24 hours	72 hours	1 week	> 1 month
Reputational impact	0	0	0	1	2	4
Regulatory impact	0	0	0	0	1	2
Financial impact	0	0	0	0	1	2
Product or service impact (maximum of impacts above)	0	0	0	1	2	4
Result						MTPD

D.2.6 Step 5 — Identify MTPD and set RTO for each activity

In a similar way, the BIA leader meets with the activity owner and asks the following for each activity:

- the output for each product or service delivered;
- the interested parties who would be affected by the disruption;
- the time of the day/month/year, peak periods or circumstances when the disruption will result in the greatest impact (worst case), as this worst case will be used for the following discussion;
- the impacts of disruption for each of the agreed time frames, challenging the answers as needed.

During the meeting, the worksheet (see [Table D.11](#)) is completed as follows:

- document the activity name and its description;
- document the worst case;
- start with the first impact type and for each “Impact over time” column record the impact level using the impact matrix (see [Table D.8](#));
- repeat for subsequent impact types;
- record the largest value of each column on the “Activity impact” row;
- record the time frame at which the activity impact reaches the MTPD and the time frame to set the RTO at the bottom of the worksheet to define the result;

- make sure that the activity RTO has been set within the activity MTPD.

Table D.11 — Completed activity worksheet

Activity name	Register orders online					
Worst case	Peak period Black Friday					
Impact types	Impact over time					
	1 hour	8 hours	24 hours	72 hours	1 week	> 1 month
Reputational impact	0	2	3	3	4	5
Regulatory impact	0	0	0	0	0	1
Financial impact	0	2	2	3	3	4
Activity impact (maximum of impacts above)	0	2	3	3	4	5
Result			RTO		MTPD	

D.3 Example 3 — Validate activity RTO with trend analysis

While facilitating the BIA, it is possible that the BIA leader will recognize inconsistencies in the way some activity owners have set their RTOs. The following are reasons why this occurs. It is possible that the activity owner will:

- misinterpret the meaning of the impact type criteria;
- be new to the business unit and does not fully appreciate the impact of disruption;
- confuse the urgency of the activity with its importance;
- be influenced by personal biases, creating an inconsistent view compared with other activity owners across the organization.

The following provides a technique, using trend analysis, to highlight RTO inconsistencies so that the BIA leader can discuss and further explore the activity owner's rationale for setting the RTO. Such a conversation can lead to the activity owner reconsidering the RTO.

Activity owners complete the impact rating table (see [Table D.12](#)) for each of their activities as part of the process for setting the RTO. The result will be an RTO and impact rating for each activity.

[Table D.12](#) presents the impact rating table used to calculate the impact rating for each activity. The key parameters are:

- time frames (see [5.3.3](#)) to consider the impact of a disruption over time;
- impact types (see [Table 3](#)) and their levels of impact (i.e. 0 to 5, where 0 indicates no impact at all) to consider the magnitude of impact at each time frame.

Table D.12 — Impact rating table

Impact types	Time frame 1						Time frame 2						Time frame 3					
	1 day						1 week						1 month					
	Level of impact						Level of impact						Level of impact					
	0	1	2	3	4	5	0	1	2	3	4	5	0	1	2	3	4	5
Financial																		
Market share																		
Legal																		
Regulatory																		
Reputational																		
Business objectives																		

Start with the first impact type (in this example: “Financial”). If the activity is disrupted and delays the delivery of the product or service to the interested parties by the first time frames (i.e. 1 day), select the closest level of financial impact described in the impact matrix (see [Table 3](#)) and mark the corresponding cell (see [Table D.12](#)) under the level of impact. Then consider the financial impact for each of the subsequent time frames and repeat this process for each of the other impact types.

Based on the sample impact rating table (see [Table D.12](#)) presenting six impact types and three time frames, there should be 18 responses which will derive the impact rating in the range 0 to 90.

The following examples (see [Tables D.13](#) and [D.14](#)) present the results of two activities each set with a three day RTO by the activity owner:

- Customer Help Desk (see [Table D.13](#)) with an impact rating of 39;
- Accounts Payable (see [Table D.14](#)) with an impact rating of 14.

In this example, the impact ratings are considerably different, suggesting that the Customer Help Desk will deliver a far greater magnitude of impact compared to Accounts Payable even though their respective activity owners have set the RTO at the same time point.

Table D.13 — Impact rating table for Customer Help desk

Business unit	Sales
Activity	Customer Help Desk
Location	Head Office
Activity output	Resolve product issues

RTO	3 days
Impact rating	39

Impact rating table for Customer Help Desk																		
Impact types	Time frame 1						Time frame 2						Time frame 3					
	1 day						1 week						1 month					
	Level of impact						Level of impact						Level of impact					
	0	1	2	3	4	5	0	1	2	3	4	5	0	1	2	3	4	5
Financial																		
Market share	X																	
Legal	X						X											
Regulatory																		
Reputational																		
Business objectives																		

1 + 2 + 4 = 7
0 + 1 + 3 = 4
0 + 0 + 3 = 3
2 + 3 + 4 = 9
1 + 3 + 5 = 9
1 + 2 + 4 = 7
39

Table D.14 — Impact rating table for Accounts Payable

Business unit	Finance		
Activity	Accounts Payable	RTO 3 days	
Location	Head Office	Impact rating 14 ▼	
Activity output	Funds to suppliers		

Impact rating table for Accounts Payable																		
Impact types	Time frame 1					Time frame 2					Time frame 3							
	1 day					1 week					1 month							
	Level of impact					Level of impact					Level of impact							
	0	1	2	3	4	5	0	1	2	3	4	5	0	1	2	3	4	5
Financial	X						X						X					
Market share	X						X						X					
Legal	X						X								X			
Regulatory	X						X								X			
Reputational	X							X						X				
Business objectives	X						X							X				

0 + 0 + 0 = 0

0 + 0 + 0 = 0

0 + 0 + 3 = 3

0 + 1 + 3 = 4

0 + 2 + 2 = 4

0 + 1 + 2 = 3

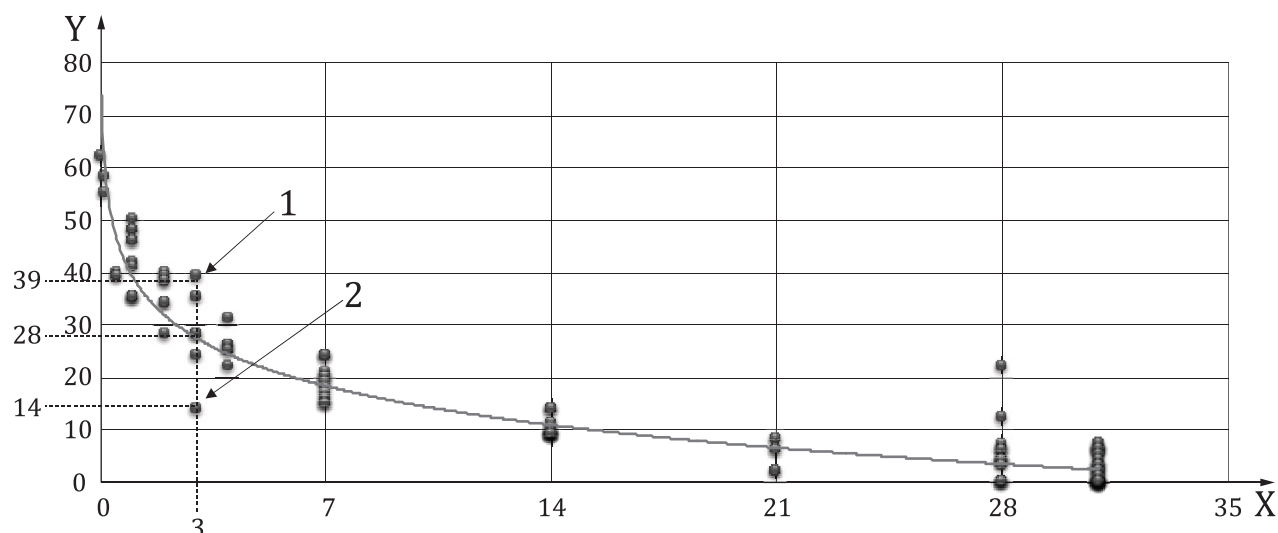
14

To determine whether the Customer Help Desk should have a shorter RTO, or whether Accounts Payable should have a longer RTO will require a holistic review of the relationship between the RTO and the impact rating for all activities within the BCMS scope.

When all activities in the BCMS scope have their RTO set and their impact rating calculated, a worksheet can be created with the following columns of data:

- business unit;
- business activity;
- activity owner;
- the RTO, used as the primary sort in ascending order;
- the impact rating, used as the secondary sort in descending order.

Then, the RTO and impact rating columns are selected and a scatter graph created to see the trend line that best fits the data, as shown by [Figure D.1](#).



Key

- X RTO days
- Y impact rating
- 1 Customer Help Desk
- 2 Accounts Payable

NOTE 1 The dots present the RTO/impact rating position of each activity.

NOTE 2 The line presents the trend of RTO/impact rating dots. The dots do not have to be actually on the trend line. You can allow a confidence margin, e.g. an impact rating of ± 5 to 10.

Figure D.1 — RTO scatter graph and impact rating trend line

Dots representing activities well above the trend line indicate that either the activity owner has set the RTO too late on the timeline or overestimated the magnitude of impact on the impact rating table. For example, consider the Customer Help Desk:

- if there is great confidence that the impact rating appropriately reflects the true magnitude of impact, then the RTO should move left towards the trend line and be reset towards 1 day;
- however, if there is great confidence that the RTO reflects a pragmatic recovery time frame, then the impact rating should be reassessed by redoing the impact rating table (see [Table D.12](#)) to bring the impact rating down toward the trend line, i.e. towards an impact rating of 28.

Conversely, dots representing activities well below the trend line indicate that either the activity owner has set the RTO too early on the timeline or underestimated the magnitude of impact on the impact rating table. For example, consider Accounts Payable:

- if there is great confidence that the impact rating appropriately reflects the true magnitude of impact, then the RTO should move right towards the trend line and be reset towards 11 days;
- however, if there is great confidence that the RTO reflects a pragmatic recovery time frame, then the impact rating should be reassessed by redoing the impact rating table (see [Table D.13](#)) to raise the impact rating up toward the trend line, i.e. towards an impact rating of 28.

It is important to remember this technique should not force the activity owner to change the result. It is designed to highlight that their RTO needs a review because it is not consistent with the thoughts and requirements of other activity owners. The BIA leader should always remember that the choice of RTO is the responsibility of the activity owner.

This methodology can be scaled to suit each organization. For example:

- there can be more or less than six impact types;
- impact types can be weighted, e.g. reputation has twice the impact of legal so the reputation sub-score in the impact rating table can be doubled;
- the scale of impact type metrics can be more or less than six;
- there can be more time frames.

Bibliography

- [1] ISO 22313:2020, *Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301*
- [2] ISO/TS 22331, *Security and resilience — Business continuity management systems — Guidelines for business continuity strategy*

This page deliberately left blank