TECHNICAL SPECIFICATION

ISO/TS 22331

First edition
2018-10

Security and resilience — Business continuity management systems — Guidelines for business continuity strategy

Sécurité et résilience — Systèmes de gestion de la poursuite des activités — Lignes directrices relatives à la stratégie de poursuite des activités

Reference number
ISO/TS 22331:2018(E)

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

Published in Switzerland

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Prerequisites **1**
4.1 General 1
4.2 Context of the organization 2
4.3 Interested parties 2
4.4 Business continuity roles, authorities and competencies 2
4.4.1 General 2
4.4.2 Business continuity strategy roles 2
4.4.3 Business continuity strategy authorities 3
4.4.4 Business continuity strategy competencies 3
4.5 Top management commitment 3
4.6 Business continuity strategy resources 4
4.7 Business impact analysis and risk assessment 4
5 Performing business continuity strategy determination and selection **4**
5.1 General 4
5.2 Principles 4
5.3 Planning and management 6
5.3.1 Overview 6
5.3.2 Initial strategy design considerations 7
5.3.3 Strategy monitoring and continual improvement 7
5.4 Business continuity strategy gap analysis 7
5.5 Determining business continuity strategies 8
5.5.1 Overview 8
5.5.2 Business continuity strategy consolidation 8
5.5.3 Business continuity strategy categories 8
5.5.4 Business continuity strategy types for activities and resources 9
5.6 Selecting business continuity strategies 17
5.6.1 General 17
5.6.2 Strategies for protecting prioritized activities and resources 17
5.6.3 Strategies for resuming and recovering prioritized activities and resources 18
5.6.4 Approval of selected strategies 21
6 Next steps after determining and selecting business continuity strategies **22**
6.1 Implementing business continuity strategies 22
6.2 Establishing and implementing business continuity procedures 22
7 Monitoring and reviewing business continuity strategies **22**
7.1 Performance review 22
7.2 Management review 22
Annex A (informative) **Business continuity strategy within an ISO 22301 business continuity management system** **24**
Bibliography **25**

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.*

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

Introduction

This document provides detailed guidelines for business continuity strategy determination and selection. It is consistent with the requirements of ISO 22301. It is applicable to the performance of any business continuity strategy determination and selection effort, whether part of a business continuity management system (BCMS) or a business continuity programme. Hereafter, the term "business continuity programme" means either a BCMS or a business continuity programme.

The organization's business continuity strategy determination and selection should include strategy options for:

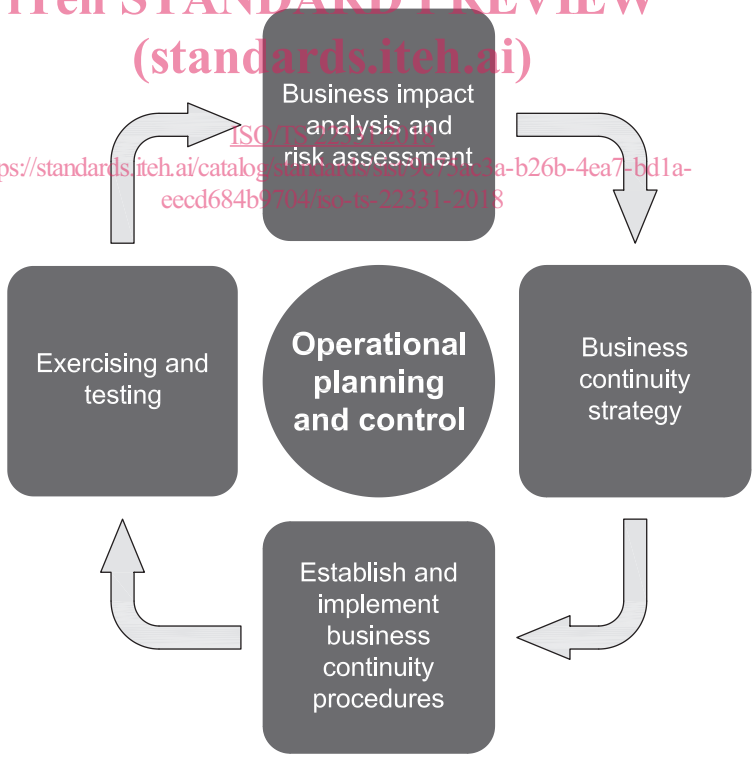
— protecting prioritized activities;

— stabilizing, continuing, resuming and recovering prioritized activities;

— mitigating, responding to and managing impacts (see ISO 22301:2012, 8.3).

NOTE In this document, business continuity strategy options has the same meaning as solutions and capabilities.

Figure 1 notes the relationship of the business continuity strategy determination and selection process to the business continuity programme as a whole. The business impact analysis and risk assessment provide the requirements for a range of business continuity strategies. The determination and selection of a business continuity strategy is the basis for the development of effective business continuity procedures.



NOTE Source: ISO 22313:2012, Figure 5.

Figure 1 — Elements of business continuity management

Business impact analysis identifies the product/service delivery requirements and the prioritized timeframes for activity and resource recovery. The business impact analysis enables the organization to determine the resources needed to perform priority activities (e.g. facilities, people, equipment, information, communication and technology assets, supplies and financing). The business impact

analysis also identifies interdependencies between activities and dependencies on supply chains, partners and other interested parties.

The risk assessment identifies, analyses and evaluates the risk of disruption and identifies risk treatment options.

Business continuity strategy addresses the outcomes of the business impact analysis and risk assessment and determines how the organization can become more resilient and capable of dealing with a wide range of disruptive incidents.

The purpose of this document is to provide guidance that will enable organizations to:

— identify a range of business continuity strategy options;

— select appropriate capabilities based on business continuity requirements;

— ensure the ongoing suitability of business continuity strategies;

— coordinate business continuity strategy determination and selection effectively within the overarching business continuity programme.

Business continuity strategy determination and selection outcomes include:

— measures to attempt to decrease the frequency of disruptive incidents and the impact associated with these disruptive incidents;

— identification of the financial resources needed to respond to a disruptive incident;

— effective internal and external communications capabilities;

— alternate workspace capabilities to address the loss or inaccessibility of premises;

— arrangements to address the unavailability of personnel;

— alternative methods of maintaining, fixing and replacing resources for performing activities in the event of loss;

— capabilities to recover lost information and communications technology (ICT) assets, including data;

— alternate means to deliver products and services when faced with a supply chain disruption.

Figure 2 displays the business continuity strategy determination and selection process, together with prerequisites and its relationship to the creation of business continuity procedures.

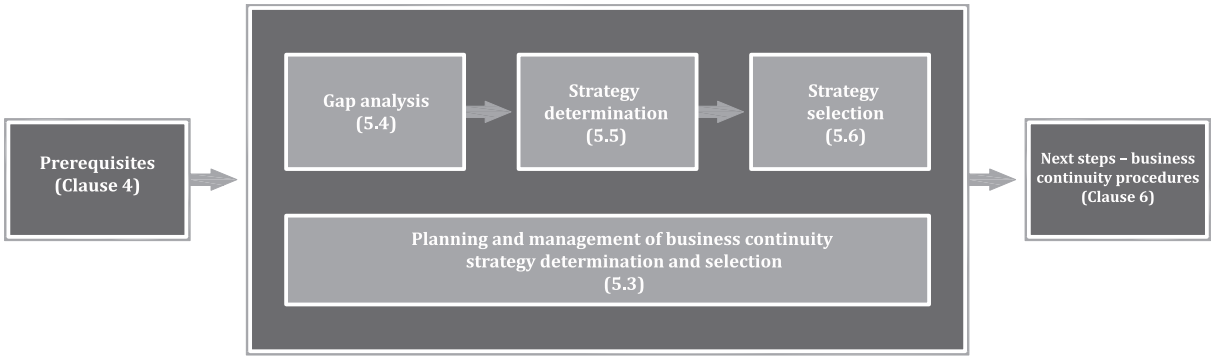


Figure 2 — Business continuity strategy determination, selection and implementation approach

Security and resilience — Business continuity management systems — Guidelines for business continuity strategy

1 Scope

This document gives guidance for business continuity strategy determination and selection. It is applicable to all organizations regardless of type, size and nature, whether in the private, public or not-for-profit sectors.

It is intended for use by those responsible for, or participating in, strategy determination and selection.

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 Guide 73, *Risk management — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and ISO Guide 73 apply.

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

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

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

4 Prerequisites

4.1 General

Although this document is consistent with ISO 22301, it can also be used for business continuity strategy determination and selection when aligning or subscribing to other standards, obligations or regulatory requirements. Regardless of the approach, there are several prerequisites that should be addressed.

Before starting the business continuity strategy determination and selection process, the organization should:

— define the context and scope (4.2);

— understand the needs and expectations of interested parties (4.3);

— define and communicate roles and responsibilities (4.4);

— obtain leadership and management commitment (4.5);

— allocate adequate resources (4.6);

— complete a business impact analysis process (4.7);

— complete a risk assessment (4.7).

NOTE See Annex A for a mapping of each strategy determination and selection process prerequisite or task to ISO 22301.

4.2 Context of the organization

Aspects of context that are particularly relevant to business continuity strategy include:

— the organization's external environment, because of the influence it has on the organization's ability to recover delivery of its products and services to customers;

— laws, regulations and other legal obligations that specify mandatory requirements or influence business continuity strategy in other ways.

4.3 Interested parties

To be effective, business continuity should address the needs and expectations of interested parties. The organization should therefore identify its interested parties and determine their requirements based on analysis of their needs and expectations.

4.4 Business continuity roles, authorities and competencies

4.4.1 General

Top management should determine the roles needed for business continuity strategy determination and selection to ensure that responsibilities and authorities are assigned and communicated within the organization.

4.4.2 Business continuity strategy roles

Roles that are relevant to determining business continuity strategy include:

— sponsoring the business continuity programme and the strategy determination and selection process;

— overseeing the implementation and ongoing monitoring of the business continuity programme;

— managing the business continuity strategy determination and selection process;

— managing business continuity strategy projects.

Specific tasks that may need to be assigned include:

— provision of ongoing advice and guidance on the conduct of the business continuity strategy determination and selection process;

— selection of methods and identification of required outcomes;

— decision-making regarding resource requirements and risk treatments;

— determination of the competencies required for business continuity strategy determination and selection;

— ensuring that business continuity requirements are met.

4.4.3 Business continuity strategy authorities

The determination of business continuity strategies can be challenging and complicated. It requires a good understanding of how to go about it and detailed knowledge of the organization and its processes. Selected strategies may also require significant resourcing and capital expenditure.

It is therefore important that those responsible for determining and selecting strategies have the full support of top management and include persons who:

— have an organization-wide perspective;

— have knowledge of the current and future business strategy;

— have decision-making authority;

— have a detailed understanding of the organization's products, services, processes, activities and resources;

— are familiar with the organization's decision-making and capital expenditure requirements;

— understand the outputs of the business impact analysis and risk assessment; and understand the business continuity strategy determination and selection process.

4.4.4 Business continuity strategy competencies

The organization should ensure the competence of persons leading or participating in the business continuity strategy determination and selection process. Competences should include skills and abilities related to:

— project/programme planning and management;

— information gathering;

— analysis, including problem solving and cost-benefit analysis;

— effective communication and collaboration;

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

— applying business continuity principles in determining strategy within the organization's context;

— knowledge of the organization, its products and services, processes, activities and resources, as well as the outputs of the business impact analysis and risk assessment.

4.5 Top management commitment

Top management commitment is vital for:

— ensuring the organization selects the most appropriate business continuity strategies based on management-approved business continuity requirements;

— ensuring the organization meets its legal, regulatory and contractual obligations before and following the onset of a disruptive incident.

Examples of how top management could demonstrate its commitment include:

— ensuring that the necessary resources are provided;

— participating in selecting the most appropriate business continuity strategies.

4.6 Business continuity strategy resources

The organization should determine and provide the resources needed for business continuity strategy and selection that will enable it to:

— comply with its business continuity policy and achieve its business continuity objectives;

— provide for monitoring and continual improvement of its business continuity strategies.

Resources and their allocation should be identified in business plans and reviewed periodically to ensure their adequacy. It may be appropriate to involve top management in this review.

4.7 Business impact analysis and risk assessment

The organization should complete business impact analysis and risk assessment to determine business continuity requirements of products, services, processes and activities, including their:

— priority;

— timescales for resumption;

— minimum levels of operation;

— resource requirements;

— interdependencies;

— dependencies on external suppliers.

For prioritized activities, business impact analysis and risk assessment should also identify:

— data backup requirements, including the currency of data;

— risks to the activity and its dependencies;

— risk treatments already in place.

5 Performing business continuity strategy determination and selection

5.1 General

The business continuity strategy determination and selection process results in capabilities that the organization can implement and improve over time to mitigate the effects of disruption-related risk and to improve the ability to respond and recover from a disruptive incident, consistent with business continuity requirements.

The organization should have in place a mechanism for business continuity strategy determination and selection, including a review and approval of recommended solutions. This clause describes the determination and selection process, as well as the principles and assumptions necessary to determine and select the most appropriate capabilities.

5.2 Principles

The guidelines in this clause are based on the following principles.

— Strategies are required for:

  — protecting prioritized activities from disruption;

  - stabilizing, continuing, resuming and recovering prioritized activities, dependencies and resources that have been disrupted.

- The determination and selection of business continuity strategies should be based on the outputs from the business impact analysis and risk assessment.
- Strategies should deliver the business continuity requirements needed to achieve business continuity objectives:
  - the recovery time objective (RTO) for a resource may be longer than the RTO for an activity due to business requirements, which may include the availability of workarounds;
  - the RTO for a resource may be shorter than the RTO for an activity if there is a significant set-up time or if it is shared with other activities with more demanding RTOs.
- In general, the higher the priority (and the shorter the RTO) that has been assigned to a product, service, process or activity in the business impact analysis, the more complex and expensive the appropriate strategy to recover it.
- Doing nothing:
  - is an acceptable strategy when there is sufficient time after a disruption to source the required resources and to resume the activity before the non-delivery of products and services leads to unacceptable impacts on the organization;
  - is not an acceptable strategy if management decides not to implement appropriate capabilities and this inaction would prevent the delivery of products or services beyond their RTO; in this case, these products and services should be explicitly excluded from the scope of the BCMS.
- The business context in which the organization operates may also determine the applicability of strategy options for their products and services. For example:
  - a public sector organization (such as local emergency services) could rely on similar neighbouring organizations to provide the service if it is unable to do so (this may be called “mutual aid”);
  - a commercial organization could similarly consider employing outsourcing to provide its products and services during a disruption. However, directing clients towards a competitor could lead to a long-term loss of business. Therefore, the commercial organization might decide to keep its recovery capability in-house.
- There might be statutory or regulatory rules prohibiting outsourcing to other organizations where this strategy might reduce the overall resilience of the sector or could lead to breaches of information security.
- Consideration should be made of the most severe disruptions that the organization is prepared to cope with through its business continuity programme, without compromising its current objectives.
- Any alternate resource should be located at a sufficient separation distance from the primary resource. There is no specific or prescribed distance separation for all organizations and resources. The distance could be based on the perceived likelihood of large scale destructive events from which the organization seeks to protect itself. Factors may include:
  - climatic events;
  - environmental quality;
  - geological stability;
  - infrastructure resilience;
  - political stability.
- Diversity of resources, including suppliers, can provide some protection.

— The evaluation of strategies should include consideration of the following aspects.
  — Reliability: Will the strategy work? Will it be possible to test the effectiveness of the strategy before an incident?
  — Agility: How flexible or adaptable is the strategy to changing circumstances?
  — Risk: What is the risk of the strategy being ineffective due to resources not being available?
  — Cost-benefit: Does the strategy meet business continuity objectives for a justifiable cost?
  — Context: Does the strategy address human, cultural, political and technical factors?
— Where strategies depend on key suppliers, the business continuity of those suppliers should be evaluated.
— There should be sufficient resources to implement the selected strategy options.
— The organization should have a mechanism in place for the review and approval of recommended solutions.

5.3 Planning and management

5.3.1 Overview

Project planning and management of business continuity strategy determination and selection allows the organization to optimize and coordinate resources and timelines. The organization should identify a wide range of strategy options and then implement the chosen strategy as one or more projects.

Tasks may include:

— deciding on the scope of the business continuity strategy determination and selection process;
— communicating expectations to strategy determination and selection participants;
— identifying the person sponsoring strategy determination and selection and top management participation;
— specifying competencies for strategy determination and selection responsibilities;
— establishing the project plan;
— allocating resources for strategy determination and selection;
— gaining acceptance of the project approach and plan;
— establishing or sourcing the skills necessary to meet strategy process objectives;
— developing periodic reports on the determination and selection status to improve performance in line with top management expectations;
— performing modifications of the strategy approach and scope to meet top management expectations and external (regulatory, statutory, customer, contractual) requirements;
— collecting and reviewing lessons learned;
— making recommendations regarding strategy determination and selection approach improvement for future use.