TECHNICAL SPECIFICATION

ISO/TS 22317

First edition

Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)

Sécurité sociétale — Titre manque

PROOF/ÉPREUVE

Reference number
ISO/TS 22317:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

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 on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 292, *Security and resilience*.

Introduction

This Technical Specification provides detailed guidance for establishing, implementing, and maintaining a business impact analysis (BIA) process consistent with the requirements in ISO 22301. This Technical Specification is applicable to the performance of any BIA process, whether part of a business continuity management system (BCMS) or business continuity programme (BC programme). Hereinafter, BC programme means either BCMS or BC programme.

Figure 1 notes the relationship of the BIA process to the BC programme as a whole. The organization should complete a cycle of the BIA process before business continuity strategies are selected.

Figure 1 — Elements of business continuity management (Source: ISO 22313)

The BIA process analyses the consequences of a disruptive incident on the organization. The outcome is a statement and justification of business continuity requirements.

The BIA process consists of a number of individual BIAs, each focusing of a sub-set of the BC programme scope. The BIA process prioritizes products and services, and continues with prioritizing processes and activities that together cover the entire scope of the BC programme. After a period of time determined by the organization, individual BIAs are repeated to ensure that the BC requirements remain current.

NOTE In this Technical Specification, business continuity requirements has the same meaning as continuity and recovery priorities, objectives, and targets (ISO 22301:2012, 8.2.2).

The purposes of this Technical Specification are the following:

— provide a basis for understanding, developing, implementing, reviewing, maintaining, and continually improving an effective BIA process within an organization;

— provide guidance for planning, conducting, and reporting on a BIA;

— assist the organization with conducting a BIA in a consistent manner that reflects good practices;

— enable proper coordination between the BIA process and the overarching BC programme.

The outcomes of the BIA process include the following:

— endorsement or modification of the organization's BC programme scope;

— identification of legal, regulatory, and contractual requirements (obligations) and their effect on business continuity requirements;

— evaluation of impacts on the organization over time, which serves as the justification for business continuity requirements (time and capability);

— identification and confirmation of product/service delivery requirements following a disruptive incident, which then sets the prioritized timeframes for activities and resources;

— identification and establishment of the relationships between products/services, processes, activities, and resources;

— determination of the resources needed to perform prioritized activities (e.g. facilities; people; equipment; information, communication and technology assets; supplies; and financing);

— understanding of the dependencies on other activities, supply chains, partners, and other interested parties;

— determination of how up to date the information needs to be.

NOTE For purposes of this Technical Specification, supply chains produce supplies of goods, works, and services, which are referred to as 'supplies' throughout the remainder of this document.

The following diagram displays the BIA process, together with prerequisites and its relationship to strategy identification. The clauses referenced in the diagram are subsections of this Technical Specification.

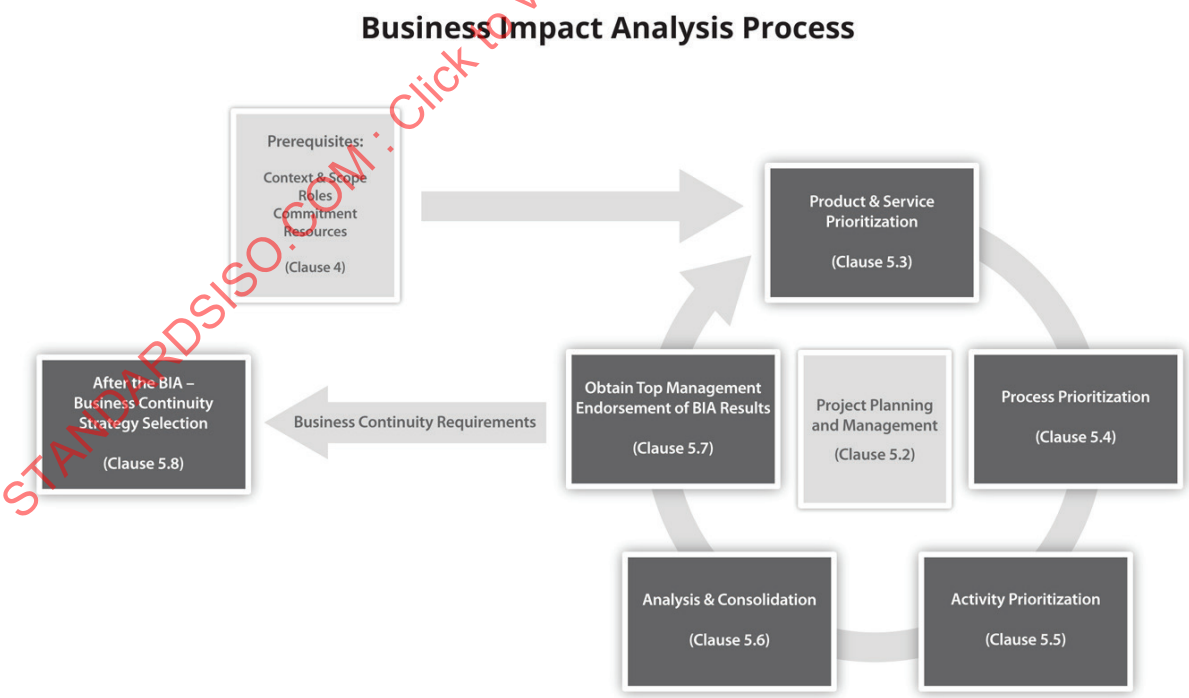

Figure 2 — Business impact analysis process

Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)

1 Scope

This Technical Specification provides guidance for an organization to establish, implement, and maintain a formal and documented business impact analysis (BIA) process. This Technical Specification does not prescribe a uniform process for performing a BIA, but will assist an organization to design a BIA process that is appropriate to its needs.

This Technical Specification 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.

It is intended for use by those responsible for the BIA process.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22300, *Societal security — Terminology*

3 Terms and definitions

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

4 Prerequisites

4.1 General

As noted in the Introduction, this Technical Specification is consistent with ISO 22301, but it could be used to develop, implement, review, maintain, and continually improve a BIA process addressing other standards or regulatory requirements. Whether part of a BCMS or a BC programme, the organization should consider a number of prerequisites before starting the BIA process. Clause 4 summarizes these prerequisites, many of which are from ISO 22301.

The organization should take a number of steps within the BC programme before beginning the BIA process, which include the following:

— define the context and scope (4.2);

— define and communicate roles and responsibilities (4.3);

— obtain leadership commitment (4.4);

— allocate adequate resources (4.5).

NOTE For additional information, see Annex A for a mapping of each step to ISO 22301.

4.2 BC programme context and scope

4.2.1 BC programme context

Successful BIA process outcomes are dependent on the organization understanding the following:

— the external environment in which it operates so that it can achieve its purpose by delivering its products and services to customers;

— the internal operating environment, inclusive of processes, activities, and resources, as well as the potential impact caused by disrupting the delivery of products and services; and

— laws and regulations mandating the BIA process and how it is performed.

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

4.2.2 Scope of the BC programme

Before determining the BIA process scope, the organization should define and document the scope of the BC programme in terms of its products and services.

The BIA process may assist the organization to review the scope of the BC programme.

Following the definition of the BC programme scope, the organization can determine the BIA process scope which may be conducted as a single BIA to cover the whole scope of the BC programme; or undertaken in a number of phases that, over time, covers the whole scope of the BC programme.

NOTE If the organization chooses to undertake the BIA process in phases, it should first determine the prioritization of all products and services (see 5.2) and then continue with the remaining individual BIAs.

4.3 BC programme roles

4.3.1 BC programme roles and responsibilities

Prior to performing the BIA process, top management should ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

4.3.2 BIA process-specific roles and competencies

Following the assignment of BC programme roles, top management should provide resources necessary to perform the BIA process, which may include appointing the following roles:

— the person sponsoring the BIA process;

— BIA steering committee;

— the person leading the BIA process;

— the person managing the BIA project (project manager);

— process owners;

— activity managers.

The person sponsoring the BIA process should

— be an executive representing top management,

— be well respected within the organization by other members of top management,

— have an organization-wide perspective,

— have the authority to commit the organization to action, and

— make final decisions regarding the BIA process.

The BIA steering committee should

— represent top management,

— provide ongoing advice and guidance on the conduct of the BIA process,

— agree on the methods and outcomes,

— make decisions regarding business continuity requirements, and

— assist the person leading the BIA process and project manager in determining the competences required for BIA process-specific roles and responsibilities and the awareness, knowledge, understanding, skills, and experience needed to fulfil them.

The person leading the BIA process should

— have an understanding of the organization, in particular products, services, processes, and activities, and

— have experience in conducting a BIA process.

The person managing the BIA project should

— plan for and manage the BIA process,

— have an understanding of project planning tasks, and

— be familiar with the BIA process.

Process owners should have a relatively detailed understanding of the process they represent in order to assist the project manager in identifying subject matter experts, organizational units, and impacts of downtime.

Activity managers should

— have very detailed understanding of the activity in which they represent, including all of the resources that enable the activity to operate, and

— be aware of alternate processes and resources that could be available in the event of a loss of primary resources.

NOTE In smaller organizations, these roles can be combined.

The organization should ensure the competence of persons leading or participating in the BIA process. Competences should include skills and abilities related to the following:

— project/programme planning and management;

— information gathering;

— analysis;

— effective communication and collaboration;

— translating organizational objectives to business continuity requirements and resource needs;

— applying BIA concepts in the specific organization's context;

— knowledge of the organization, its products and services, processes, activities, and resources.

4.4 BC programme commitment

Top management commitment to the BIA process is necessary to ensure effective participation. To obtain this support, the organization may consider communicating the BIA process' value that includes the following:

— ensuring the appropriate and most cost effective strategies are selected by determining the correct business continuity requirements;

— providing evidence to management that business continuity requirements align with organizational objectives;

— ensuring the organization meets its legal, contractual, and customer requirements during a disruptive incident;

— identifying linkages between products and services and process, activities, and resources;

— providing an overview of the organization that can be used to improve its efficiency or explore new opportunities (see Annex D).

4.5 BC programme resources

The organization should provide resources to the BIA process that are sufficient to the following:

— achieve its BC policy and objectives;

— make adequate provision for people and people-related resources, including the time to fulfil BIA process-specific roles and responsibilities, and training and awareness;

— meet the changing requirements of the organization;

— provide for ongoing operation and continual improvement of the BC programme, as well as the BIA process.

5 Performing the business impact analysis

5.1 General

The BIA process prioritizes the various organizational components so that product and service delivery can be resumed in a predetermined timeframe following a disruptive incident to the satisfaction of interested parties. For purposes of this Technical Specification and consistent with ISO 22301, products and services are created by processes that are made up of activities.

The products and services are prioritized first; this sets the time and service level parameters for process prioritization. If required by the complexity of the organization, the processes can then be separated into their constituent activities for prioritization.

Suitable, adequate, and effective outcomes of subsequent phases of the BC programme depend on the accuracy of the BIA process. Each BIA should be completed consistently, carefully, and thoroughly.

Figure 3 shows how the various elements of the BIA process relate to each other. The diagram illustrates that there can be overlap between the timing of these constituent phases of the process.

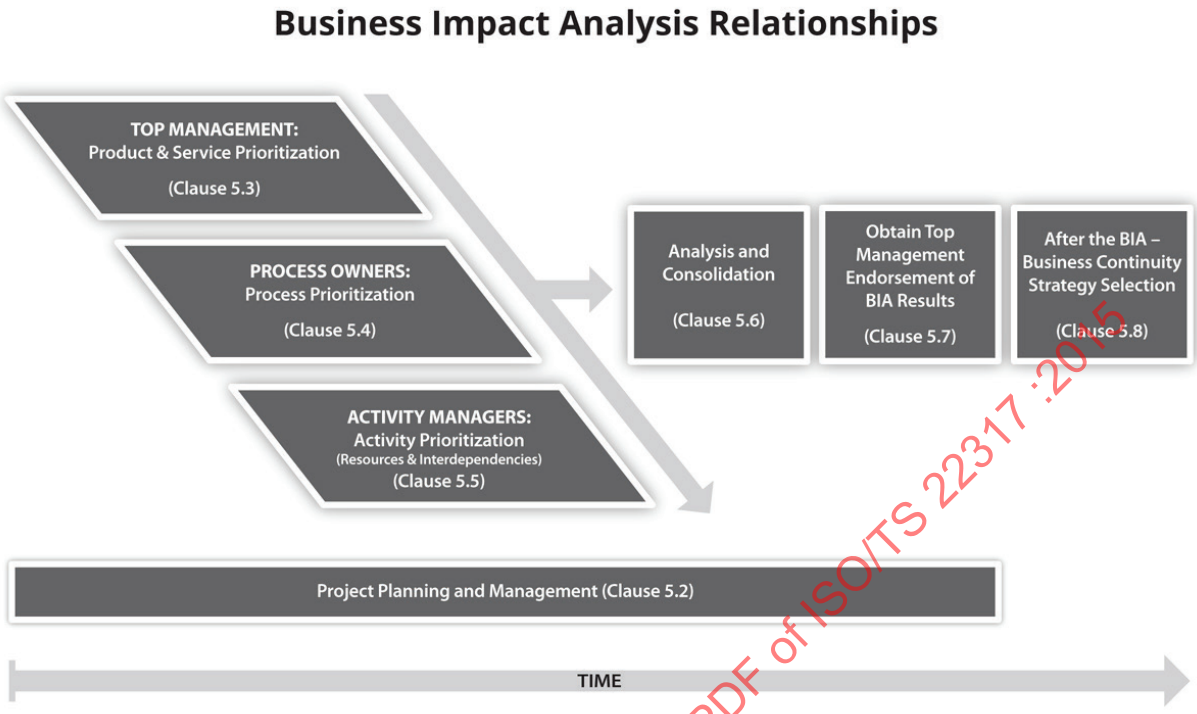

Figure 3 — Business impact analysis relationships

Successful BIA process outcomes may depend on the following:

— identifying customers and other interested parties, and anticipating their reactions to a disruptive incident;

— engaging all relevant interested parties with an appropriate mandate;

— developing appropriate skills and competencies within the organization or project to conduct the analysis and present the results;

— gathering generally complete and accurate information (some information may be unavailable, poorly understood, confidential or withheld, thus identifying areas for further work);

— ensuring that those contributing to the BIA information gathering process have sufficient knowledge and authority to speak on behalf of the organization, process, or activity;

— ensuring management representatives have sufficient authority to approve BIA results.

5.2 Project planning and management

5.2.1 General

Although BIA is a process, organizations may use project management methods for a phase of the BIA process. As the BIA process is potentially complex, using project management methods allows organizations to coordinate resources and timelines.

Project planning tasks may include the following:

— deciding on the scope of this phase of the BIA process;

— communicating expectations to BIA process participants;

— identifying the person sponsoring the BIA process and top management participation;

— establishing BIA process-specific roles and responsibilities (including competencies);

— establishing the project plan;

— allocating resources for the BIA project;

— gaining acceptance of the project approach and plan;

— establishing or sourcing the skills necessary to meet BIA process objectives.

Project management tasks may include the following:

— implementing the BIA process (see 5.2 through 5.6);

— monitoring the implementation of the BIA process (see through 5.6);

— developing periodic reports on the status, noting performance expectations and recommendations to improve performance in line with top management expectations (see 5.2);

— performing modifications of the BIA process approach and scope to meet top management expectations and external (regulatory, statutory, customer, contractual) requirements (see Clause 6);

— collecting and reviewing lessons learned (see Clause 6);

— making recommendations regarding BIA process improvement for future implementation (see Clause 6).

5.2.2 Initial BIA considerations

An organization undertaking a BIA for the first time should plan additional time to

— identify products and services,

— create awareness and ensure education,

— identify a top management representative to sponsor the BIA process and/or BIA steering committee,

— determine impact categories and criteria,

— determine importance of the organization's business/political environment,

— identify the organization's structure to an appropriate level of detail,

— identify and select the right information sources for information gathering,

— document the work flow to a process and activity level, and

— complete information gathering through document review, interviews, workshops, and questionnaires.

During the initial BIA, the organization may use the BIA results to prioritize subsequent business continuity phases, including strategy selection.

5.3 Product and service prioritization

5.3.1 Overview

As the first step in the BIA process, top management should agree on the priority of products and services following a disruptive incident which may threaten the achievement of their objectives.

It is top management's responsibility to make these decisions because they

— set the objectives of the organization,

— have the ultimate responsibility for ensuring the continuity of the organization and the fulfilment of its objectives,

— have the widest view of the entire organization from which to assess priorities,

— can choose to override contractual and other obligations in setting priorities in exceptional circumstances, and

— are aware of planned future changes and other factors which may affect the business continuity requirements.

If an organization has too many products and services to identify individually, the organization may group together products and services when they have similar priorities. Conversely, it may be necessary for the organization to identify customers that, despite sharing the same products and services, have differing delivery timeframe expectations, or their value to the organization differs.

For each group of products and services, the organization should understand the impacts that may result from a disruptive incident by

— identifying customer expectations and obligations, and the penalties associated with failing to meet them and

— taking into account the views of other interested parties in assessing impacts.

Other interested parties and their reaction to a disruptive incident may include the following:

— partner organizations: their willingness to continue to cooperate;

— media and society: brand value and public opinion;

— potential customers: loss of current and future market share;

— shareholders: effect on current share price and future investment;

— competitors: who may attempt to take advantage of the situation;

— staff: retention;

— regulators and government: penalties and rule changes.

The organization may use the examples in Table 1 to understand the impacts of a disruptive incident on the organization over time:

Table 1 — Product and service level impact category examples

Impact categories	Examples of impacts
Financial	Financial losses due to fines, penalties, lost profits, or diminished market share
Reputational	Negative opinion or brand damage
Legal and regulatory	Litigation liability and withdrawal of license to trade
Contractual	Breach of contracts or obligations between organizations
Business objectives	Failure to deliver on objectives or take advantage of opportunities

Impacts almost always increase over time. However, impacts may not increase at the same rate. For instance, financial impacts can suddenly increase as contract penalties are incurred or as customers are lost, and reputational damage can occur suddenly at a point during the disruptive incident. See Figure 4 for an example of how different impact categories increase over time.

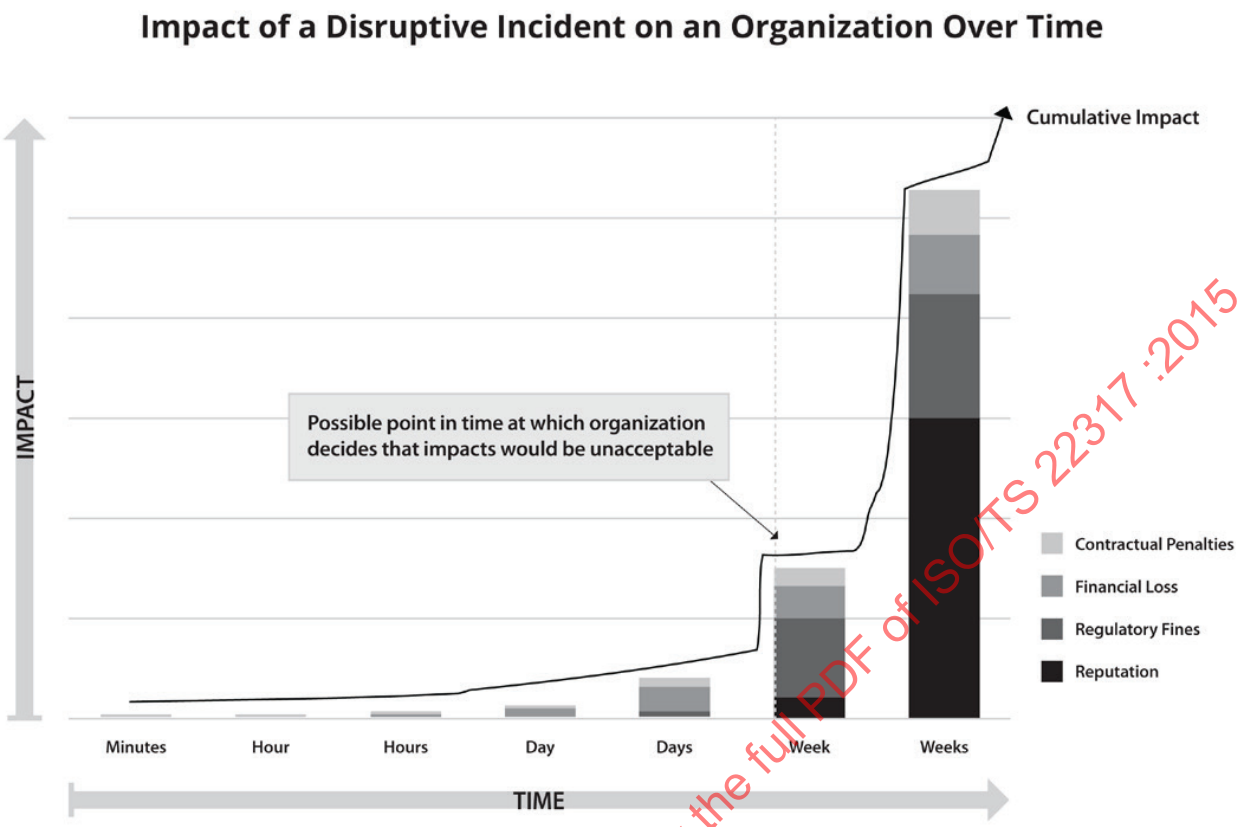

Figure 4 — Impact of a disruptive incident on an organization over time

For each group of products and services, the top management should decide and document the following:

— time after which continued failure to deliver them becomes unacceptable to the organization because the impacts noted above threaten its survival or make its objectives no longer achievable (see Annex B for related terms);

— reason(s) why this time period has been identified with reference to the growing impacts over time.

The organization may, based on the example timeframe in Figure 4, set a target time for resuming delivery of products and services at specified minimum levels (see Annex B for related terms).

5.3.2 Inputs

Top management may consider the following information in setting business continuity requirements for products and services:

— current organizational mission, objectives, and strategic direction;

— current BC programme scope;

— assessment of product and service priorities from a previous top management review;

— list of legal and regulatory requirements to which the organization or specific products and services are subject (as well as an assessment of the consequences of breaching each requirement);

— contractual requirements, including penalties for failure to deliver;

— assessment of reputational, financial, or other impacts for failure to deliver;

— recent post-incident reports which describe the impact associated with the disruptive incident.

5.3.3 Outcomes

The outcomes of the product and service prioritization process should be

— endorsement or modification of the organization's BC programme scope,

— identification of legal, regulatory and contractual requirements (obligations),

— evaluation of impacts over time as it relates to a failure to deliver products or services, which serves as the justification for business continuity requirements,

— confirmation of product and service delivery requirements (that may include time, quality, quantity, service levels, and capability specifications) following a disruptive incident that then sets the priorities for activities and resources,

— identification of processes (that deliver the products and services),

— nomination of lead personnel to assist in identifying which processes deliver products and services, and

— documentation of a list of prioritized products and services (grouped by timeframe or customer).

The organization may retain documentation describing the decisions made during the product and service prioritization process.

5.4 Process prioritization

5.4.1 General

A process is a set of interrelated or interacting activities which transform inputs into outputs (ISO 22300). Its priority is determined by the priority of the products and services which are its output.

Depending on its complexity, the organization may choose to omit process prioritization and proceed directly to activity prioritization. If the organization chooses to perform a process prioritization, the organization should determine activities that make up those processes.

5.4.2 Inputs

The information required for process prioritization includes the following:

— the scope of this BIA;

— product and service delivery requirements (which may include time, quality, quantity, service levels, and capability specifications);

— processes and the products and services they deliver;

— impacts over time of a failure to deliver products and services;

— legal, regulatory, and contractual requirements (obligations).

5.4.3 Outcomes

The outcomes of process prioritization should be the following:

— identification of the relationship between product and services, processes, and activities;

— identification of dependencies on other business processes;

— evaluation of impacts over time of a process failure (the impact categories in Table 1 could be used to confirm the impacts of process disruption);

— priorities of processes;

— interdependency analysis of the processes that deliver products and services to customers;

— interdependency analysis of the activities that deliver processes;

— documented list of prioritized processes that deliver products and services; and

— initial documented list of activities that deliver processes.

5.5 Activity prioritization

5.5.1 Overview

An activity is a set of one or more tasks with a defined output. The priority of the activity is determined by the priority of the processes of which it forms a part.

The organization should perform activity level prioritization to understand the resources needed to operate each activity following a disruptive incident, and to confirm the potential impact associated with a disruptive incident.

Organizations should perform activity level prioritization to obtain a detailed understanding of day-to-day resource requirements, enabling the organization to identify the quantity and timing of resources necessary for recovery and to help confirm impact-related conclusions developed at the process level. Resource-related information includes the following:

— people/skills/roles;

— facilities;

— equipment;

— records;

— financing;

— information and communications technologies (including applications, data, telephony, and networks);

— supplies, supply chains, and partners;

— dependencies on other processes and activities;

— special tools, spare parts, and consumables;

— limitations imposed on resources by logistics or regulations.

In addition to the impacts already considered in Table 1, the organization may consider evaluating operational impact, such as delays due to backlog of workload or manual workarounds or impacts to interrelated activities.

5.5.2 Inputs

The inputs required to undertake activity prioritization include the following:

— scope of this BIA;

— process priorities;

— organizational chart;

— constituent activities of processes.

5.5.3 Information collection

The organization needs to collect the following information to perform the activity level BIA, including activity detail, resource requirements, and interdependencies.

5.5.3.1 Activity detail

The organization may collect the following details during activity prioritization:

— the processes that this activity supports;

— the operational methods of the activity;

— the duration or lead-time of this activity;

— fluctuations in demand or peak operating periods;

— factors not already discovered that may affect the determination of business continuity requirements (e.g. backlogs or legal and regulatory requirements of this activity).

5.5.3.2 Resource requirements

The resource information to be collected during an activity prioritization may include the following:

— staff and contractors (including minimum acceptable level for required service, and knowledge, skills or qualifications required);

— workplace requirements;

— IT applications and communications (noting special requirements);

— records (e.g. electronic or hard copy);

— equipment (e.g. information and communications technology (ICT), office equipment, manufacturing equipment);

— components and raw materials.

5.5.3.3 Interdependencies

The interdependency information required to be collected during an activity prioritization includes the following:

— reliance on other internal activities and resources, or supply chains;

— reliance on other internal activities on the outputs of this activity.

For the specification of ICT requirements, the following additional information may be collected:

— ICT asset name, location, and configuration (e.g. memory, capacity, processor speed, and disk drive space);

— dependencies on other ICT assets;

— end user profiles and usage characteristics;

— unique legal or regulatory requirements regarding the use of the ICT asset.

5.5.4 Outcomes

The outcomes of activity prioritization should be the following:

— confirmation of impacts over time, which serves as justification for business continuity requirements (time and capability);

— resource needs to perform each prioritized activity (including facilities, people, equipment, ICT assets, supplies, finance and information);

— how up to date the information needs to be (see Annex B for related terms);

— dependencies on other activities, supply chains, partners, and other interested parties;

— analysis of dependencies on the resources needed to deliver each activity;

— documented list of activities and their prioritized timeframes that support processes;

— documented list of resources and their prioritized timeframes that enable activities.

5.6 Analysis and consolidation

5.6.1 Overview

While analysis occurs during the entire BIA process, the organization should perform a final analysis (or consolidation of analyses). This involves reviewing the outcomes from the prioritization, and drawing conclusions that lead to business continuity requirements.

The organization should choose the appropriate quantitative and/or qualitative analytic approach(es), which may 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

— correct: accurate and reliable,

— credible: believable and reasonable,

— consistent: clear and repeatable,

— current: up-to-date and available in a timely manner, and

— complete: comprehensive.

5.6.2 Inputs

The organization should obtain validated and approved information gathered from all levels of the BIA process in order to perform analyses.

5.6.3 Methods

The organization may use a combination of quantitative and qualitative techniques to analyze the information collected. Table 2 contains examples of analytic techniques.

Table 2 — BIA analysis techniques

Quantitative analytic techniques	Qualitative analytic techniques
Interdependency analysis Financial analysis approaches	Common sense and cross checks Stress testing Review of post-incident reviews and recommendations Supplier-Input-Process-Output-Customer (SIPOC) Fishbone (Ishikawa) diagrams

5.6.4 Outcomes

The outcomes of applying analysis techniques and consolidating information are the following:

— confirmation of impacts over time;

— review and confirmation of resource dependencies and requirements;

— consolidation of resource requirements (e.g. across processes, organizational structures, or locations);

— review and confirmation of the interdependencies of processes and activities, and their relation to the delivery of products and services, that serve as the input to business continuity strategy selection.

5.7 Obtain top management endorsement of BIA results

5.7.1 General

The organization should seek management endorsement of results, including product and service, process, activity, and resource prioritization following one or more individual BIAs.

The organization should compile BIA results to ensure the information collected can be maintained and updated on a periodic basis before seeking management endorsement. The presentation of BIA results can be in a variety of media and may contain different levels of detail depending on the audience.

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

— product and service prioritization (if changed from original determination);

— process prioritization; and

— pctivity prioritization (including resources and interdependencies).

NOTE The organization can choose to receive this endorsement during a management review (see Annex A).

5.7.2 Inputs

The person responsible for the BIA process should use outputs from 5.2 to 5.6 as inputs into top management endorsement.

5.7.3 Methods

The organization should include at least the following topics in the BIA summary report:

— an overview of the BIA process, including objectives and scope;

— impacts influencing the assignment of business continuity requirements (see 5.3.1);

— recommended prioritized timeframes for products and services, processes, activities, and resources;

— conclusions and next steps.

The organization may develop materials to be presented to top management following the completion of the BIA summary report, by performing the following methods:

— summarizing information to top management by facilitating one-on-one meetings with top management members or facilitating a group meeting with top management;

— extracting and providing the executive summary, which highlights key findings and conclusions; and

— facilitating one-on-one meetings with top management to review the summary report in detail.

5.7.4 Outcomes

The endorsement of the BIA results by top management should be documented according to established document management practices. The BIA results can then be passed to the business continuity strategy selection process.

5.8 After the BIA — Business continuity strategy selection

Following the completion of the BIA, the organization should continue to business continuity strategy selection. Approved business continuity requirements enable the organization to determine and select appropriate business continuity strategies to enable an effective response and recovery from a disruptive incident. Examples include the following:

— alternate workplace arrangements;

— alternate supply chain arrangements;

— ICT recovery options;

— alternate sources of people;

— alternate sources of equipment;

— workarounds and alternate procedures.

The BIA may also lead to a reconsideration of how the organization delivers its products and services (see Annex D).

6 BIA process monitoring and review

Organization should review/perform the BIA process on a periodic basis (typically annually) or as part of organizational change that may affect the accuracy of business continuity requirements.

Top management may publish an annual strategic plan or review that confirms or revises the organization's strategic objectives. A change in the strategic objectives of the organization may be

— reflected in the business continuity policy by a change in the scope of the BC programme, by adding or removing certain products and services or

— a change in the priorities of products and services which may initiate a review of each BIA at the process and activity levels.

A review of different components of the BIA process may be triggered by the following considerations:

— annual review;

— strategic directional change;

— product or service change;

— regulatory change;

— customer and/or contractual change;

— operational change, including new/change application/ICT, supply chain (insourcing/outsourcing), and site/facility resources;

— structural change;

— following a business continuity exercise;

— following a disruptive incident.

In areas of the organization which have changed little since the last BIA, it may be appropriate to check and confirm the previous results rather than conduct a full review.

Annex A
(informative)

Business impact analysis within an ISO 22301 business continuity management system

Table A.1 — Business impact analysis within an ISO 22301 business continuity management system

ISO/TS 22317	ISO 22301
Introduction	0.3 Components of PDCA in this International Standard
4.2 BC programme context and scope	4 Context of the organization
4.3 BC programme roles	5.4 Organizational roles, responsibilities and authorities 7.2 Competence
4.4 BC programme commitment	5 Commitment
4.5 BC programme resources	7.1 Resources
5 Performing the business impact analysis	8.2 Business impact analysis and risk assessment
5.8 Next step — Business continuity strategy selection	8.3 Business continuity strategy

Annex B
(informative)

Business impact analysis terminology mapping

B.1 Business impact analysis terminology mapping

Some of these ISO 22301 terms are not used in this Technical Specification. However, these terms are common with respect to the performance of the BIA process.

Table B.1 — Business impact analysis terminology mapping

Number	Term	Definition	ISO/TS 22317 references
1	Maximum Acceptable Outage (MAO) or Maximum Tolerable Period of Disruption (MTPoD or MTPD)	Time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable.	5.3.1
2	Minimum Business Continuity Objective (MBCO)	Minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption. Note: This should not be confused with BC objectives in ISO 22301:2012, 6.2 which refer to BC programme objectives	5.3.1
3	Recovery Time Objective (RTO)	Target time following an incident for: Product or service delivery resumption, or Activity resumption, or Resources recovery NOTE For products, services and activities, the recovery time objective must be less than the time it would take for the adverse impacts that would arise as a result of not providing a product/service or performing an activity to become unacceptable.	5.3.1
4	Recovery Point Objective (RPO) or Maximum Data Loss (MDL)	Point to which information used by an activity must be restored to enable the activity to operate on resumption.	5.5.4

Annex C
(informative)

Business impact analysis information collecting methods

C.1 Business impact analysis information collecting methods

This Annex summarizes common methods to collect information necessary to reach BIA conclusions. 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 organization should consider the following factors which may influence the selection of the method or methods:

— the information needed: Is the information required to perform the analysis quantifiable/discrete or subjective?;

— previous experience with performing a BIA: Is this the first BIA performed?;

— the need to create business continuity awareness with BC programme participants: Is business continuity an understood concept and are its outcomes known among interested parties?;

— the complexity of the business: How complex are the activities within the scope of the BIA process?;

— BIA process participant competency: What skills and experiences do business continuity practitioners have with implementing the BIA process?;

— BIA process participant availability and geographic location: What are the physical locations and time constraints for those representing activities?

In general, the five most common methods of BIA information gathering are

— documentation review,

— interview,

— survey/questionnaire,

— workshop, and

— scenario-based exercise (caution is advised as different scenarios may result in different magnitudes of impact).

The methods to ensure information consistency, regardless of information collection method, are the following:

— provide training for those who are leading or participating;

— identify information requirements;

— provide oversight or quality assurance of outputs;

— perform a trial of information collection method before implementing on a whole scale.

C.2 Documentation review

The organization should review the following documentation as an essential step in preparing for interviews, developing survey questions, and eventually performing analysis-related work:

— strategy documents;

— marketing materials;

— annual reports;

— business performance metrics;

— standard operating procedures describing day-to-day task execution;

— equipment and information and communications technology (ICT) lists;

— insurance policies;

— post-incident reports;

— training materials;

— prior BIA information;

— process documentation;

— organizational charts;

— roles and responsibilities;

— customer-related service level agreements;

— contractual requirements.

C.3 Interview

Organizations may perform interviews to enable discussion regarding day-to-day operations, resource needs, obligations, and possible impacts if a disruptive incident were to affect the activity's capability to deliver processes, and products or services.

Although many ways to structure an interview exist, topics should include the following:

— BIA process overview, objectives, desired outcomes, and the relationship of the BIA process to the remaining business continuity planning process;

— BIA participant expectations;

— the relationship of activities to processes;

— activity discussion;

— next steps, including a review of the interview summary, comments and corrections, and approval.

The activity discussion may cover the following topics:

— activity overview and relationship to products and services and processes, with emphasis on key tasks and the timeframes 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 5.5.1), including existing workarounds and how long they remain viable;

— known impact associated with process downtime (see 5.3.1);

— known activity-specific obligations.

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.

C.4 Survey/Questionnaire

Organizations may use surveys or questionnaires to effectively collect discrete information, meaning information with a finite number of possibilities or information that can be quantified. Organizations can choose to deliver surveys as

— hard-copy documents,

— electronic documents, or

— online survey service.

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

Common survey content may include the following:

— validation of the impacts associated with a disruptive incident, including how the impact changes over time;

— identification of additional legal, regulatory, or contractual obligations specific to the activity;

— identification of resource dependencies and requirements, as well as recovery timeline following a disruptive incident.

C.5 Workshops

Workshops with participants representing different activities or processes may be used to collect similar information to interviews but in addition may develop and share outcomes with the group in order to

— produce additional, more complete information and

— resolve competing, possibly unrealistic expectations.

C.6 Scenario-based exercise

Using a scenario-based exercise enables participants to decide on the priority of products and services, processes, and/or activities within the context of a simulated disruptive incident. At a top management level, the exercise should be sufficiently challenging that the tolerance of customers is stretched to breaking point so that impacts can be identified and evaluated and difficult decisions about priorities can be made. At a process and activity level, an exercise can explore the logistics, timing and dependencies on other activities and supply chains.

For a top management exercise, scenarios should be kept simple so that participants concentrate on priorities prompted by information injects relating to external pressures such as complaints from customers and media pressure. Time should be allowed for priorities to be debated rather than following a strict incident timeline.

