TECHNICAL SPECIFICATION

ISO/TS 22332

First edition
2021-05

Security and resilience — Business continuity management systems — Guidelines for developing business continuity plans and procedures

Reference number
ISO/TS 22332:2021(E)

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

Contents

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

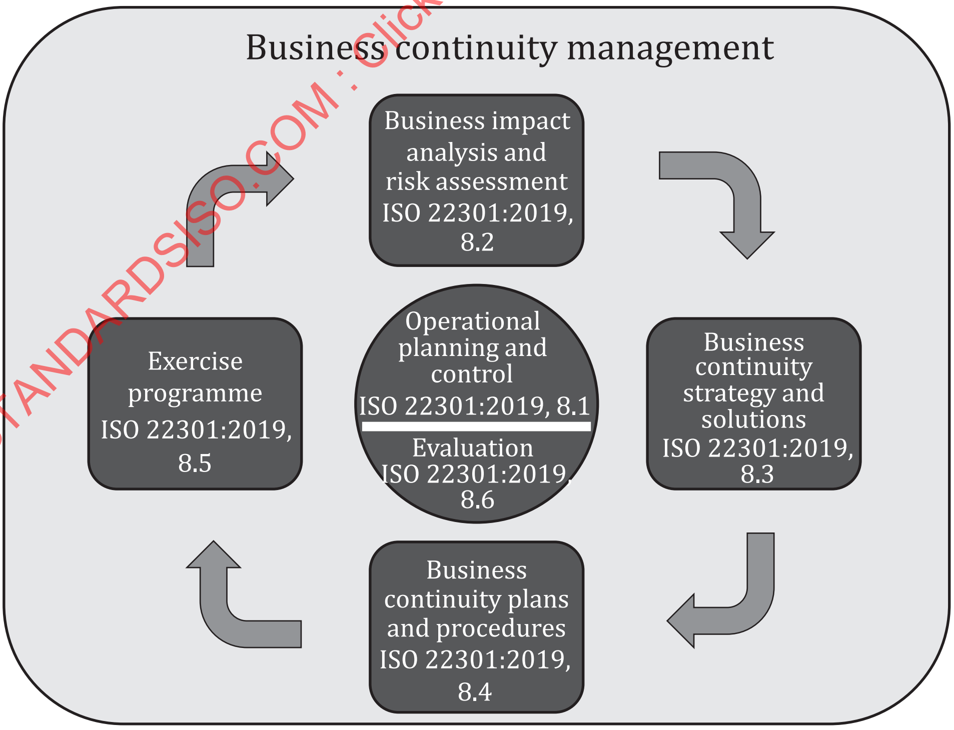
This document provides guidelines for developing and maintaining business continuity plans and procedures. This document is consistent with the requirements in ISO 22301 and the guidance in ISO 22313, and is applicable to the performance of any business continuity plan development, or as part of a business continuity management system (BCMS).

A business continuity plan provides guidance and information to assist teams responding to a disruption (ISO 22301:2019, 8.4.1) in order to meet expectations regarding delivery of products and services. The organization should create plans and procedures to address communications, emergency management, incident response, crisis management, recovery and restoration.

Business continuity plans and procedures should be consistent with organizational goals and objectives and business continuity objectives (see ISO 22301:2019, 3.4) and detail the actions that teams will take during a disruption in order to:

- activate the response;
- manage the immediate consequences of a disruption;
- continue or recover prioritized activities within predetermined time frames utilizing, if appropriate, the agreed business continuity strategies and solutions;
- monitor the impact of the disruption and the organization's response to it;
- deliver products and services at agreed capacity.

Figure 1 presents the flow between the different components that constitute business continuity management. The business continuity strategy and solutions process (ISO 22301:2019, 8.3) provides the input for identifying, developing and maintaining business continuity plans and procedures (ISO 22301:2019, 8.4). In turn, the business continuity plans and procedures are a prerequisite for coordinating and performing business continuity exercises and tests (ISO 22301:2019, 8.5).


Business continuity management
Business impact analysis and risk assessment ISO 22301:2019, 8.2
Exercise programme ISO 22301:2019, 8.5
Operational planning and control ISO 22301:2019, 8.1
Evaluation ISO 22301:2019, 8.6
Business continuity strategy and solutions ISO 22301:2019, 8.3
Business continuity plans and procedures ISO 22301:2019, 8.4

SOURCE ISO 22313:2020.

Figure 1 — Elements of business continuity management

The purpose of this document is to provide organizations with:

- detailed methods to develop business continuity plans and procedures;
- a structured approach to collect and organize information to develop plans and procedures;
- advice for maintaining plans and procedures over time to establish a continual improvement environment.

Following these guidelines will lead to the:

- establishment of a management structure to respond to a disruption, appointing competent and responsible personnel and teams with the authority to manage the response;
- implementation and maintenance of response processes addressing the protection of life and assets;
- establishment of command and control of the recovery effort following the onset of the disruption;
- implementation and maintenance of communication and warning procedures, including those necessary to manage the media response and coordination with other interested parties throughout a disruption;
- continuity or recovery of disrupted business activities and unavailable resources within predetermined time frames, including procedures necessary to return business activities from the temporary measures adopted during the incident to normal operations;
- recovery of disrupted technology assets;
- establishment of procedures to maintain capabilities and response readiness such as cross-training and exercising.

Security and resilience — Business continuity management systems — Guidelines for developing business continuity plans and procedures

1 Scope

This document provides guidelines for developing and maintaining business continuity plans and procedures. It is applicable to all organizations regardless of type, size and nature, whether in the private, public, or not-for-profit sectors, that wish to develop effective business continuity plans and procedures in a consistent manner.

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 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 https://www.electropedia.org/

4 Prerequisites

4.1 General

Although these guidelines are consistent with ISO 22301, they can be used to develop and maintain business continuity plans and procedures when aligning or subscribing to other standards, obligations or regulatory requirements. Regardless of approach, several prerequisites need to be addressed. The organization should:

- understand the needs and expectations of interested parties (4.2);
- complete strategy determination and selection (4.3);
- define and communicate roles and responsibilities of those required to develop plans (4.4);
- allocate adequate resources to develop and maintain plans (4.5).

4.2 Interested parties

Business continuity should address the needs and expectations of interested parties. Therefore, the organization should identify its interested parties and determine their requirements for the response and recovery effort during a disruption.

4.3 Identify approved business continuity strategies and solutions

Prior to developing business continuity plans and procedures, the organization should have completed the determination, selection and approval of business continuity strategies and solutions, including identification of:

- alternate working arrangements to address the loss or inaccessibility of premises;
- arrangements to address the unavailability of personnel;
- capabilities to recover disrupted technology assets and services, including data and communications;
- alternate means to deliver products and services when faced with a supplier disruption.

NOTE See ISO 22301 and ISO 22331.

4.4 Business continuity plan development, roles and competencies

Top management should assign someone with the appropriate authority to oversee a team to develop the business continuity plans and procedures to cover the scope of the business continuity management system (BCMS).

Roles or tasks that are relevant to developing business continuity plans and procedures can include:

- managing business continuity planning projects;
- designing a plan template to ensure consistency;
- contributing content to business continuity plans and procedures;
- approving business continuity plans and procedures.

The organization should ensure the competence of persons leading or participating in developing and maintaining business continuity plans and procedures. Competences should include:

- understanding the organization;
- project planning, management and collaboration;
- information gathering;
- understanding organizational processes and workflows;
- effective oral and written communication;
- methods and techniques necessary to manage the response to a disruption.

4.5 Resources for developing and maintaining business continuity plans and procedures

The organization should determine and provide the resources needed for developing and maintaining business continuity plans and procedures that will enable it to:

- comply with its business continuity policy and achieve its business continuity objectives;
- activate its response and recovery strategies and solutions in a timely manner;
- maintain the readiness of its response;
- provide for the continual improvement of its business continuity plans and procedures (e.g. conducting regular tests).

Resources include personnel time and financial resources necessary to document and maintain business continuity plans and procedures.

5 Response

5.1 General

During a disruption, business continuity plans and procedures should:

- enable the organization to make timely decisions;
- be sufficiently flexible to accommodate unanticipated and evolving situations;
- focus on minimizing the anticipated impacts of disruptions;
- make use, where appropriate, of the prepared business continuity strategies and solutions to minimize impacts;
- identify roles and assign responsibilities for all response activities;
- have available resources required to support response activities.

5.2 Response structure

The organization should establish a response structure consisting of one or more teams, each supported by a set of documented plans and procedures. Working together during a disruption, these teams will enable the organization to:

- identify, escalate and manage the incident;
- manage the needs of all interested parties;
- resume the delivery of products and services within predetermined time frames at acceptable capacity.

If the nature of the incident threatens life or property, immediate actions to protect these can be initiated.

A hierarchical team structure can be created comprising:

- Strategic team: a top management team that will, if required, manage the strategic issues of the incident, in particular those external to the organization such as communication, regulatory and reputation. Top management can choose to delegate the delivery of internal and external messages to a separate communication team.
- Tactical team(s): a management team, or a number of teams, that manage the internal response to the incident and recovery of activities. Tactical team(s) analyse the impact of the incident and direct the operational teams to implement the appropriate solutions from those available, ensure the timely resumption of product and service delivery and provide progress updates to the strategic team.
- Operational teams: each department or business unit can have plans which, depending on its function, describes how it will respond to disruptions. It operates under the direction of a tactical team and reports progress to them.

In a small organization, one team can be appropriate to manage all aspects of the response.

5.3 Competence of team members

In order to meet the objectives of the teams, careful consideration should be given to the selection of team members. Table 1 highlights characteristics that members of each of the teams should have.

Table 1 — Characteristics of team members

Team level	Team member competence
Strategic team	— understand the strategic goals of the organization; — knowledge of their responsibilities and capability to execute; — provide oversight to teams; — decisive under pressure; — ability to anticipate possible impact(s) to the organization.
Tactical team	— knowledge of their responsibilities and capability to execute; — understand relationships among all teams and plans; — ability to coordinate multiple activities at the same time and communicate with strategic, tactical and operational teams; — understand complexities of the organization and consequences of decisions; — ability to work and make decisions under pressure; — demonstrate pragmatic problem solving; — ability to challenge decisions.
Operational team	— knowledge of their responsibilities and capability to execute; — ability to work accurately and methodically under pressure; — disciplined to follow instructions; — ability to escalate concerns or problems.

6 Types of business continuity team plans and procedures

6.1 General

Procedures are documented in plans.

Each team requires a plan to ensure the team:

- understands its scope, objectives and responsibilities;
- has the information immediately available that will enable it to perform its assigned tasks.

The content of each plan will therefore be different, though there should be a common structure across all the organization’s plans to make them easier to understand, maintain and ensure consistency.

6.2 Strategic team plan

6.2.1 Purpose

The strategic team plan ensures that the organization's response to an incident is coordinated and effective, as well as timely. The procedures should include the basis for managing all possible issues facing the organization during an incident. Strategic plans assist top management in managing:

- strategic direction of the organization during the incident;
- monitoring the severity of the disruption;
- maintaining its reputation through internal and external communications to interested parties;
- continued compliance of the organization with statutory and regulatory requirements.

6.2.2 Team composition

The strategic team will consist of top management. Additional expertise can be brought in, depending on the nature of the disruption and the competency required.

The responsibility for initiating and leading the response can be given to a member of the top management team, as it requires the following attributes:

- ability to be decisive under pressure;
- make decisions when current information can be inadequate, erroneous or delayed;
- manage people who are operating under stress.

Some, more complex organizations can establish local, regional or global strategic teams.

The strategic team should have appropriate administrative support.

6.2.3 Owner

A member of top management should own the strategic plan.

6.3 Tactical teams' plans

6.3.1 Purpose

Tactical teams' plans provide guidance to manage and coordinate the continuity of the processes and activities required to deliver products and services and ensure that resources are allocated appropriately. Tactical teams' plans are more general or broader than operational plans. Each team's plan should clearly define their member's interrelationships with the organization's strategic and operational plans. Less complex organizations can define all their plans as operational plans.

Example of a tactical plan includes the coordination:

- of how staff from multiple business units will be transported to an alternate site;
- of the resources needed to support multiple business units;
- with other tactical teams to ensure prioritized activities are performed, as defined in operational plans can be recovered.

6.3.2 Team composition

A tactical team will consist of senior managers or business unit leaders who convene to make decisions for more than one operational plan. Some, more complex organizations can establish tactical plans led by division heads, or product and service heads responsible for the areas covered by the plan.

6.3.3 Owner

A tactical team's plan should be owned and maintained by the person with authority to make decisions on behalf of the area being coordinated.

6.4 Operational teams' plans

6.4.1 Purpose

Operational teams' plans provide action-oriented guidance and information to assist each team to respond to the immediate effects of a disruption by containing it where possible and managing the direct consequences to ensure the delivery of products and services. Each team's plan should clearly define their member's interrelationships with the organization's strategic and tactical plans.

Example of an operational plan includes:

- emergency response plan which describes the tasks and steps needed for response to protect life safety and secure the facility;
- business unit recovery plan which describes the steps to recover and resume business activities;
- technology recovery plan which describes the steps to restore the technology infrastructure.

6.4.2 Team composition

An operational team can be led by the head of the business unit (or their delegate) and is comprised of select business unit personnel.

6.4.3 Owner

The owner of an operational plan should be the head of the business unit or other member of staff with a detailed working knowledge of the activities needed to resume operations, as well as execution of the plan and procedures. The owner is also responsible for maintaining the plan.

7 Content of business continuity plan and procedures

7.1 General

Teams will have some common responsibilities, and team members can have specific roles, therefore the plan for each team can be created by incorporating relevant sections from those described in 7.2 and 7.3. These are either:

a) common to all, or most, plans;

b) specific to one, or a few, plans.

Any plan can consist of all common sections in 7.2 and the relevant specific procedures in 7.3. The order of sections in the plan should be chosen to make the document easy to use.

7.2 Common sections

7.2.1 Purpose

The purpose of the plan should provide a short statement regarding the intent of the plan, its scope and any exclusions. The introduction can also provide an overview of assigned responsibilities in executing the plan and procedures.

7.2.2 Objectives

Each business continuity plan should contain a list of objectives that define outcomes when using the plan.

Examples of objectives include:

- ensure safety and security of people and assets;
- recover activities based on agreed recovery time objectives;
- provide information about alternative workplace solutions;
- recover applications, data and connectivity;
- provide communications to interested parties;
- protect the organization’s brand and reputation.

7.2.3 Assumptions

Each plan is based on the assumption that the solutions described within the plan are available when it is activated.

Examples of assumptions include:

- funding is available;
- alternative workplace is available;
- assigned personnel are trained.

7.2.4 Activating and assembling the team

Each plan should contain criteria for activating the team and a procedure for notification and assembly of its members.

7.2.5 Team member roles and responsibilities

Team roles and responsibilities can be assigned to individual team members. Alternate team members for each role should also be determined. Organizational titles or names should be assigned to each role. For organizations that operate from more than one location, consideration can be given to also nominate an alternate from a different location in a secondary or tertiary role.

Examples of roles and responsibilities in a business continuity plan include:

- Plan owner: Ensures plan is in place, is current and exercised. This role can become team leader at time of incident.
- Team leader: Coordinates and oversees the team in the execution of documented recovery procedures.

- Team member: Performs business continuity procedures, recovering business activities and resources within agreed recovery time objectives.

7.2.6 Tasks

Tasks should address actions to achieve the plan's objectives. Tasks should reference other documentation or procedures where needed. Tasks should also allow for flexibility in case of unexpected events.

7.2.7 Communications

The plan should include mechanisms that will be used to communicate among team members and other teams. This includes reporting up and down the response and recovery team hierarchy.

Plans should have procedures that cover:

- communication between team members when they are at separate locations;
- regular reporting of the team's status;
- escalation of issues, for example the unavailability of resources;
- the protocols for communicating with interested parties;
- alternative means of communication.

7.2.8 Interrelationships with other plans

Interrelationships and dependencies between plans should be identified.

When developing plans, the organization should consider how they affect other plans and procedures. Examples include:

- timing (i.e. procedure needed before another procedure can be accomplished);
- impact on the organization's interested parties.

7.2.9 Standing down the team

The plan should include a procedure for formally standing down the team based on predefined criteria.

7.2.10 Resource information

The plan should include resources, alternatives and workarounds available to the team to obtain stated objectives. These can include:

- accommodations;
- people;
- technology;
- suppliers;
- sources of information;
- transportation.

The quantity of resources needed over time should be identified and can need to be quantified by location.

7.2.11 Contact information

Contact information should include:

- team members and alternatives;
- other teams that are interdependent;

Some plans can include contact information for:

- business unit personnel;
- warning and informing sources, emergency services, utilities;
- lawyers, regulators, local authorities;
- suppliers, contractors;
- media contacts;
- other interested parties.

NOTE The recording and secure storage of contact information can be subject to privacy regulations. The organization will need to ensure effective availability during a disruption.

7.2.12 Appendices

The plan can include appendices such as:

- a blank event log for completion during a disruption;
- maps of alternative locations;
- contents of team's equipment box;
- checklists;
- meeting agenda.

7.2.13 Version control

Version control should be included in the plan.

A procedure should be in place to ensure the most up to date plan is in use and distributed to team members.

7.2.14 Plan control and distribution

Each plan should identify:

- who owns the plan;
- who maintains the plan;
- who has read or update access to the plan;
- security confidentiality classification;
- how circulation is controlled.

7.3 Specific procedures

7.3.1 Emergency response procedures

Emergency response procedures can include:

- response to warning systems;
- assessing the impacts against escalation criteria;
- ensuring the first priority is safety of life;
- preventing or minimizing harm to the organization and its assets;
- event-specific responses (different risks trigger different responses e.g. earthquake, fire, evacuation);
- restoring damaged facilities.

7.3.2 Communications procedures

Internal communication procedures can include:

- internal communication methods (e.g. intranet, pre-recorded message or mass notification system);
- internal contact details of parties interested in the communication;
- roles and responsibilities for internal communications;
- predefined internal messages that can include:
  - a reminder to staff about who is entitled to speak on behalf of the organization;
  - the prohibition to post on social media about the organization's internal issues;
  - how interested parties will be updated on the evolving incident (thus avoiding undesired insistence to be informed);
- templates and pre-written statements for any anticipated communications, allowing messages to be adapted to individual requirements;
- pre-written answers to general questions that are applicable for most incidents;
- approval of the release of communications.

External communication procedures can include:

- external communication channels (including social media);
- external contact details of parties interested in the communication;
- external interested parties' expectations;
- assignment of key roles including:
  - the spokesperson(s);
  - press officer;
  - social media monitoring;
  - technology support;
- guidelines for media response;

- legal advice for public communications;
- pre-written statements for any anticipated communications, allowing messages to be adapted to individual requirements;
- pre-written answers to general questions that are apply to most incidents or crises;
- pre-written positive messages to exploit the media attention on the organization (including general background statement about the organization);
- pre-approved press releases;
- guidelines for safe communication tools;
- guidelines to activate a website section or webpages that will be used as a focus point to communicate specific and relevant information;
- list of who will communicate with each interested party, and the method of communication (e.g. phone, email, emergency notification system);
- approval of the release of communications.

7.3.3 Information and Communication Technology (ICT) procedures

ICT procedures should include the following to recover from ICT failures:

- alignment with business requirements for recovery time objective (RTO) and recovery point objective;
- acquisition of necessary resources;
- tasks to recover data, ICT networks and interfaces, considering the sequence of recovery and dependencies;
- validation of resumption of ICT services by the impacted business;
- solutions for returning to normal.

The ICT business unit should also document a business continuity plan, including procedures, for the resumption of their own activities.

7.3.4 Alternative facilities setup procedures

Procedures can include the set-up of facilities at an alternative location, such as ICT equipment, meeting room, communications facilities, office environment, production or testing facilities. This can include:

- the location(s) for the facilities;
- activating an alternative location;
- what equipment is required, with technical specification if appropriate;
- where resources can be sourced from (with alternatives);
- the details of the required layout;
- tests to be conducted to ensure the facilities and resources are working.

7.3.5 Alternative resource procedures

Procedures for acquiring alternative resources can include:

- specification of resource requirements;

- identification of potential alternatives;
- acquisition of resource alternatives;
- activation of resource alternatives;
- contact list of potential suppliers.

8 Plans for response to specific disruptions

8.1 General

The organization can document its approach to specific anticipated disruptions. This can include steps to mitigate the impact of the disruption and describe specifically how strategies, solutions and resources can be deployed if the disruption happens.

These plans need to be kept up to date and be adjusted to the specifics of the disruption, when it occurs, to ensure the response is appropriate. There are many cases of specific anticipated disruptions. Two examples are provided in 8.2 and 8.3.

8.2 Pandemic (global) and epidemic (regional)

The pandemic/epidemic plan should include procedures for continuing activities in a pandemic/epidemic event. It should consider a multi-phased model to respond to the progression of an outbreak.

To assist with the activation of pandemic/epidemic-related strategies, the following triggers should be considered:

- media coverage of potential pandemic/epidemic threats;
- evidence of pandemic/epidemic outbreak within the community or region;
- declaration by government health agency;
- potential for direct contact with the illness;
- evidence of pandemic/epidemic affecting the organization (e.g. increased absenteeism, supply chain interruptions).

Procedures should support the organization through a prolonged period of disruption and include:

- capability to redirect workload outside the affected region;
- capability to support increased work from home;
- processes to ensure a sanitized work location;
- increased monitoring of employee travel;
- contact tracing for employees in affected areas;
- provision of personal protective equipment;
- support to affected employees and their families.

Pandemic/epidemic plans should consider guidance and regulations from national and local authorities.

8.3 Cyber-attack

The cyber-attack plan should be aligned with the overall information security response strategies. The plan should contain procedures that:

- ensure that there are ICT access controls in place;
- identify the type, scope and impact of the cyber-attack;
- identify immediate actions to contain the attack;
- identify unique external communication requirements, such as law enforcement or regulatory bodies;
- respond to a ransomware request;
- respond to a data breach;
- address total loss of ICT services, data, and the network, for an extended period of time, including the reconstruction of lost data;
- activate external cyber security providers to assist during the attack;
- provide workarounds which do not depend upon availability of another application or the network.

9 Guidance on documenting plans

9.1 Clarity

A business continuity plan is a document intended to be used in high pressure, time limited situations. Plans are not manuals or reports and should not contain unnecessary information which is not relevant during a disruption. To reduce the need to refer to external sources, keep the plan self-contained as possible. Where possible, team members should be involved in developing and maintaining the plan, so its content is clear to them.

9.2 Clarity

The plan's content should be:

- clear and consistent in its choice of words and avoiding acronyms;
- explicit about defining what to do, when and by whom.

9.3 Completeness

The plan's content should:

- be based on chosen strategies – do not leave gaps in describing how to respond or recover, or how to operate differently until returning to normal business operations;
- suggest a number of options, where these exist, to enable a flexible response to the given situation;
- provide more detail written into a procedure to provide greater clarity and reduce misunderstanding. It should avoid excessive details.

10 Plan controls, storage and availability

Plans and procedures should be subject to the organization's document control practice. They should be:

- available and suitable for use, where and when needed – in particular when an incident occurs;
- adequately protected (e.g. from loss of confidentiality, improper use, improper access, improper modification or loss of integrity).

For the control of documented information, the organization should address the following activities, as applicable:

- distribution, access, retrieval and use;
- storage and preservation, including preservation of legibility;
- control of changes (e.g. version control);
- retention and disposition.

The organization should determine how business continuity plans and procedures will be stored and made accessible. Formats include:

- software purpose-built for business continuity (internal or hosted);
- general internal or cloud-based document sharing services;
- mobile file repositories;
- hard copy (pre-positioned, possibly in multiple locations, where the plans are likely to be used).

All team members should be responsible for ensuring they have access to a current version of the plan at all times.

11 Next steps after documenting business continuity plans and procedures

11.1 Awareness

The implementation of a new or significantly revised plan and procedures should be communicated to team members and affected personnel as part of an awareness programme. Some personnel can require detailed knowledge of their plan, whereas others just need to know that the plan exists or has changed. This communication can take the form of:

- e-mail;
- presentation;
- training session.

11.2 Exercising and testing

Business continuity plans are considered effective once validated. Exercising and testing is among the most important milestones of the BCMS as they build participant competency and create confidence in the capability of the teams and plans.

Every business continuity plan and procedure should be exercised and tested based upon management-endorsed objectives and success criteria. The organization should identify lessons learned and opportunities for improvement that can be used to improve business continuity plans and procedures.

NOTE Guidelines on exercises are given in ISO 22398.

12 Monitoring and reviewing business continuity plans and procedures

12.1 Performance review

The organization should monitor and review the performance of its business continuity plans. Reviews should include the following:

- assessing the performance of the plans and procedures;
- confirming the adequacy and performance of established business continuity strategies and solutions;
- identifying and addressing any instances of noncompliance with applicable legislation, statutory and regulatory requirements.

During the review, management should ensure that the continual improvement of each plan is actively pursued.

12.2 Maintenance

Business continuity plans and procedures need to be kept up to date with internal and external changes to the organization and its response and recovery strategies and solutions.

The organization should monitor the status of all of the organization's plans and take action if plans are not being appropriately maintained. This can be conducted by the business continuity manager.

Circumstances that can require modifications to plans include:

- issues identified during an exercise or an incident;
- organizational changes;
- changes to products or services or the way they are delivered;
- personnel or supplier changes;
- changes in standards, regulations or internal business procedures.

The organization should implement procedures for maintaining business continuity plans to ensure documentation remains current, complete and fit for purpose. See Annex A.

12.3 Management review

Formal management reviews should include an evaluation of the plan documentation and maintenance process, including the existence of current plans that address the scope of the BCMS.

In some geographies and sectors, local laws and requirements can mandate top management's formal, documented endorsement of business continuity plans and procedures.

A review of the effectiveness of business continuity plans and procedures should be performed following a disruption, regardless of the outcome of the event.

Annex A
(informative)

Procedures for maintenance of a business continuity capability

A.1 General

To ensure the effectiveness of business continuity plans and procedures at time of disruption, it is necessary that supporting capabilities are established and maintained during normal operations. These capabilities require their own procedures.

A.2 Skills cross-training

Cross-training is commonly used to enable activities to continue if the disruption results in a shortage of staff resources. The time taken after an incident for this substitution to be effective is a significant factor in the choice of solution.

The requirement for, and process of, the transfer of knowledge between individuals to enable them to be a viable substitute for one another can need to be documented and the results recorded. This can be the responsibility of the department or business unit that requires the skill, or by the human resources department which can centrally maintain such information. When an individual moves from one job to another, the procedure should include a mechanism for the substitution to be reviewed.

The organization can also choose to record the skills and experience acquired by individuals in previous roles which can be relevant during an incident where these are permanently or temporarily lost. Contact details of staff who are retiring or moving to other organizations can be recorded so they can be tempted to return if this would assist recovery. There needs to be a process to ensure this information is captured and maintained in a useful form.

The transfer of knowledge to a substitute can be achieved by:

— on-the-job training or mentoring;

— training courses;

— documentation of processes that can be used to train replacement staff.

The knowledge and skills gained need to be refreshed by regular substitution at the frequency required to ensure they remain current and quickly reflect any changes.

A.3 Outsourcing

Outsourcing functions on a temporary basis can be a suitable solution during an incident involving a shortage of staff.

The transfer of work to an outsourcer can require the following, depending on the urgency of the activity the outsourcer will undertake:

— a contract to enable the work to be undertaken to an agreed standard and with the appropriate safeguards in place (intellectual property, confidentiality, etc.);

— a procedure to enable the work to be handed over to the outsourcer in a form that they can quickly take it on and complete, which can include:

  — a checklist of the required information;