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)

## COPYRIGHT PROTECTED DOCUMENT

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

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

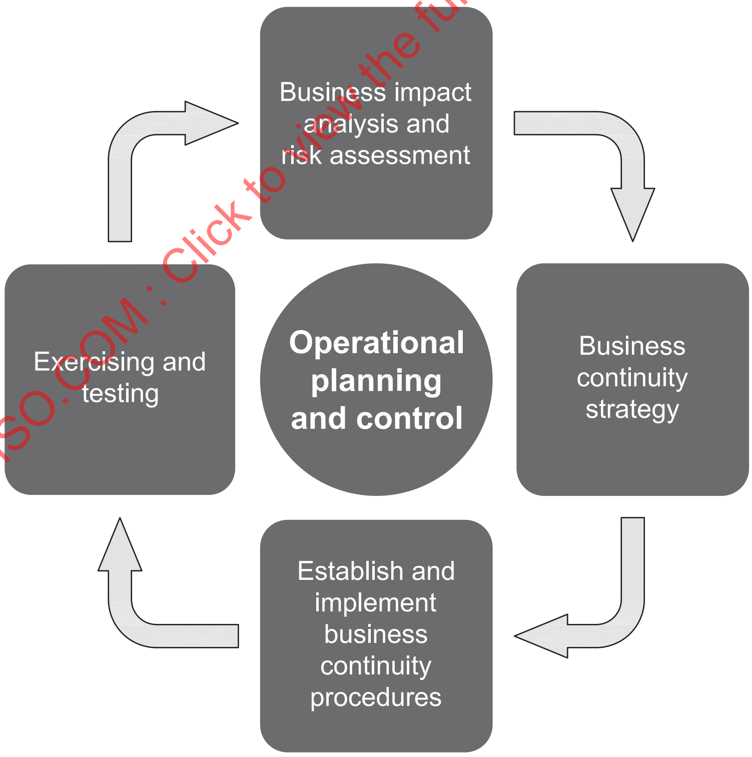
This document provides detailed guidelines for business continuity strategy determination and selection. It is consistent with the requirements of ISO 22301. It is applicable to the performance of any business continuity strategy determination and selection effort, whether part of a business continuity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


Business impact analysis and risk assessment
Business continuity strategy
Establish and implement business continuity procedures
Exercising and testing
Operational planning and control

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.

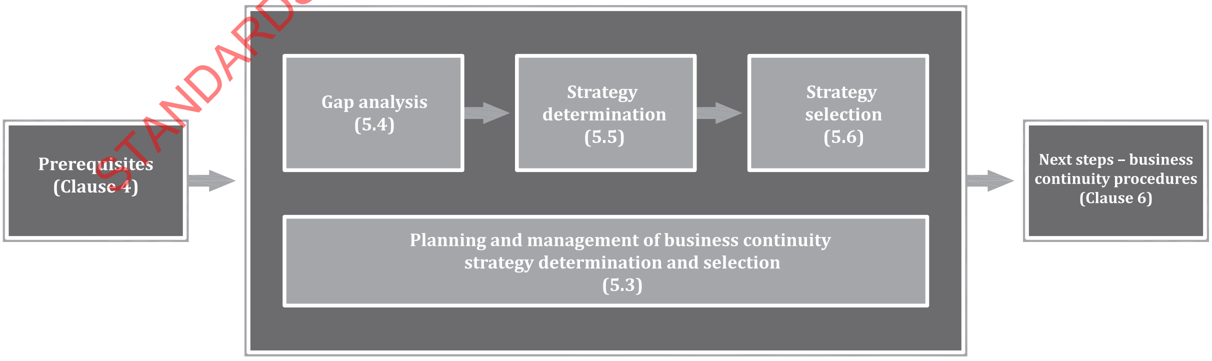

Prerequisites
(Clause 4)
Gap analysis
(5.4)
Strategy determination
(5.5)
Strategy selection
(5.6)
Planning and management of business continuity strategy determination and selection
(5.3)
Next steps – business continuity procedures
(Clause 6)

**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.

### 5.3.2 Initial strategy design considerations

An organization undertaking a strategy determination and selection process for the first time should plan time to:

- create awareness;
- negotiate business continuity requirements;
- perform gap analysis;
- identify available strategy options;
- perform cost/benefit analysis.

### 5.3.3 Strategy monitoring and continual improvement

Once an organization selects and implements business continuity strategies, the organization should monitor performance to ensure that strategies continue to meet business continuity requirements. If strategies do not meet requirements, the organization should perform the strategy determination and selection process again, with the aim of adjusting strategy capabilities to meet business continuity requirements.

Additionally, after the organization performs the business impact analysis, the organization should ensure those strategies that meet business continuity requirements are the best possible option and that no better options exist. As time goes on, the organization may find strategies that:

- are more suitable or cost effective;
- require less resources to execute;
- result in a faster or easier recovery;
- are better able to meet the needs of the organization.

## 5.4 Business continuity strategy gap analysis

Following the business impact analysis and risk assessment, the organization should perform a gap analysis comparing its approved business continuity requirements (time and capability) to current-state response and recovery capabilities.

The organization should confirm current capabilities meet business continuity requirements by performing the following actions.

a) Sequencing the output of the business impact analysis by RTO for products/services, processes, activities and resources.

b) Summarizing the performance of current-state business continuity strategies, including the ability to meet time and capability expectations.

c) Comparing the performance of business continuity strategies to business continuity requirements.

   1) Business continuity strategy performance may be determined based on results from disruptive incidents and exercises, and possibly based on service level agreements or contractual obligations if a third party is enabling the strategy.

d) Determining where current-state response and recovery performance fall short (meaning downtime is greater and/or capability is less than required), which will indicate gaps in meeting interested party expectations.

e) Determining where current-state response and recovery performance is greater (meaning downtime is shorter and/or capability is less than required), which will indicate an over-investment in meeting interested party expectations.

f) Presenting and seeking management acknowledgement of gaps and over-investment prior to determining business continuity strategies. Where gaps exist, management should request business continuity strategies be investigated based on the anticipated impact to the organization. In the instance of over-investment, management may request alternate business continuity strategies be investigated.

g) Prioritizing the implementation of business continuity strategies based on management acknowledgement of gaps or over-investment.

## 5.5 Determining business continuity strategies

### 5.5.1 Overview

The organization should determine which strategy options are available to the organization to close gaps and reduce over-investment and, where possible, should provide additional benefits in a business-as-usual situation.

The results of strategy determination at the product, service, process or activity levels may mean there is no need to progress to strategies for resources. For example, if the strategy is to outsource the delivery of a service to a third-party organization, then the recovery of the associated capability may be managed by that third-party arrangement while the organization focuses on restoring the affected resources (e.g. a facility rebuild).

### 5.5.2 Business continuity strategy consolidation

If a specific resource (e.g. a software system) is required by many activities, then the organization may develop a consolidated business continuity strategy to meet the business continuity requirements of the activity with the highest priority (and the shortest RTO).

Similarly, if many activities are to adopt the same business continuity strategy (e.g. ten activities on floor 7 of building A are to relocate to floor 3 of building B), then the organization may develop a consolidated business continuity strategy rather than replicate the strategy multiple times.

There may also be a need to select different strategies over time after an incident. For example, people may be able to work from home for a few days after an incident but the organization may then need to provide an alternative work area.

### 5.5.3 Business continuity strategy categories

Organizations may use a framework that categorizes or groups business continuity strategies for recovering resources, based on defined RTO ranges, which links appropriate strategies to activity and resource RTOs. The categories are only a naming convention used to organize strategy options used by an organization in conversation. Categorization examples include:

- Category A, B, C and D;
- Platinum, Gold, Silver and Bronze;
- Tier 1, 2, 3 and 4.

If categorization is used by an organization, it is important to avoid category names that could invoke an emotional response by the business continuity programme interested party, which then could lead to inappropriate strategy selection. For example, using “critical” as a category name.

If categorization is used, the organization should nominate a specific timeframe for each category.

Figure 3 gives an example of a conceptual framework addressing strategy categories over time. This framework aligns to the key principles of business continuity, urgency, meaning continuity and restoration requirements based on how urgent each product, service, process, activity and resource is to interested parties. Shorter RTOs (Category A) require capabilities and arrangements that are significantly more complex, detailed and expensive compared with those that can tolerate a longer RTO (Category D).

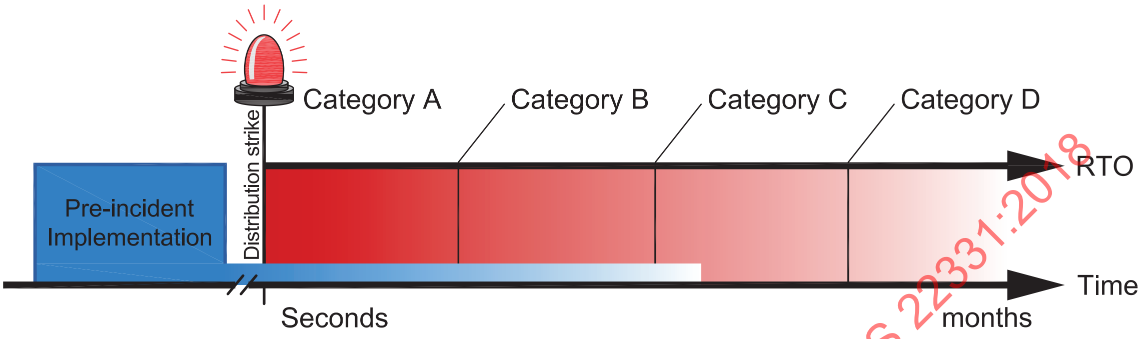


**Figure 3 — Strategy categories over time**

The organization should determine the number of categories and the period of coverage each category will span on a timeline. Categories will overlap, i.e. a strategy that satisfies the time requirement of Category A will also satisfy those of Categories B, C and D. Those of Category B will also satisfy C and D, and so on.

### 5.5.4 Business continuity strategy types for activities and resources

The following business continuity strategy category framework can be applied to activities and resources.

The organization should, as a prerequisite for determining viable strategy options, identify considerations that need to be addressed for the strategy to be feasible. The tables and information in the following clauses provide examples that may be a useful prompt and starting point.

The objective of the strategies summarized in Tables 1 to 8 is to ensure each activity or resource will continue, and that the re-provision, repair, replacement or delivery of alternate resources is achieved, in accordance with the approved business continuity requirements of the specific activity they support. Each table provides examples of strategy options that are categorized by the approximate minimum time in which they can be operational after the onset of a disruptive incident and include some prerequisites for consideration during pre-incident planning.

**Table 1 — People**

| Effective minimum recovery time | Examples of strategy options | Prerequisites |
|---|---|---|
| Within an hour | Other staff at same location with required skills/capability take over | — Cross-train staff working at same location<br>— Document business-as-usual business processes |
| | Staff at non-affected location with the required skills/capability take over as a result of the activity transferring to a non-affected location | — Cross-train staff working at an alternate location<br>— Document business-as-usual business processes |
| | Succession planning for key roles | — Nomination and training of replacements |
| | Alternate delegated authorities are available | — Nominate and bestow delegated authority to nominated managers |
| Within hours | Confirm other staff with the required skills/capability are on site and can take over | — Cross-train staff working at different locations/sites/regions<br>— Geographically separate staff with the same skills |
| | Transfer roles to contracted suppliers or partners | — Resources with the required skills supplied by an external provider/supplier are on site and can take over<br>— Set-up/prepare the process to transfer (or outsource) the activity to an external party or supplier |
| | Engage external people with the required skills | — Identify external suppliers able to deliver the required skills set |
| Within days | Nominate available staff on-site from activities that can tolerate downtime and provide training before transitioning work | — Develop training material for each skill set and deliver the training to nominated staff |
| | Nominate staff at non-affected locations from activities that can tolerate downtime and provide training before transitioning work | — Develop training material for each skill set and deliver the training to nominated staff<br>— Develop staff selection criteria |
| Within a week | Contact former employees and engage on short-term contracts | — Maintain lists of former employees with the necessary skills |
| | Search and engage temporary/contract staff via external agency(ies) | — Develop training material for each skill set and deliver the training to nominated staff when they arrive on-site |
| Within weeks/months | Recruit replacement staff from the market via external agencies | None |
| | Recruit replacement staff from competitors via external agencies | None |
| NOTE For additional information, see ISO/TS 22330. | | |

Table 2 — Information and data

| Effective minimum recovery time | Examples of strategy options | Prerequisites |
|---|---|---|
| Within an hour | Data availability from online replication | — Establish an off-site replicated data storage facility or contract a third-party service provider |
| | Paper-based information is available from online storage media | — Establish a process and facility to scan paper-based documents as processed during business-as-usual and store data off-site |
| Within days | Data is restored from remote storage | — Establish or contract an off-site data storage facility (data or document storage |
| | Request originator of documents to send a copy upon request | — Maintain a register of document originators with contact details and an approved method/channel for transmitting documents |
| | Data is rekeyed from source documentation | — Determine the location/owner of source documentation and establish an agreement for the provision of the required information |
| Within weeks | Identify a processor to source original documentation and rekey the information into the system | — Determine resource levels and facilities required to rekey information<br>— Consider insurance cover for this capability |

With respect to information and data, additional considerations include:

- all external environments, including third-party service providers and personnel working from home, should satisfy the organization’s information security management policies, including:
  - required levels of confidentiality, integrity, accountability and currency of each data category to be stored/accessed off-site;
  - required currency of information;
  - logical and physical access control;
  - data and information transport;
  - appropriate destruction of confidential information and deletion of data;
  - sovereignty, including where the data is physically stored.

Table 3 — Buildings, work environment and associated utilities

| Effective minimum recovery time | Examples of strategy options | Prerequisites |
|---|---|---|
| Within an hour | Split the activity’s work across multiple locations | — Run the activity at other location(s) at all times |
| | Have the capability and skills to transfer the activity to another location | — Practise the transfer of work regularly to maintain capability |
| | Prepare and activate on-site utility replacement technology (e.g. on-site generator, solar) | — Install self-gen or co-gen capabilities (e.g. on-site power generator) |

**Table 3** *(continued)*

| Effective minimum recovery time | Examples of strategy options | Prerequisites |
|---|---|---|
| Within a day | Displace lower priority activities (those with higher RTOs) with personnel from high priority activities (those with lower RTOs) within the site | — Agree displacement priorities and location within the site with the departments affected |
| | Reconfigure buildings or work environment (e.g. meeting rooms, cafeteria) within the location | — Do preparatory work or make plans to facilitate this |
| Within days | Displace lower priority activities (those with higher RTOs) with personnel from high priority activities (those with lower RTOs) at another location | — Document prioritized preferences for alternate work areas and agree them with affected departments<br>— Consider staff issues on relocation<br>— Identify which additional resources are required to enable the activity to restart at the alternate location |
| | Reconfigure buildings or work environment (e.g. meeting rooms, cafeteria) at an off-site location/site/region for relocation or transfer then activate the facility | — Document prioritized preferences for off-site alternate work areas<br>— Consider staff issues on relocation<br>— Identify which additional resources are required to enable the activity to restart |
| | Relocate activity to a partner or a commercial work area recovery provider | — Establish an agreement with another organization or contract with a third-party commercial service work area recovery provider |
| | Relocate the activity to staff's own residences | — Inspect the work area/space of each nominated home to confirm compliance with appropriate health and safety and security policies<br>— Confirm insurance coverage and liability |
| | Contract a supply of temporary utility feeds | — Contract to supply power, water, heating, lighting to a service level agreement (SLA) |
| Within weeks | Find an alternate work area | — Maintain a register of commercial offices, estate agencies or providers |
| | Repurpose existing buildings to provide required work space | — Draw up plans prior to an incident |
| | Ad-hoc supply of temporary utility feeds | — Maintain a register of portable utility providers |
| More than weeks | Rebuild and refurbish the work areas | — Consider, in advance, the opportunities that rebuild or refurbishment may offer |
| | Re-install utility feeds | — None |

**Table 4 — Facilities, equipment and consumables**

| Effective minimum recovery time | Examples of strategy options | Prerequisites |
|---|---|---|
| Within an hour | Split capacity at the location across two or more similar items of equipment | — Maintain spare capacity for each operation |
| | Immediately initiate a work-around for the loss of the equipment or consumable | — Document and prepare any additional resources required by workarounds<br>— Rehearse workarounds regularly |
| | Draw from an on-site stockpile of consumables | — Maintain an adequate on-site supply of consumables with due consideration to:<br>— the period of time for which the stockpile will suffice;<br>— the lead time on new deliveries from the supplier. |
| Within days | Spare equipment stored on-site | — Have a plan to install and commission spare equipment to meet the required timescales |
| | Prepare and then initiate a work-around for the loss of the equipment or consumable | — Identify work around options and any resources required |
| | Undertake a salvage activity to retrieve equipment and consumables from the impacted location | — Research contract/subscription to a specialist asset restoration company or consult salvage specialists for advice in advance |
| | Draw from an off-site stock-pile of consumables | — Maintain an adequate supply of consumables at another site/region with due consideration to:<br>— the period of time for which the stockpile will suffice;<br>— the time to deliver the item from the off-site location. |
| Within days or weeks (depending on the specific equipment) | Relocate and commission spare equipment installed or stored off-site | — Ensure that spare equipment is stored off-site and can be relocated and commissioned in the time available |
| | Order/lease or rent replacement equipment from a supplier | — Document a plan for installation |
| | Repair damaged equipment | — Contract a maintenance agreement with a supplier that covers incident damage |
| | Order replacement consumables from a supplier | — Consider the lead time of delivery |
| Within months | Purchase new equipment | — Maintain knowledge of available equipment, specification changes and vendor contact information |

**Table 5 — Information and communication technology (ICT) systems**

| Effective minimum recovery time | Examples of strategy options | Prerequisites |
|---|---|---|
| Within one hour | Application system is replicated and live on another platform, which may be referred to as "hot" or "active/active". Data across the two platforms, network drives and/or storage arrays are synchronized in real time. | — Establish replicated systems across two or more well-separated locations:<br>— owned by the organization; or<br>— via service level agreement and contract with a third-party hosting service provider<br>— Identify the timescales of reconfiguration (if any) if one location is lost and test periodically |
| | Data communications links and communication devices (e.g. routers, switches, modems) are replicated<br>Data communication paths have divergent routing | — Implement replicated divergent routing of LAN and WAN links<br>— Install redundancy in communication devices |
| | Automatic or contracted redirection of voice communication to other locations | — Contract for managed telephony services, which may be used for business-as-usual and reconfigured during an incident |
| Within days | The application system is preloaded on another platform and requires maintenance/updates to match the production version<br>Application data requires restoration from the most recent back-up or transaction log, which is typically referred to as "warm standby"<br>Hosting of the service either by the organization in another data centre or by a third-party ICT service provider | — Establish a copy of the application system on an alternate platform<br>— Establish a process that transfers data backups to a location accessible to the location of the alternate platform<br>— Perform regular testing of the data restoration process, especially after system upgrades |
| | Replacement of desktop equipment through a contracted service; equipment can be pre-configured by the supplier before delivery | — Ensure the required desktop configurations are held by the supplier |
| | Data communications links are replicated<br>Communication devices (e.g. routers, switches, modems) are replaced by spare devices stored on- or off-site<br>Install wireless networks to cover new work areas | — Maintain a pool of spare compatible network and communication devices |

**Table 5** *(continued)*

| Effective minimum recovery time | Examples of strategy options | Prerequisites |
|---|---|---|
| Within a week | Platform of suitable capacity is identified and used to establish a contingency platform for the restoration of the system and data from back-ups | — Maintain a list of target platforms (i.e. servers, server farms, etc.) suitable for reinstating specific application systems |
| | Communication devices (e.g. routers, switches, modems) are replaced by purchasing new devices from suppliers | — Maintain a list of spare compatible communication devices and potential sources |
| Within weeks | Replacement equipment is purchased, installed and commissioned, followed by a process where the system is restored from back-ups media, then tested and finally becomes the production system<br>This may be required as the second step of relocation after temporary use of a third-party recovery site | — List the equipment required and the vendor details<br>— Keep documentation of the current configurations of all equipment and any upgrade path required to new equipment |

**Table 6 — Transportation**

| Effective minimum recovery time | Examples of strategy options | Prerequisites |
|---|---|---|
| Within hours | Additional capacity provided by a logistics company already providing that service to the organization | — Source transport in advance from two or more companies<br>— Ensure a contract is in place to provide additional capacity on a stand-by basis |
| | Staff transport to home or another location by taxi or bus | — Ensure a contract is in place with a stand-by transport provider |
| | Contracted capabilities to deliver using several modes of transport or via different media | — Document any changes required to change the mode/media, e.g. repackaging |
| | Request the customer arrange transport | — Consider establishing a prior agreement with the customer |
| Within days | Post-incident contract with an alternative logistics supplier | — None |

**Table 7 — Finance**

| Effective minimum recovery time | Examples of strategy options | Prerequisites |
|---|---|---|
| Within hours | Make cash available or ensure appropriate lines of credit | — Ensure cash reserves or credit vehicles are at an appropriate level |
| | Purchase goods or services via corporate credit cards | — Maintain a register of corporate credit card holders and their credit limit |
| | Increase delegated purchasing authority limits to nominated staff | — Nominate corporate credit card holders to have their delegated purchasing authority limit increased and the amount of the increase |
| | Seek financial support from parent company | — Consider agreeing terms in advance |
| | Establish/increase the line of credit with suppliers and place orders for goods or services | — None |
| Within a day | Cancel term deposits and retrieve funds | — Ensure term deposit terms and conditions allow for early cancellation or withdrawal |
| Within weeks | Rely on cash from insurance payments<br>Policies could be held for:<br>— business interruption/ increased cost of working<br>— damage (all-risks)<br>— insurance for costs incurred by the organization in the replacement of key staff such as executives | — Ensure appropriate insurance cover |
| | Liquidate assets | — None |

**Table 8 — Partners and suppliers**

| Effective minimum recovery time | Examples of strategy options | Prerequisites |
|---|---|---|
| Within a day | Supplier disruption: ensure alternative sources of supply are available | — Retain a stockpile of materials<br>— Source materials from two or more suppliers |
| Within a day | Disruption to product or service delivery: pass responsibility (but not accountability) for product or service delivery to a partner organization | — Establish a contractual arrangement with a partner that:<br>— operates from a location sufficiently far from the organization's location;<br>— does not rely on the same suppliers;<br>— maintains and exercises its own business continuity capabilities. |
| Within days | Engage previous suppliers that are still able to provide the product or service | — Maintain a register of ex-suppliers |
| | Engage pre-qualified suppliers that can provide the products or services but retain responsibility and control | — Maintain a register of pre-qualified suppliers |
| Within weeks | Research and engage alternate partners and supplies when needed | — None |
| NOTE For additional information, see ISO/TS 22318. | | |

## 5.6 Selecting business continuity strategies

### 5.6.1 General

The selection of business continuity strategies involves comparing potential solutions to business continuity requirements and choosing, on merit, those with the best fit for the organization (short- and long-term), considering implementation and maintenance costs. The organization should use an appropriate method to compare options, taking into account their costs and possible benefits and making clear the assumptions on which benefits have been calculated. Some measures will provide day-to-day benefits for business operations, which should be taken into account.

At this stage in the process, the costs associated with implementing the business continuity strategy may result in revisiting business continuity requirements for the affected activities and resources.

### 5.6.2 Strategies for protecting prioritized activities and resources

Information from the risk assessment should be used during the cost-benefit analysis to assess the value to the organization of selecting protection options. Protection options seek to decrease likelihood of disruption to the organization's ability to deliver products or services, or enable the organization's activities and resources to be recoverable. It is unlikely that prioritized activities and their dependencies can ever be fully protected and in many cases the costs of protection can be prohibitive.

Key questions and considerations during strategy selection for protecting prioritized activities and resources include the following.

- Are capabilities available that can realistically decrease the likelihood of a disruption to the activities and resources that deliver in-scope products and services?
- Has the organization identified infrastructure single points of failure that, if down, would:
  - disrupt the organization's ability to deliver products and services?

  - benefit from redundancy or diversity to decrease the likelihood of disruption (examples include electricity, fuel, water, voice and data communication lines, and air handling)?

- Should the organization seek to implement a capability (e.g. a backup power generator) or create a diverse environment that is less likely to experience a disruption (e.g. split capacity with geographic separation)?
- Are there resources that would be difficult to source or recover due to lead times or obsolescence that may require a safety stock or advanced preparations to enable timely sourcing?
- Does the protection measure provide any day-to-day organizational benefit?

For additional information on methods to select protective measures, see IEC 31010.

### 5.6.3 Strategies for resuming and recovering prioritized activities and resources

It is likely that there will be a range of options for stabilizing, continuing, resuming and recovering prioritized activities to address different disruption scenarios. No two organizations are the same, so there are no rules for choosing the best options. In general, strategy options that address multiple scenarios and address the multiple loss of dependencies are likely to be preferable, particularly if their cost of implementation is also low. Preference should also be given to strategies that can be shown to be effective during normal business. When selecting business continuity strategies, organizations should first consider two strategic questions regarding the method of recovery.

- Should the organization transfer product/service delivery to a third-party's responsibility following the onset of a disruptive incident (with the organization retaining accountability for product/service delivery)?
- Should the organization continue product/service delivery internally?

Following this decision regarding product/service delivery and, if continuing to retain the responsibility for product/service delivery internally, the organization should consider additional questions to enable business continuity strategy selection for recovering prioritized activities and resources. (In considering these questions, the organization may choose to return to the strategic questions above.)

- Is it necessary to use internal resources for the business continuity strategy or is it feasible to recover via a third-party service provider? (Key considerations include security, performance and the guaranteed availability of recovery resources.)
- Does the performance of the business continuity capability option appear to align to business continuity requirements?
- Does the initial implementation and long-term maintenance costs of the business continuity capability option align to the availability of funding?
- Does the organization have the skills and experiences to effectively use the business continuity capability option?
- Is the business continuity capability option a sufficient distance from the primary resource while, at the same time, is it close enough to be used in a practical manner following the onset of a disruptive incident?
- When needed, is there sufficient time to enable the business continuity capability option to meet the RTO?
- Does the business continuity capability option provide any day-to-day organizational benefit?
- Does the use of the business continuity capability option meet all internal and external obligations, including regulatory, contractual and statutory obligations?

— Is the business continuity capability option flexible enough to address any anticipated or possible changes in the business environment (such as technology) and business continuity requirements in general?

Regarding resource-specific business continuity strategy options, the organization should consider the questions listed in Table 9 when selecting the most appropriate strategy.

**Table 9 — Selection of appropriate strategy**

| Resource strategy type | Selection questions and considerations |
|---|---|
| People | — Are there personnel at other locations or in other parts of the organization that can perform the prioritized activities?<br>— Are third-party sources of personnel guaranteed to be available and will they be effective within the RTO?<br>— Are roles and responsibilities effectively documented to enable non-qualified personnel to become competent within the RTO?<br>— Consideration should be given to succession planning for management and staff personnel.<br>— Consider the implications of shift working. |
| Information and data | — Are there other sources of the information to enable recovery (electronically or in a physical form)?<br>— Can the information be accurately and completely recreated in a timely manner and, if so, are internal or third-party personnel available to perform the work?<br>— Are there technical considerations or limitations that dictate the backup or replication method? |
| Work environments and utilities | — Can the activity be performed effectively in more than one location not subject to the same threats?<br>— Can some less urgent work be paused to enable more urgent work to be performed using internal work space?<br>— Are mutual aid agreements possible whereby a third-party could provide work space to enable recovery? If so, are guarantees in place?<br>— Are staff equipped to work from home in a manner that enables a minimum level of performance and meets safety and security obligations?<br>— Is it realistic to assume that adequate work space could be sourced and implemented under the RTO?<br>— Is the alternate work space served by the same utilities as the primary work space?<br>— Does the alternate work space have adequate parking and are there suitable entrances (for equipment placement and special needs personnel?<br>— Is the alternate work space realistically subject to the same climatic, environmental quality or geologic threats?<br>— Can the organization source the disrupted utility from an alternate source following the onset of the disruptive incident? |