
**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*



This document is a preview generated by ERS



COPYRIGHT PROTECTED DOCUMENT

© ISO 2018

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
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

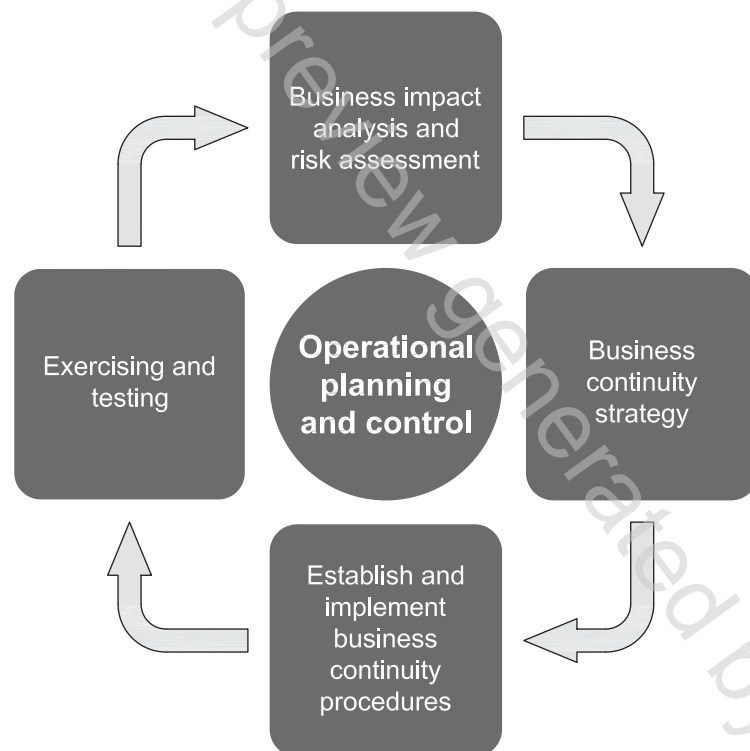
This document provides detailed guidelines for business continuity strategy determination and selection. It is consistent with the requirements of ISO 22301. It is applicable to the performance of any business continuity strategy determination and selection effort, whether part of a business continuity 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.

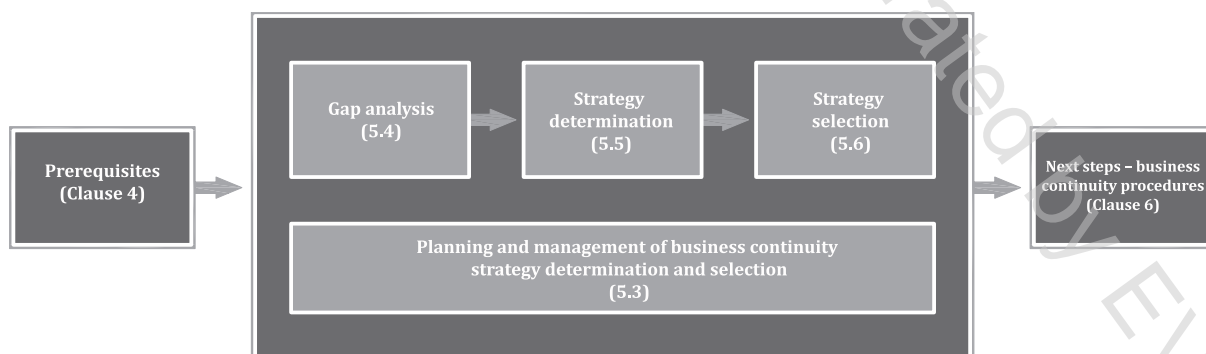


Figure 2 — Business continuity strategy determination, selection and implementation approach

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);