PRIVATE CIRCULATION
SSM/1_14_0077
For vote - Action Due Date: 2015/02/09

DRAFT TECHNICAL SPECIFICATION OR TECHNICAL REPORT

Proposed ISO/DTS 22317	
Date 2014-12-19	Reference number **ISO/TC 292 N 5**
Supersedes document	

WARNING: This document is not approved. It is distributed for review and comment. It is subject to change without notice.

ISO/TC 292

Title

Security

Secretariat

SIS

Circulated to P- and O-members, and to technical committees and organizations in liaison for:

☐ discussion at
[venue/date of meeting]

☒ comments by 2015-02-20
[date]

☒ approval for publication as a Technical Specification or Technical Report (as indicated below) by

2015-02-20
[date]

(P-members vote only: ballot form attached)

P-members of the technical committee or subcommittee concerned have an obligation to vote.

Title (English)

Societal security – Business continuity management systems – Business impact analysis

Title (French)

Proposed Technical Specification ☒ or *Technical Report* ☐

Reference language version: ☒ English ☐ French ☐ Russian

Introductory note

ISO/DTS 22317

ISO/TC 292 N 5

Date: 2014-12-19

ISO/TC 292

Secretariat: SIS

Societal security – Business continuity management systems – Business impact analysis

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75% of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of normative document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

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.

ISO/TS 22317 was prepared by Technical Committee ISO/TC 223, Societal security.

Introduction

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

Figure 1 (below) notes the relationship of the BIA process to the BCM programme as a whole. The organization must complete the BIA before business continuity strategies are selected.

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

The business impact analysis is a process for analyzing the consequences of a disruptive incident on the organization. The outcome is to produce a statement and justification of business continuity requirements.

The purpose of this International Technical Specification is to:

- provide a basis for understanding, developing, implementing, reviewing, maintaining, and continually improving an effective business impact analysis process within an organization;
- provide guidance for planning, conducting, and reporting on a business impact analysis;
- assist the organization to conduct a business impact analysis in a consistent manner that reflects good practices; and,
- enable proper coordination between the business impact analysis and the overarching BCM programme.

NOTE In this document, business continuity requirements has the same meaning as business continuity priorities, objectives, and targets (ISO 22301, Clause 8.2.2).

The outcomes of the BIA process include:

- endorsement or modification of the organization's BCM programme scope
- identification of legal, regulatory, and contractual requirements (obligations) and their effect on business continuity requirements
- confirmation of product/service delivery requirements following a disruptive incident, which then sets the priorities for activities and resources
- identification of, and establishment of, the relationships between products/services, processes, activities, and resources
- determination of the resources needed to perform prioritized activities (facilities, people, equipment, information, communication and technology assets, suppliers, and financing)
- understanding of the dependencies on other activities, suppliers, outsource partners, and other interested parties
- evaluation of impacts on the organization over time, which serves as the justification for business continuity requirements (time, capability, and quality)
- determination of the required currency of information

The following diagram displays the BIA lifecycle, together with prerequisites and its relationship to strategy identification. The clauses referenced in the diagram are subsections within this document.

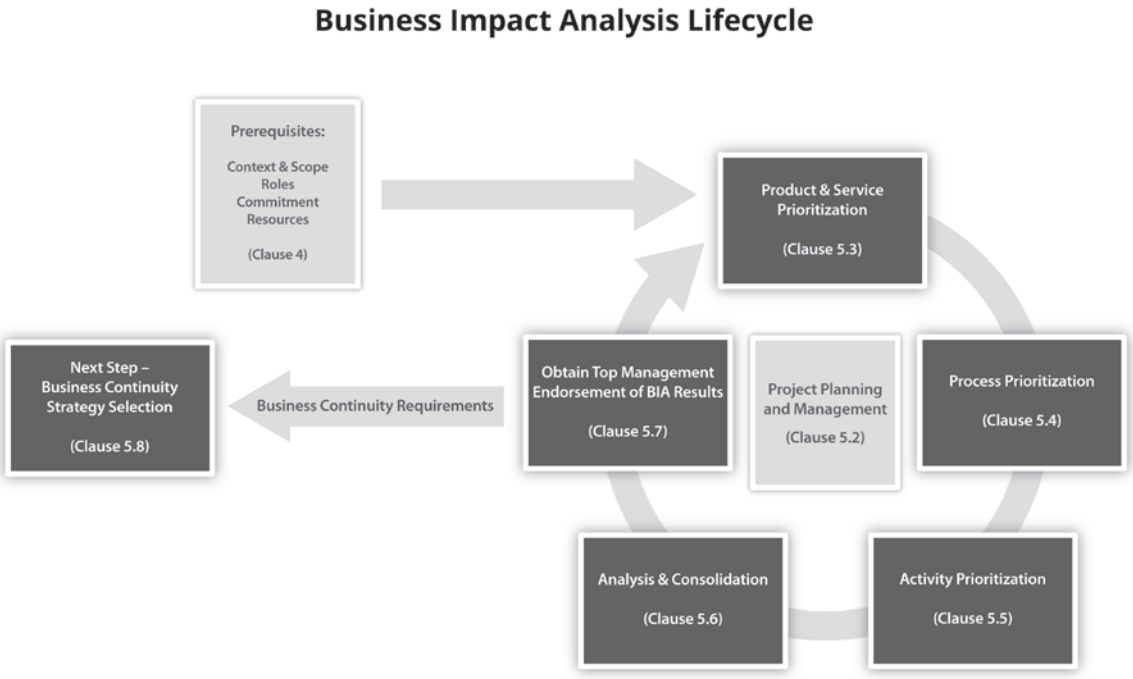

Figure 2 – Business Impact Analysis Lifecycle

Societal security – Business continuity management systems – Business impact analysis

1 Scope

This International Technical Specification recommends good practice and guidelines for an organization to establish, implement, and maintain a formal and documented process for business impact analysis. This International Technical Specification does not prescribe a uniform process for performing a business impact analysis, but will assist an organization to design a BIA process that is appropriate to its needs.

This International Technical Specification is applicable to all organizations regardless of type, size, and nature of the organization, 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 with responsibility for ensuring the competence of the organization's personnel (particularly the organization's top management), as well as those responsible for managing the business impact analysis process.

2 Normative references

The following referenced documents are indispensable for the application 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, *Societal security - Terminology*

3 Terms and definitions

The terms and definitions contained in ISO 22300 apply and are available on the ISO Online Browsing Platform (www.iso.org/obp)

4 Prerequisites

4.1 General

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

— define the context and scope,

— define and communicate roles and responsibilities,

— obtain leadership commitment, and

— allocate adequate resources.

The organization typically documents the outcomes of these steps in a BCM programme policy.

NOTE For additional information, see Annex A for a mapping of each step to ISO 22301:2012.

4.2 BCM Programme Context and Scope

4.2.1 BCM Programme Context

Successful BIA outcomes are dependent on the organization understanding:

- 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 influencing the BIA process.

4.2.2 Scope of the BCM Programme

Before determining the scope of the BIA process, the organization should:

- define and document the scope of the BCM programme, in terms of its products and services; and
- document the justification behind management's decision to exclude parts of the organization from the BCM programme.

Following the definition of the BCM programme scope, the organization can determine the scope of the BIA process which may be:

- conducted as a single BIA to cover the whole scope of the BCM programme; or
- undertaken in a number phases that, over time, covers the whole scope of the BCM programme.

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

The BIA may assist the organization to review the continuing appropriateness of the scope of the BCM programme.

4.3 BCM Programme Roles

4.3.1 BCM Programme Roles and Responsibilities

Prior to performing the BIA process, top management should:

- assign and communicate responsibilities and authorities;
- ensure all roles, responsibilities, and authorities are defined and documented; and
- assume overall responsibility and accountability for the BCM programme.

4.3.2 BIA-Specific Roles and Competencies

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

- Project Sponsor
- Project Steering Committee
- BIA Leader

62 — Project Manager

63 — Process Owners

64 — Activity Managers

65 The Project Sponsor should:

66 — be an executive representing top management

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

68 — have an organization-wide perspective

69 — have the authority to commit the organization to action

70 — make final decisions regarding the BIA process

71 The Steering Committee should

72 — represent top management

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

74 — agree on the methods and outcomes

75 — make decisions regarding BIA results

76 — assist the BIA leader and project manager in determining the competences required for BIA roles and
77 responsibilities and the awareness, knowledge, understanding, skills, and experience needed to fulfil them

78 The BIA Leader should:

79 — conduct the BIA process

80 — have an understanding of the organization, in particular product, services, services, and processes

81 — have experience in conducting a BIA process

82 The Project Manager should:

83 — plan for and manage the BIA process

84 — have an understanding of project planning tasks

85 — be familiar with the BIA process

86 Process Owners should:

87 — have a relatively detailed understanding of the process in which they represent in order to assist the project
88 manager in identifying subject matter experts, organizational units, and impacts of downtime

89 — have the authority to assign prioritization of process-specific resources

90 Activity Managers should:

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

— 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 may 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:

— 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, and technologies

4.4 BCM Programme Commitment

Top management should:

— demonstrate leadership by making timely decisions, allocating resources, and ensuring the motivation and engagement of other staff; and

— foster a culture and environment of awareness, participation and communication across the organization to achieve its business continuity objectives.

Top management commitment to the BIA process is necessary to ensure that the organizational components participate effectively. To obtain top management in demonstrating leadership in support of the BIA process, the organization may consider communicating the BIA process's value that includes the following:

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

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

— collecting the information necessary to establish appropriate business continuity requirements in order to select applicable business continuity strategies and document business continuity plans,

— identifying linkages between products and services and process, activities, and resources that support the execution of other project or change activities throughout the organization,

— prioritizing the recovery of the organization's resources during a disruptive incident, focusing resources on the restoration of key product and service delivery, and

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

4.5 BCM Programme Resources

The organization should provide resources to the BCM programme, and to the BIA process, that are sufficient to:

- achieve its policy and objectives;
- make adequate provision for people and people-related resources, including the time to fulfil BIA roles and responsibilities, and training and awareness;
- meet the changing requirements of the organization; and
- provide for ongoing operation and continual improvement of the BCM programme, as well as the BIA process.

5 Performing the Business Impact Analysis

5.1 Introduction

The purpose of the BIA process is to prioritize the various organizational components so that product and service delivery can be resumed in a predetermined order following a disruptive incident to the satisfaction of interested parties.

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

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

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

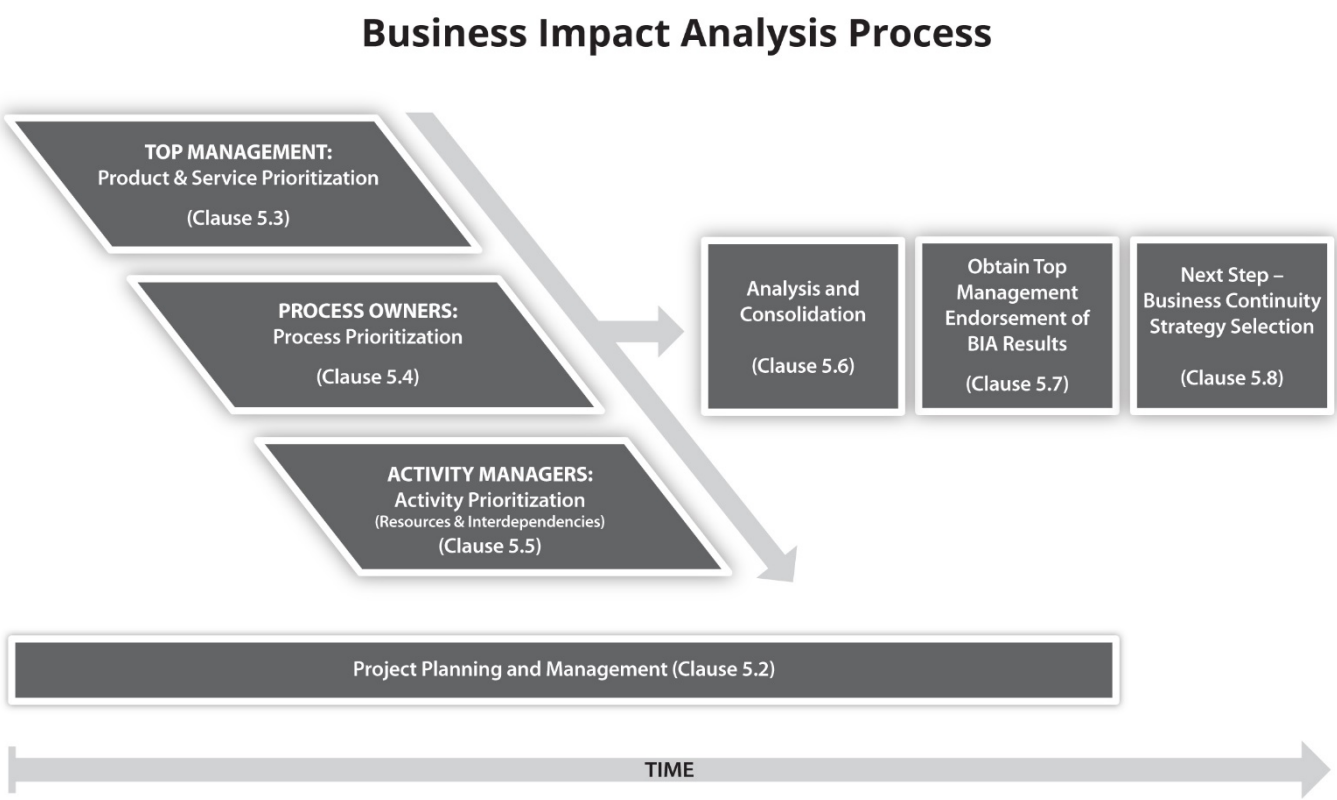

Figure 3 – Business Impact Analysis Process

Successful BIA outcomes may depend on:

- 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 scope and results.

5.2 Project Planning and Management

5.2.1 Introduction (overview)

Although the BIA is a process, organizations may use project management methods to conduct a BIA for a specific time period as a project with a defined start and finish. As the BIA process is potentially complex, using project management methods allows organizations to coordinate resources and timelines.

Project planning tasks may include:

- decide on the scope of the BIA process;
- communicate expectations to BIA process participants;
- identify the BIA sponsor and top management participation;
- establish BIA process roles and responsibilities (including competencies);
- establish the project plan and with consideration given to the use of Gantt charts and work breakdown structures;
- allocate resources for the BIA project;
- gain acceptance of the project approach and plan are secured; and
- establish or source the skills necessary to meet BIA process objectives.

Project management tasks may include:

- implement the BIA process (see clauses 5.2 through 5.6);
- monitor the implementation of the BIA process (see clauses 5.2 through 5.6);
- develop periodic reports on the status, noting performance expectations and recommendations to improve performance in line with top management expectations;
- perform modifications of the BIA approach and scope to meet top management expectations and external (regulatory, statutory, customer, contractual) requirements (see clause 6);
- collect and review lessons learned (see clause 6); and
- make recommendations regarding BIA process improvement for future implementation (see clause 6).

5.2.2 Initial versus Ongoing BIA Processes

An organization undertaking a BIA for the first time may be unable to clearly identify products and services, processes, and activities making the initial BIA effort more exploratory and investigative than subsequent iterations.

During the initial BIA process, the organization should plan for additional time to:

- create awareness and ensure education;
- identify an executive sponsor and/or steering committee;
- determine impact 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 data gathering;
- document the work flow breakdown to a process and activity level; and
- complete data gathering through document review, interviews, workshops, and questionnaires.

During the initial BIA process, the organization may use the BIA results to prioritize subsequent business continuity tasks, including strategy identification and implementation. During subsequent BIA iterations, the organization can focus the BIA process on the changes in the organization's structure and environment, as well as changes to impact tolerance.

5.3 Product and Service Prioritization

5.3.1 Introduction (Overview)

As the first step in the BIA process, the organization's 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

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

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

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

— They 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, for this analysis, the organization may group together products and services when they have similar priorities. 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 a disruption may cause by:

— Identifying customer expectations and the sanctions they have over the organization if these expectations are not met and the impacts they will have on the organization if the sanctions are imposed

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

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

Other interested parties and their impact following a disruption on the organization may include:

— Partner organizations – their willingness to continue to cooperate

— The 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 – sanctions and rule changes

For each group of products and services the organization should document:

- The 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 (maximum tolerable periods of disruption or maximum acceptable outage - see Annex B)
- The reason(s) why this time period has been identified with reference to the growing impacts over time
- The requirements for delivery (to be confirmed later in the BIA process)

The organization may use the information in the following table to understand the impacts of a disruptive incident on the organization:

Table 1 – Product and service level impact categories and 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. Whilst costs may increase at a rate proportional to the disruption time, some impacts may not increase linearly – financial impacts can suddenly increase as contract penalties are incurred or customers lost and reputational damage can occur suddenly at a point during the disruption.

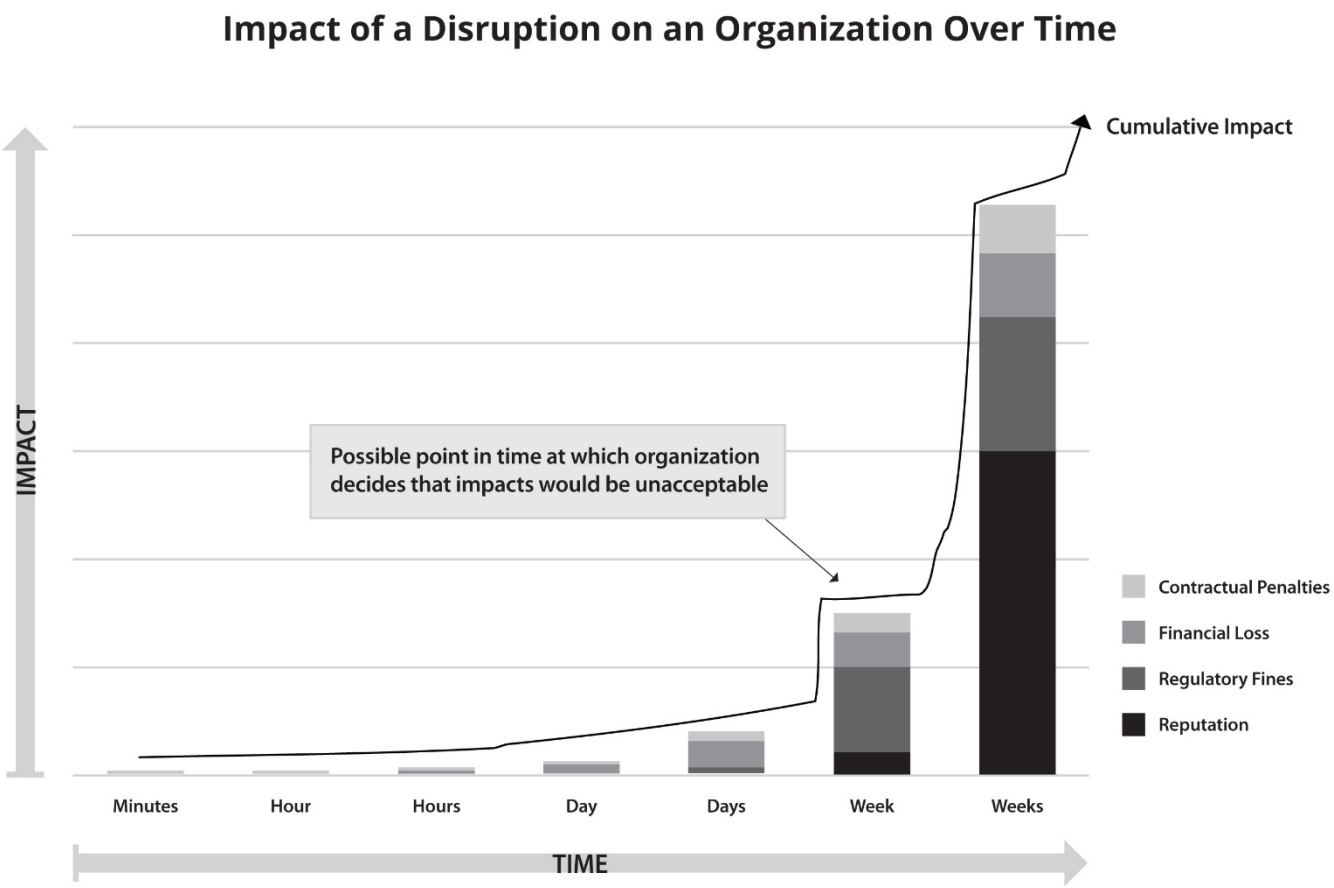

Figure 4 – Impacts over time

The organization should, within the timescale identified above, set a target time for resuming delivery of products and services at specified minimum levels (recovery time objective or minimum business continuity objective). For additional information, see Annex B.

5.3.2 Inputs

Top management may consider the following information in setting product and service priorities:

- current organizational mission, objectives, and strategic direction
- current BCM 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 serious post-incident reports and their impact, if relevant

5.3.3 Outcomes

The outcomes of the product and service prioritization process should be:

- endorsement or modification of the organization's BCM programme scope
- identification of legal, regulatory and contractual requirements (obligations)
- evaluation of impacts over time as it relates to a failure to deliver products/services, which serves as the justification for business continuity requirements (time, capability, quality, etc.)
- 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 the process mapping task (that is the next step in the BIA process)
- Analysis of the organization's strategic objectives, products and services, customers and other interested parties, and downtime requirements.
- Documented list of prioritized products and services (grouped by timeframe or customer, or individual).

5.4 Process Prioritization

5.4.1 Introduction (Overview)

The organization should perform a process level prioritization to determine the interrelationships between internal processes and how they deliver products and services. The organization may also determine activities that make up those processes during the process prioritization task, depending on the size and complexity of the organization. In addition, the process prioritization will, later, assist the organization to develop a timetable for the recovery of activities across the organization.

5.4.2 Inputs

The information required for process prioritization includes:

- the scope of this BIA process
- 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:

- 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 table of impacts in 5.3.4 could be used to consider the impacts of disruption of processes. It may be appropriate to add additional internal impact categories at this level.
- 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.
- initial documented list of activities that deliver processes.

5.5 Activity Prioritization

5.5.1 Introduction (Overview)

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 resources necessary for recovery and to help confirm impact-related conclusions developed at the process level. Resource-related information includes:

- people/skills/roles
- facilities
- equipment
- records
- financing
- information and communications technologies, including applications, data, telephony, and networks
- suppliers, third-parties, and outsource 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 further impact categories outlined in Table 2 below, which may affect the prioritization of specific activities.

Table 2 – Activity level impact categories and examples

Impact Categories	Examples of Impacts
Operational	Delays due to backlog of workload or manual workarounds; impacts to interrelated activities
Welfare	Physical or mental harm to staff or visitors (e.g. injury or stress)

5.5.2 Inputs

The information required to undertake activity prioritization includes:

- process, and product and service priorities
- constituent activities of processes
- scope of the BIA
- organizational chart

5.5.2.1 Information

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

- the processes, products and services that this activity supports
- the method of operation of the activity
- the duration or lead-time of this activity
- fluctuations in demand – peak operating periods
- factors not already discovered that may affect the impact or duration of an acceptable disruption (e.g. backlogs)

5.5.2.2 Resource requirements

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

- staff and contractors – minimum acceptable level for required service
- knowledge, skills or qualifications required
- workplace requirements – can they work from home?
- IT applications and communications (noting special requirements)
- records – electronic or hard copy and their location
- equipment – ICT, office equipment, manufacturing equipment
- legal and regulatory requirements of this activity
- components and raw materials

5.5.2.3 Interdependencies

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

- Reliance on other internal activities or external suppliers of goods or services
- Reliance on other internal activities on the outputs of this activity

For the specification of ICT requirements additional information may be collected such as:

- ICT asset name, location, and configuration (for example, 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

5.5.3 Outcomes

The outcomes of activity prioritization should be:

- confirmation of impacts over time, which serves as justification for business continuity requirements (time, capability, quality, etc.)
- resource needs to perform each prioritized activity (including facilities, people, equipment, ICT assets, suppliers, and finance)
- dependencies on other activities, suppliers, outsource partners, and other interested parties
- required currency of business (operational) information or data (recovery point objective - see Annex B)
- analysis of impacts over time associated with activity downtime.
- analysis of interdependencies of the resources (and other dependencies) needed to deliver processes.
- documented list of prioritized activities that deliver processes, and products and services.
- documented list of prioritized resources that enable activities to operate.

5.6 Analysis and Consolidation

5.6.1 Introduction (Overview)

While analysis occurs during the entire BIA process, the organization should perform a final analysis (or consolidation of analyses) of the BIA process. This involves: reviewing the results from the prioritization activities, 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 depend on the type of information gathered and the desired BIA outcomes.

Regardless of approach, the organization should ensure that the data is:

- Correct = The data are accurate and reliable
- Credible = The data are believable and ‘reasonable’
- Consistent = The data are clear and repeatable
- Current = The data are up-to-date and available in a timely manner
- Complete = The data are comprehensive (no records are missing and every field is known for each record)

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. The following are examples of analytic techniques which may be used:

Table 3 – BIA Analysis Techniques

Quantitative Analytic Techniques	Qualitative Analytic Techniques
Interdependency Analysis Financial Analysis Approaches	Common Sense and Cross Checks Stress Testing Strengths, Weaknesses, Opportunities, and Threats (SWOT) Analysis Quality Criteria for Data Validation (i.e. complete, correct, current, credible, and consistent) Review of Post-Incident Reviews and Recommendations Supplier-Input-Process-Output-Customer (SIPOC)

5.6.4 Outcomes

The outcomes of applying analysis techniques and consolidating information are:

- confirmation of impacts over time
- review and confirmation of resource dependencies and requirements
- consolidation of resource requirements, where appropriate
- review and confirmation of the interdependencies of processes and activities, and their relation to the delivery of products and services results that serve as the input to the business continuity strategy selection

5.7 Obtain Top Management Endorsement of BIA Results

5.7.1 Introduction (Overview)

The organization should seek management endorsement of results, including product and service, process, activity, and resource prioritization following the BIA process and analysis.

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 reporting outputs for 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
- Activity prioritization
    - o Resources and interdependencies

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

5.7.2 Inputs

The following data is needed for top management endorsement:

- products and services, processes, activities, and resources and interdependencies
- organizational downtime impacts over time (see Section 5.2.3)
- recommended business continuity requirements/prioritization, including justification for recommended prioritization (quantitative and qualitative impacts)
- activity and resource interdependency analysis

5.7.3 Methods

An organization should compile summary-level information into a formal report to be presented and approved by top management. The organization may choose to develop report documentation by compiling data (from the analysis effort) or using a word processing or business continuity software tool to pull data into reports.

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

- an overview of the BIA process, including objectives and scope
- impacts influencing the assignment of business continuity requirements (see Section 5.2.3)
- recommended business continuity requirements/prioritization of 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
- facilitating one-on-one meetings with top management to review the summary report in detail

Top management should provide documented endorsement of BIA findings once the organization delivers summary information. Top management should inform the organization of its intention to amend BIA findings such as business continuity requirements, which would require the organization to update summary documentation. The organization should maintain documented approval according to established document management practices.

5.7.4 Outcomes

The outcomes of top management endorsement include a summary of business continuity requirements and all other previous outcomes (5.2 to 5.5). These outcomes are documented in a top management endorsed BIA summary report and presentation.

5.8 Next Step – Business Continuity Strategy Selection

The BIA process results in a number of outcomes, including business continuity requirements. Quantifying business continuity requirements enables the organization to determine and select appropriate business continuity strategies to enable an effective response and recovery from a disruption. Examples include:

- Alternate work area
- Contingent supplier arrangements
- ICT recovery options
- Contingent sources of people
- Equipment and sources of raw materials

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 restates 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 BCM 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 the 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, supplier (insourcing/outsourcing), and site/facility resources
- Structural change
- 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

22317	22301
Introduction	0.3 Components of PDCA in this International Standard
4.2 - BCM Programme Context and Scope	4 - Context of the Organization
4.3 - BCM Programme Roles	5.4 - Organizational Roles, Responsibilities and Authorities 7.2 - Competence
4.4 - BCM Programme Commitment	5 - Commitment
4.5 - BCM 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

These ISO 22301 terms are not used in the document; however, these terms are common with respect to the performance of business impact analysis.

Number	Term	Definition	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.	Clause 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 clause 6.2 which refer to BCM programme objectives	Clause 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.	Clause 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.	Clause 5.5.3

Annex C
(informative)
Business Impact Analysis Data Collecting Methods

This annex summarizes common methods to collect information necessary to reach business impact analysis conclusions.

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 BCM 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?
- BIA process participant competency – What skills and experiences do business continuity professionals have with implementing a 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
- Scenario-Based Exercise

Methods to ensure information consistency, regardless of data collection method:

- Training for those who are leading or participating
- Identifying information requirements
- Oversight or quality assurance of outputs
- Perform a trial of data collection method before implementing on a whole scale
- Identify data points before beginning method

C.1 Documentation Review

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

- 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
    - Documents that describe and detail the processes used in the organization, their inputs and outputs, their constituent activities, and the organizational entities responsible for these activities.
- Organizational charts
    - Hierarchal diagrams that show the relations of individual managers to the organization's top management.
    - Hierarchal diagrams that show the relationship between the processes and organizational units.
- Roles and responsibilities
    - Details on the roles and responsibilities of the various players depicted in organizational charts.
- Service level agreements
    - Agreements with specific details on the minimum acceptable levels of product or service delivered and its associated timelines with customers, clients, business partners, regulatory bodies and government agencies, as well as other internal processes.
- Contractual requirements
    - Agreements between the organization and a customer for the delivery of a service or product.
    - Agreements between the organization and a vendor or supplier for the receipt of a service or product.

C.2 Interview

Organizations may perform interviews, at a process or activity-level (depending on complexity), 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:

1. BIA process overview, objectives, desired outcomes, and the relationship of the BIA to the remaining business continuity planning process
2. BIA participant expectations
3. The relationship of activities to processes
4. Activity discussion:

a) 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

- Peak operating times, seasonality, work cycles

b) Resource dependencies and requirements (see Section 5.4.2)

- Existing workarounds and how long they remain viable

c) Known impact associated with downtime (see Section 5.2.3)

d) Known activity-specific obligations

5. Next steps, including a review of the interview summary, comments and corrections, and approval

Interview good practice includes:

— 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.3 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.

Since, unlike in an interview or workshop, the analyst will not be present to assist the user in completing the information, it is important that the questions be clear in their intent and language.

Common survey content may include:

- Validation of the impacts associated with a disruptive incident, including how the impact changes over time (see Section 5.2.3)
- 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.4 Workshops

Workshops with participants representing different activities or processes may be used 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.5 Scenario-based exercise

Using a scenario-based exercise enables participants to decide on the priority of products and services, process 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 suppliers.

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.

For a process or activity level exercise the objectives should focus on identifying the resources required for recovery requirements and the order, feasibility and maximum time available for recovery to achieve the required recovery of product and service delivery.

The outcomes of an exercise may include:

- The identification of the impacts that would result from a disruption to product and service delivery and the time at which such impacts would become unacceptable
- The prioritization of product and service delivery, processes and/or activities
- The resources required to support an activity including suppliers
- The interdependencies of the activity on other activities

These outcomes may not give results that are as comprehensive as a series of structured interviews but the engagement of the participants and the apparent realism of the situation may give more reliable results. This method is also useful when the time available with the participants is limited.

NOTE When performing scenario-based data collection, be sure to concentrate on the impact of the scenario, as opposed to cause of the scenario.

614 The table below gives additional information regarding strengths, weaknesses, opportunities, and tips regarding
615 each of these information gathering approaches.

616 **Document Review**

Strengths	Weaknesses
Potentially detailed and thought through Evidence already exists / does not require additional effort or verbal communications Leverages previous efforts / promotes cooperation Easy to access	Time consuming Lack of explanation and context Could be out-of-date or incorrect Needed information could be difficult to locate due to volume
Opportunities	**Tips**
Information can come from many sources Can enable the compilation of draft questionnaires/interview questions Can confirm data from other method	Pair with meeting to ensure understand context Read available documentation in preparation for interviews and workshops

617

618 **Interviews**

Strengths	Weaknesses
Involves staff and raises awareness Interviewer gains knowledge of people and functions Discovers actual impacts (near-misses) Address personal views and fears	Time consuming Need to prepare May use more staff time Questionnaire draft still needed Personal response Lacks consistency if more than one interviewer
Opportunities	**Tips**
Use of senior participants Where qualitative assessment is required Use where awareness is a requirement	Formalize interview structure Interview in location Try to interview in context of business deliverables not process aims Take time to explain purpose of BIA

619
620 **Workshops**

Strengths	Weaknesses
Cross-process perspective Brain storming Shows organization's commitment Fewer distractions More professional	Difficult to timetable Difficult to deal with dissent and internal politics in a group Facilitation skills required Lots of preparation
Opportunities	**Tips**
When rapid results required High level of organizational commitment	Sell to management on the basis of cost savings Prepare it well - you only get one chance! Run as an exercise

621 **Scenario-Based Exercise**

Strengths	Weaknesses
Forces decision on timescales and priorities Provides relatable context for understanding strategy options and decisions (including manual workarounds and alternate procedures) More realistic decisions may emerge	Significant preparation required Could narrow scope of discussion to scenario at hand (leaving out other resource losses or threats)
Opportunities	**Tips**
Can also be used to raise awareness of business continuity Plans can be developed or exercised in addition	Make the scenario and exercise realistic to encourage buy-in and involvement

622

623 **Questionnaires/Surveys**

Strengths	Weaknesses
Easy to analyze Easier to standardize response Produces 'hard-copy' evidence Can be automated Software available for remote entry	Questionnaire fatigue Interpretation of Qs Need to cross-check Possibility of error in Qs nullifying results Lack of involvement Miss soft issues Miss major issues through not challenging response
Opportunities	**Tips**
In a mature BCM organization When data can be numerical or ranked As a follow-up If the number of respondents are high Remote locations	Database or spreadsheets for graphs Keep data requirements tight Verify data Mix with interviews

624

Annex D
(informative)
Other Uses for the Business Impact Analysis Process

D.1 Collection of Additional Recovery Planning Information

Throughout the document, we have explained the minimum level of information required to collect in a BIA. However, there is other information that individuals may choose to collect, which may assist in additional planning activities. This may be a rare opportunity to get in front of subject matter experts, so take advantage of it; however, only collect information that you will actually use.

- Employee names and contact information
- Others

D.2 The collection of information useful for plan development and incident response

The specification of BIA contents described in this standard comprise only the information required to select appropriate recovery strategies from the current business continuity requirements.

Conducting a BIA through any of the methods described may be an opportunity to collect additional information which will be useful in developing plans or in responding to a disruptive incident. This information may include:

- At the top management level
    - The planned strategic direction of the organisation – such as mergers, relocation or acquisitions which may affect business continuity strategy in the future and should be taken into account when selecting current strategies
    - Exploration of recovery strategy opportunities such as cooperation with other organisations (who may be competitors) to provide mutual aid.
- At the process level
    - Opportunities to outsource parts or all of a process, temporarily or permanently after a disruptive incident
- At the Activity level
    - The documentation of workarounds for the absence of resources and their limitations of quality, extra resource needs and for how long they are effective.
    - Feasibility of using alternative suppliers
    - Characteristics of staff such as:
    - Skills of individual members of staff – in current and past roles
    - Contact details
    - Their home location and mode of transport to work
    - Ability to work from home – network capacity, equipment, desk location etc.

D.2.1 Increasing the efficiency of the organisation

The overview of the operation of an organisation that emerges from the BIA process may enable participants in the process to identify changes that can improve its efficiency. These changes may not have been apparent until the web of interdependencies within the organisation is explored.

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

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

Understanding the interdependencies of activities may suggest changes in management structure.

D.2.2 To explore alternative strategic planning options

The BIA method described in this standard determines the business continuity requirements of an organization as they are at present. However the organization can also apply the BIA process on one or more future situations in order to understand the business continuity implications of planned changes.

This application of a BIA process may 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 or ICT hardware
- Product or service change – new contracts or change in business terms

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

- A call centre service delivered from two sites may 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 may be considered as potential recovery space rather than disposed of
- A change in staff numbers may affect the time taken to recover an activity
- New technologies may have different recovery timeframes and some may 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

D.2.3 To assist with longer term strategy decision-making

The method of evaluating impacts over time could be applied at a strategic level to a number of strategic decisions other than recovery requirements.
How long have we got to make a strategic change before unacceptable?

- Example: Carbon neutral due to climate change

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

- Pending regulation
- Changes the business environment
- degradation of the physical environment
- shifts in public opinion

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

D.2.4 Project or event BIA

The BIA as described in this standard assumes that the product and service delivery dates can be postponed to a point that is just acceptable to the customer. At times, the product is a project or an event without delivery date flexibility and cancellation may be unacceptable. The organization can apply the BIA process to determine if the delivery date of the event or project can be shifted but only by a set time since the consequences of further delay would be unacceptable.

In this case the process and activity level prioritization efforts can be conducted in reverse; using the time taken by each activity to work backwards from the set date to ascertain at what point each activity needs to be started to achieve the deadline and optionally to assess which activities can be omitted or scaled to deliver the event or project to the minimum acceptable specification. This is conventional project planning and critical path analysis but with the impact analysis driving the due dates and informing the duration of contingency time to be inserted into the project plan. As the project progresses this contingency time can be monitored and slippage controlled by dropping activities that are not in the minimum specification.

Whilst this approach does not guarantee on-time delivery of projects or events, it does ensure top management understanding of the impacts of delays. They may choose to identify which projects or events are within the scope of this approach and whether business continuity staff should have a responsibility within it.

D.2.5 BIA as a Risk Analysis

Some risk management standards use the term "business impact analysis".

Although it is possible to identify the impact of identified threats this is of limited use in determining business continuity strategies which are intended to be useful to respond to both identified and unexpected incidents. Recovery requirements defined only by identified incidents may not be comprehensive.

In this method the measurement of impact by a single variable ignores the essential parameter of time. The impact of an incident on an organization's reputation and finances almost always increases over time; being negligible immediately after the incident to being survival threatening at some time later. A single value for impact cannot describe this variation.

The impact of an incident on an organization appears to be more closely related to the speed and effectiveness of the return to providing products and services to customers than the nature of the incident that caused the disruption. Indeed some organizations have enhanced their reputation by their response to a disruption.

Therefore the identification of impacts by threat alone, as described in risk-based standards, appears to be inappropriate as a method to determine appropriate recovery requirements.

Bibliography

This bibliography and reference list has been complied to provide users of this Standard with the opportunity to access important source documentation used in the development of this Standard. The bibliography will provide valuable assistance to organizations wishing to further refine their knowledge and understanding of resilience and the factors that contribute to successful organisations.

ISO 22300:2012 – *Societal security - Terminology*

ISO 22301:2012 – *Societal security – Business continuity management systems - Requirements*

ISO 22313:2012 – *Societal security – Business continuity management systems – Guidance*