Säkerhet och resiliens – Ledningssystem för kontinuitet – Vägledning för att välja strategi för kontinuitet

Security and resilience – Business continuity management systems – Guidelines for business continuity strategy
Standarder får världen att fungera

SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.

Delta och påverka
Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

Ta del av det färdiga arbetet

Utveckla din kompetens och lyckas bättre i ditt arbete

Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.

Standards make the world go round

SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.

Take part and have influence
As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

Get to know the finished work
We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

Increase understanding and improve perception
With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00

Contents

Foreword .................................................................................................................. iv
Introduction ............................................................................................................... v
1 Scope .................................................................................................................... 1
2 Normative references .......................................................................................... 1
3 Terms and definitions .......................................................................................... 1
4 Prerequisites ......................................................................................................... 1
  4.1 General .............................................................................................................. 2
  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.

![Figure 1 — Elements of business continuity management](image)

NOTE Source: ISO 22313:2012, Figure 5.
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.
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

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);
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.