PD ISO/TS 22317:2021

BSI Standards Publication

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

Documents
Document Sharing Hub

Full document details: PD ISO/TS 22317:2021

# National foreword

This Published Document is the UK implementation of ISO/TS 22317:2021. It supersedes PD ISO/TS 22317:2015, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee CAR/1, Continuity and Resilience.

A list of organizations represented on this committee can be obtained on request to its committee manager.

**Contractual and legal considerations**

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2021
Published by BSI Standards Limited 2021

ISBN 978 0 539 15337 8

ICS 03.100.01; 03.100.70

**Compliance with a Published Document cannot confer immunity from legal obligations.**

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 December 2021.

**Amendments/corrigenda issued since publication**

| Date | Text affected |
|---|---|

Documents
Document Sharing Hub

Full document details: PD ISO/TS 22317:2021

TECHNICAL SPECIFICATION

# ISO/TS 22317

Second edition
2021-11

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

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

Reference number
ISO/TS 22317:2021(E)

Documents
Document Sharing Hub

© ISO 2021

Full document details: PD ISO/TS 22317:2021

**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2021

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

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

Published in Switzerland



© ISO 2021 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/TS 22317:2021

# Contents

Page

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

Documents
Document Sharing Hub

© ISO 2021 – All rights reserved


Full document details: PD ISO/TS 22317:2021

# Foreword

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

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

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

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

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

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

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

— the document has been updated to align with ISO 22301:2019;

— the document structure has been updated to improve the description of the business impact analysis (BIA) process;

— more focus has been placed on the BIA process and less on the business continuity programme;

— BIA and the BIA process have been clearly differentiated;

— BIA process roles have been consolidated to BIA leader and activity owners;

— the section "Initial BIA considerations" has been removed and the guidance redistributed;

— the section "Strategy selection" has been removed as it is part of ISO/TS 22331;

— the annex on terminology has been removed;

— the annex on BIA information collection methods has been enhanced;

— a new annex with examples for performing a BIA has been included.

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

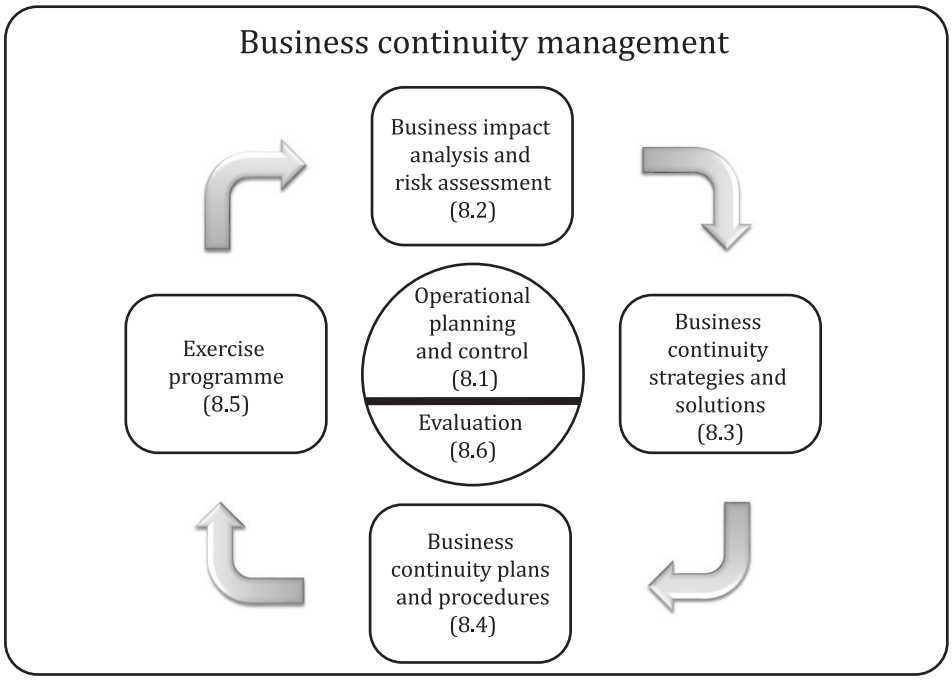

© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TS 22317:2021

# Introduction

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

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

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




NOTE Source: ISO 22313:2020, Figure 5.

**Figure 1 — Elements of business continuity management**

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

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

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

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TS 22317:2021

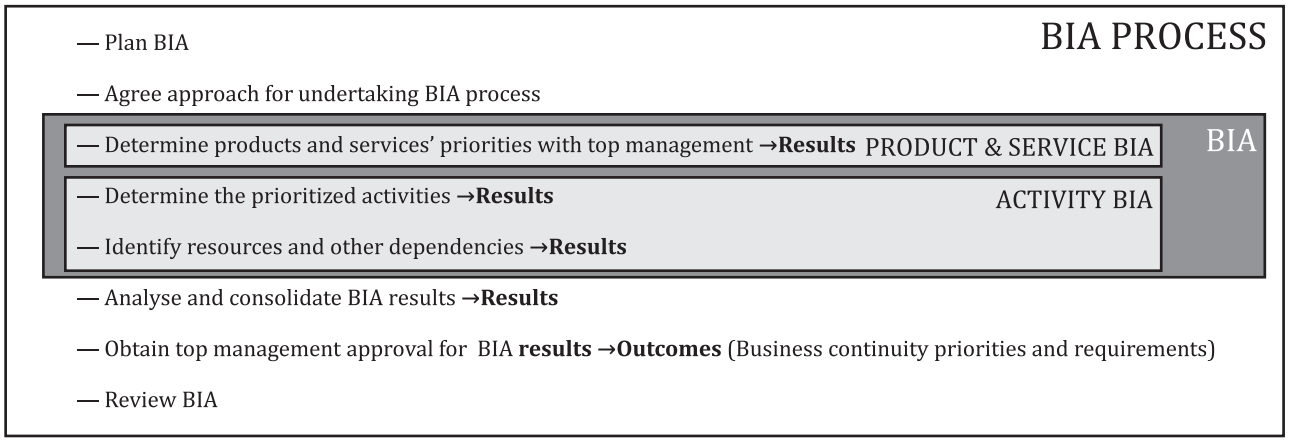



**Figure 2 — Understanding BIA, BIA process, results and outcomes**

The purpose of this document is to:

— provide a basis for implementing an effective BIA process within an organization;

— assist the organization with planning, conducting and reporting on the BIA process in a consistent manner.

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

The outcomes of the BIA process include:

a) endorsement or modification of the organization's BCMS scope;

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

c) evaluation of the impact of a disruption over time on the organization, which serves as the justification for business continuity priorities and requirements;

d) estimation of the time it would take for adverse impacts to products and services to become unacceptable [maximum tolerable period of disruption (MTPD)] following a disruption;

e) identification of the requirements [MTPD and recovery time objective (RTO)] for the prioritized activities;

f) identification of the resources needed to perform prioritized activities following a disruption, including their dependencies, and requirements, specifying RTOs and applicable recovery point objectives (RPOs);

g) identification of dependencies including suppliers, partners and other interested parties;

h) identification of the interdependencies of prioritized activities.

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


© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TS 22317:2021

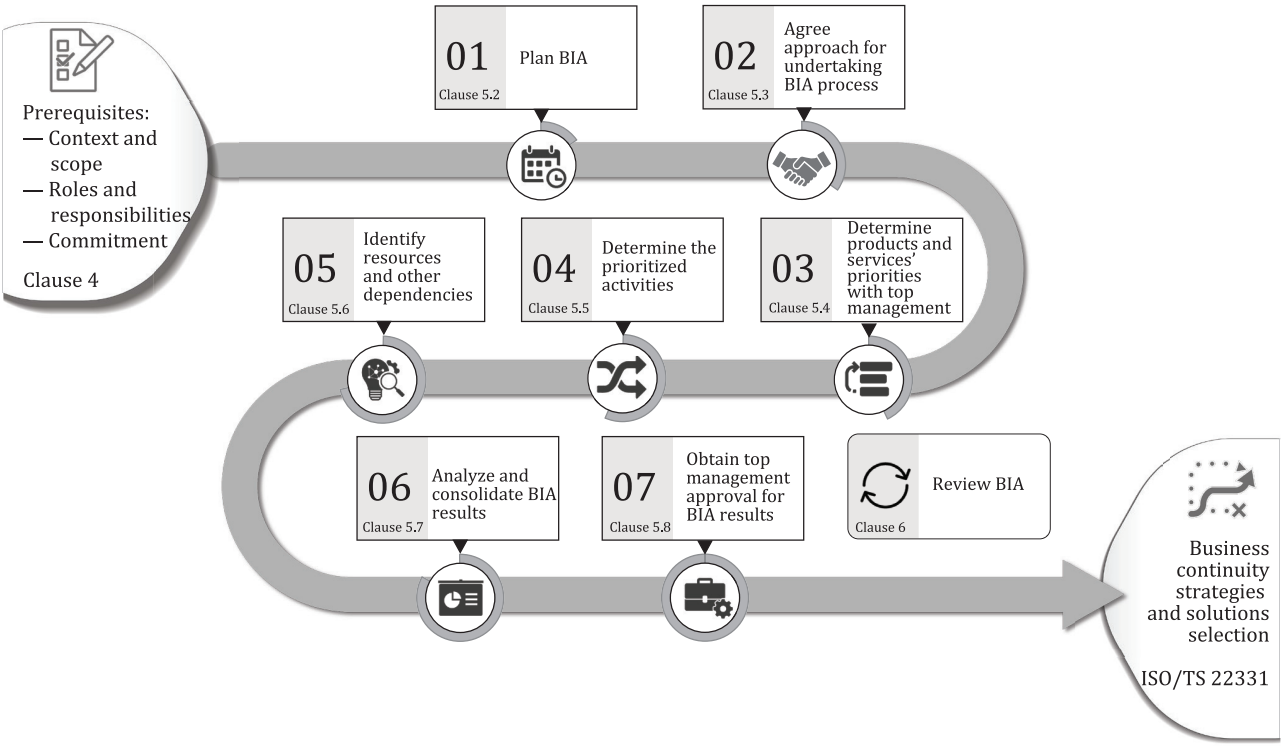



**Figure 3 — BIA process**

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

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

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

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TS 22317:2021

Documents
Document Sharing Hub

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

## 1 Scope

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

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

## 2 Normative references

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

ISO 22300, *Security and resilience — Vocabulary*

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

## 3 Terms and definitions

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

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

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

## 4 Prerequisites

### 4.1 General

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

Before commencing the BIA process, the organization should:

— define the context and scope of the BIA process (see 4.2);

— define and communicate roles and responsibilities (see 4.3);

— obtain leadership commitment and allocate adequate resources (see 4.4).

NOTE See Annex A for a mapping of each clause to ISO 22301.

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TS 22317:2021

## 4.2 Context and scope

### 4.2.1 Context

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

— the external environment (including suppliers, statutory and regulatory bodies) in which it operates;

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

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

### 4.2.2 Scope

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

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

## 4.3 Roles and responsibilities

### 4.3.1 General

Top management should ensure:

— responsibilities and authorities for relevant roles are assigned and communicated within the organization;

— that persons leading the BIA process are competent;

— resources necessary to perform the BIA process are provided.

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

a) BIA leader (this can be the same person as the BCMS manager) (see 4.3.2);

b) activity owners (see 4.3.3).

### 4.3.2 BIA leader

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

— ensure people with the required competencies are available to enable the BIA process;

— prepare and deliver the BIA methodology;

— plan and manage the BIA process;

— make sure that the information provided by the activity owners is consistent throughout the organization;

— undertake consolidation and analysis of the information provided by the activity owners;

— present the outcomes to top management for approval.


© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TS 22317:2021

#### 4.3.3 Activity owners

Activity owners should:

— provide a detailed understanding of the activity for which they are responsible, including all of the resources that enable the activity to operate;

— provide information regarding existing workarounds, business processes and resources that influence the business continuity priorities and requirements;

— apply BIA methodology and provide the relevant information to the BIA leader.

### 4.4 Commitment

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

a) communicate the value of the BIA process;

b) provide ongoing support for the BIA process;

c) provide sufficient resources for the BIA process to:

   1) fulfil BIA process-specific roles and responsibilities, as well as training and awareness requirements, in adequate time;

   2) meet the changing requirements of the organization;

d) agree on the BIA methods, priorities and time frames;

e) ensure an environment that enables continual improvement within the organization;

f) approve the outcomes of the BIA that ensure:

   1) business continuity priorities and requirements are aligned with organization's objectives and strategic direction;

   2) the organization meets its legal, contractual and customer requirements during a disruption;

   3) products and services, business processes, activities and resources are appropriately aligned;

g) ensure that BIA outcomes are available when selecting business continuity strategies and solutions.

## 5 The BIA process

### 5.1 Fundamentals

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

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

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

© ISO 2021 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TS 22317:2021

## 5.2 Plan BIA

Planning tasks can include:

a) allocating necessary resources, including competent people to lead and participate in the BIA process;

b) grouping products and services together when they have similar characteristics, e.g. they can be grouped by type, by geographic area or by line of business;

c) identifying the organization's structure and the teams or individuals that can provide information about products and services, activities and resources;

d) communicating expectations to all participants in the BIA process;

e) establishing the plan, including activities for:

   1) obtaining top management's agreement on the approach for undertaking the BIA process (see 5.3);

   2) organizing meeting(s) with top management to determine products and services' priorities (see 5.4);

   3) identifying and selecting the information collection methods (see Annex B);

   4) defining a template or tool to record the information collected (see 5.5);

   5) gathering information from the activity owners (see 5.5 and 5.6);

   6) analysing and consolidating the information received (see 5.7);

   7) obtaining top management approval for the results (see 5.8);

f) gaining approval of the planned BIA process.

## 5.3 Agree approach for undertaking BIA process

### 5.3.1 Understand impacts

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

The impacts on the organization resulting from the reactions of interested parties can include the examples given in Table 1.

**Table 1 — Impacts due to interested parties**

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


© ISO 2021 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TS 22317:2021

**Table 1** *(continued)*

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

### 5.3.2 Define impact types and criteria

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

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

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

Impact types to be considered can include:

— business objectives;

— environmental;

— financial;

— health and safety;

— legal, regulatory and contractual;

— market share;

— operational;

— reputational.

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

— business objectives;

— financial;

— legal, regulatory and contractual;

— reputational.

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

NOTE Table 3 shows five levels but the number of levels can be adapted to the organization's needs.

AVA Documents
Document Sharing Hub

© ISO 2021 – All rights reserved


Full document details: PD ISO/TS 22317:2021