BS 25777:2008

BSI British Standards

Information and communications technology continuity management — Code of practice

raising standards worldwide™

BSI British Standards

Publishing and copyright information

ISBN 978 0 580 56239 6

ICS 35.020

The following BSI references relate to the work on this standard:
Committee reference BCM/1
Draft for comment 08/30166965 DC

Publication history

First published November 2008

Amendments issued since publication

Amd. No.	Date	Text affected

Contents

Summary of pages
This document comprises a front cover, an inside front cover, pages i to ii, pages 1 to 36, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI and came into effect on 30 November 2008. It was prepared by BSI panel BCM/1/-/1, under the authority of Technical Committee BCM/1, *Business continuity management*. A list of organizations represented on this committee can be obtained on request to its secretary.

Use of this document

As a code of practice, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this British Standard is expected to be able to justify any course of action that deviates from its recommendations.

Presentational conventions

The word "should" is used to express the recommendations of this standard, with which the user has to comply in order to comply with the standard. The word "may" is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word "can" is used to express possibility, e.g. a consequence of an action or an event.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

Introduction

ICT continuity management and its relationship with business continuity management

In most organizations, the processes that deliver products and services depend on information and communication technology (ICT). Disruption to ICT can therefore constitute a strategic risk, damaging the organization's ability to operate and undermining its reputation. The consequences of a disruptive incident vary and can be far-reaching, and might not be immediately obvious at the time.

ICT continuity management supports the overall business continuity management (BCM) process of an organization. BCM seeks to ensure that the organization's processes are protected from disruption and that the organization is able to respond positively and effectively when disruption occurs. The organization sets out its BCM priorities, and it is within this context that ICT continuity management activities take place. ICT continuity management ensures that the required information and communications technology and services[1)] are resilient and can be recovered to predetermined levels within timescales required by and agreed with the top management. Thus, effective BCM depends on ICT continuity management to ensure that the organization can meet its objectives at all times, particularly during times of disruption. To be successful, both BCM and ICT continuity management have to become embedded within the organization's culture (see Figure 1).

BCM and ICT continuity management form an important element of effective management, sound governance and organizational prudence. Top management is responsible for maintaining the ability of the organization to continue to function in the face of disruption. Many organizations also have a statutory or regulatory duty to maintain effective risk-based controls, including BCM.

ICT continuity management and organizational strategy

ICT continuity management is integral to both ICT strategy and ICT service management, which align to organizational strategy. It is the element of ICT strategy and service management that enables an organization to continue to meet its goals and deliver its products and services when adverse conditions occur.

Benefits of effective ICT continuity management

All activity is susceptible to disruption from internal and external events, such as technology failure, fire, flood, utility failure, illness and malicious attack. ICT continuity management provides resilience to prevent ICT disruptions and to recover when disruptions occur.

---

1) Including supporting IT and telecommunications infrastructure (networks and their components), computer hardware, applications, ICT service delivery and support functions (e.g. service desk).

The benefits of effective ICT continuity are that the organization:

- understands the threats to, and vulnerabilities of, ICT services;
- identifies the potential impacts of disruption to ICT services;
- encourages improved collaboration between its business managers and its ICT service providers (internal and external);
- develops and enhances competence in its ICT staff by demonstrating credible responses through exercising ICT continuity plans and testing ICT continuity arrangements;
- provides assurance to top management that it can depend upon predetermined levels of ICT services and receive adequate support and communications in the event of a disruption;
- provides additional confidence in the business continuity strategy through linking investment in ICT solutions to business needs and ensuring that ICT services are protected at an appropriate level given their importance to the organization;
- has ICT services that are cost-effective and not under- or over-invested through an understanding of:
    - the level of its dependence on those ICT services; and
    - the nature, location, interdependence and usage of components that make up the ICT services;
- can enhance its reputation for prudence and efficiency;
- potentially gains competitive advantage through the demonstrated ability to deliver business continuity and maintain product and service delivery in times of disruption; and
- understands and documents stakeholders' expectations and their relationships with, and use of, ICT services.

ICT continuity is more easily achieved and is likely to be less costly when designed and built into ICT services from their inception as part of ICT strategy. This ensures that ICT services are better built, better understood, cheaper and easier to maintain. Retrofitting ICT continuity can be complex, disruptive and expensive. The content of an ICT continuity programme will be influenced by the organization's risk appetite.

Focus of ICT continuity management

ICT continuity management focuses not only on the likelihood and impact of disruptive incidents, but also on the ability of the organization to detect and respond to the occurrences of such incidents. This requires the organization to monitor its ICT services to ensure that:

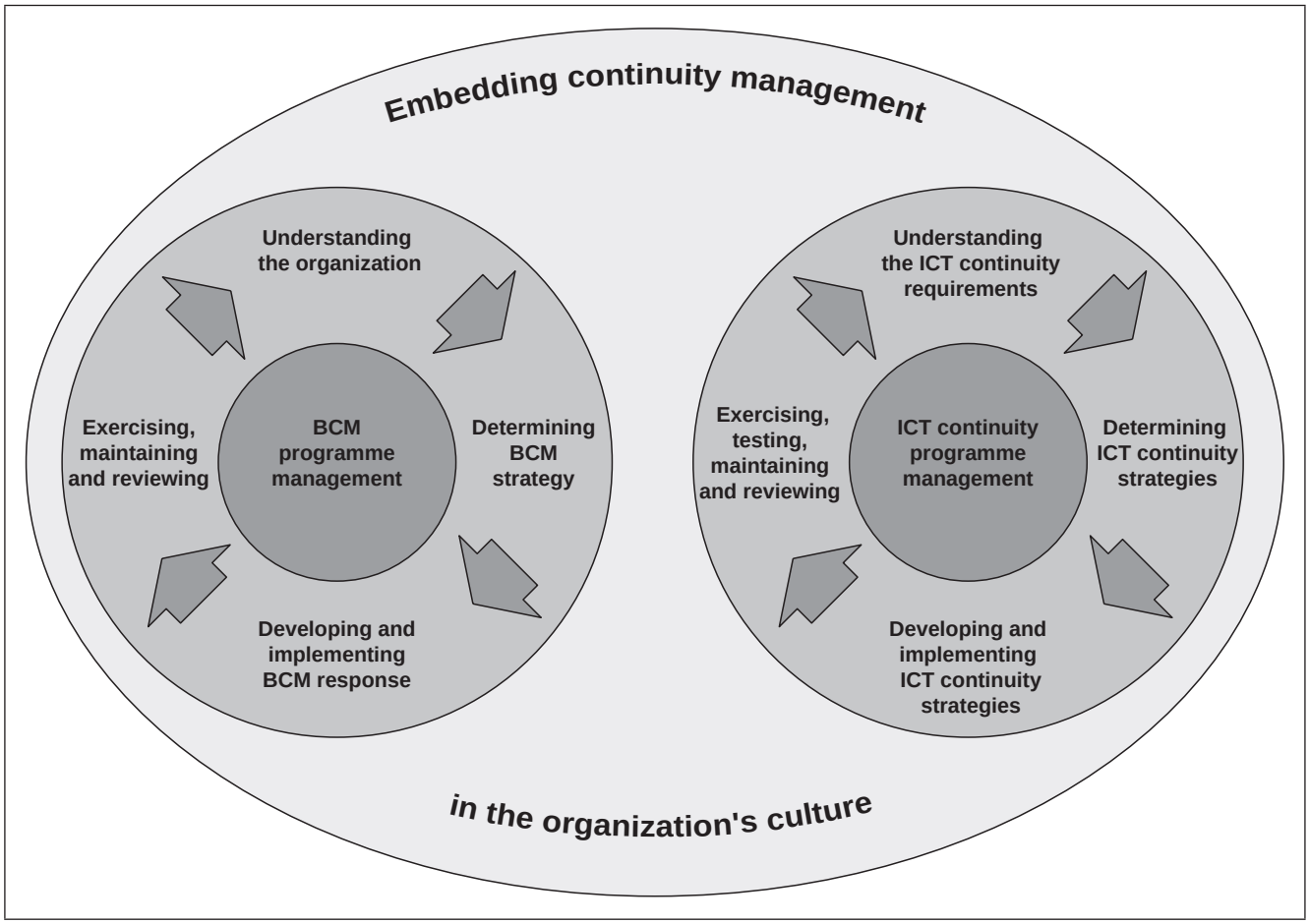
- they are resilient and recoverable at the appropriate level;
- any unexpected event within a service is detected, addressed and investigated in a timely manner;
- the dependencies between ICT services and external factors[2)] are known and used in assessing risk and the impact of change; and

2) Such as vendors, customers, supply chain partners and outsourced service providers.

- dependencies on the technical components[3)] are known and used in assessing risk and the impact of change.

ICT continuity management processes and solutions are also intended to ensure that legal obligations (such as the protection of personal and otherwise sensitive data) are not breached.

Figure 1 **Relationship between ICT continuity management and business continuity management**



Principles of ICT continuity management

ICT continuity is based around six key principles:

a) **Protect:** Protecting the ICT environment from incidents, failures and disruptions by improving the resilience of ICT services is critical to maintaining the desired levels of service availability for an organization.

b) **Detect:** Detecting incidents at the earliest opportunity will minimize the impact to services, reduce the recovery effort, and preserve the quality of service.

c) **React:** Reacting to an incident in the most appropriate manner will lead to a more efficient recovery and minimize any downtime. Reacting poorly can result in a minor incident escalating into something more serious.

3) Examples are given in "Elements of an ICT service".

d) **Recover:** Identifying and implementing the appropriate recovery strategy will ensure the timely resumption of services and maintain the integrity of data. Understanding the recovery priorities allows the most critical services to be reinstated first. Services of a less critical nature may be reinstated at a later time or, in some circumstances, not at all.

e) **Operate:** Running in ICT disaster recovery mode until return to normal is possible. This might require some time and necessitate "scaling up" ICT disaster recovery operations to support increasing business volumes needing to be serviced over time.

f) **Return:** Devising a strategy for every ICT continuity plan that allows an organization to migrate back from ICT disaster recovery mode to a position where it can support normal business.

Elements of an ICT service

The key elements of an ICT service can be summarized as follows (see also Annex A).

a) People: the specialists (including their deputies) with appropriate deputies and knowledge.

b) Premises: the physical environment in which ICT resources are located.

c) Technology:

   1) the racking, servers, storage arrays, tape devices, other hardware and other permanent fixtures;

   2) network, including data connectivity and voice services, including switches and routers;

   3) software, including operating system software and application software, links or interfaces between applications and batch processing routines.

d) Data: application data, voice data and other types of data.

e) Processes: including supporting documentation to describe the configuration of ICT resources and enable the effective operation, recovery and maintenance of ICT services.

f) Suppliers: other components of the end-to-end services[4)] where ICT service provision is dependent upon an external service provider or another organization within the supply chain, e.g. a financial market data provider, telecoms carrier or internet service provider.

---

4) From the computer room (which might be a data centre and communication room) through to the user desktop or other delivery channel, such as web application, mobile phones, point of sale and automated teller machines (ATMs or cash points).

1 Scope

This British Standard gives recommendations for information and communications technology (ICT) continuity management within the framework of business continuity management provided by BS 25999.

2 Terms and definitions

For the purposes of this British Standard, the following terms and definitions apply.

2.1 activity
process or set of processes undertaken by an organization (or on its behalf) that produces or supports one or more products or services

NOTE Examples of such processes include accounts, call centre, IT, manufacture, distribution.

2.2 business continuity (BC)
strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level

2.3 business continuity management (BCM)
holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities

NOTE Business continuity management involves managing the recovery or continuation of business activities in the event of a business disruption, and management of the overall programme through training, exercises and reviews, to ensure the business continuity plan(s) stays current and up-to-date.

2.4 business continuity management lifecycle
series of business continuity activities which collectively cover all aspects and phases of the business continuity management programme

NOTE The business continuity management lifecycle is illustrated in Figure 1.

2.5 business continuity plan (BCP)
documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical activities at an acceptable predefined level

2.6 business continuity management programme
ongoing management and governance process supported by top management and appropriately resourced to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products and services through training, exercising, maintenance and review

2.7 business continuity strategy
approach by an organization that will ensure its recovery and continuity in the face of a disaster or other major incident or business disruption

2.8 business impact analysis
process of analysing business functions and the effect that a business disruption might have upon them

2.9 consequence
outcome of an incident that will have an impact on an organization's objectives

NOTE 1 There can be a range of consequences from one incident.

NOTE 2 A consequence can be certain or uncertain and can have positive or negative impact on objectives.

2.10 critical activities
those activities which have to be performed in order to deliver the key products and services which enable an organization to meet its most important and time-sensitive objectives

2.11 disruption
event, whether anticipated (e.g. a labour strike or hurricane) or unanticipated (e.g. a blackout or earthquake), which causes an unplanned, negative deviation from the expected delivery of products or services according to the organization's objectives

2.12 exercise
activity in which the ICT continuity plan(s) is rehearsed in part or in whole to ensure that the plan(s) contains the appropriate information and produces the desired result when put into effect

NOTE An exercise can involve invoking business continuity procedures, but is more likely to involve the simulation of a business continuity incident, announced or unannounced, in which participants role-play in order to assess what issues might arise, prior to a real invocation.

2.13 ICT continuity
capability of the organization to plan for and respond to incidents and disruptions in order to continue ICT services at an acceptable predefined level

2.14 ICT disaster recovery
activities and programmes that are invoked in response to a disruption and are intended to restore an organization's ICT services

2.15 ICT services
combination of human, physical and logical assets together with data which support an organization in its day-to-day activities and consist of tools and/or facilities provided to access and use information and to communicate both internally and externally

2.16 impact
evaluated consequence of a particular outcome

2.17 incident
situation that might be, or could lead to, a business disruption, loss, emergency or crisis

2.18 incident management plan
clearly defined and documented plan of action for use at the time of an incident, typically covering the key personnel, resources, services and actions needed to implement the incident management process

2.19 invocation
act of declaring that an organization's business plan needs to be put into effect in order to continue delivery of key products or services

2.20 loss
negative consequence

2.21 organization
group of people and facilities with an arrangement of responsibilities, authorities and relationships

EXAMPLE
Company, corporation, firm, enterprise, institution, charity, sole trader or association, or parts or combinations thereof.

NOTE 1 The arrangement is generally orderly.

NOTE 2 An organization can be public or private. [BS EN ISO 9000:2005]

2.22 recovery point objective (RPO)
point in time to which data have to be recovered in order to resume ICT services

2.23 recovery time objective (RTO)
target time set for resumption of product, service or activity delivery after an incident

NOTE In the context of ICT continuity management RTO is measured from invocation through to service resumption. ICT RTO is generally less than the RTO for the resumption of products, services or activities.

2.24 resilience
ability of an ICT system to provide and maintain an acceptable level of service in the face of various disruptions and challenges to normal operation

2.25 risk
something that might happen and its effect(s) on the achievement of objectives

NOTE 1 The word "risk" is used colloquially in various ways, as a noun ("a risk" or, in the plural, "risks"), a verb (to risk [something], or to put at risk), or as an adjective ("risky"). Used as a noun the term "a risk" could relate to either a potential event, its causes, the chance (likelihood) of something happening, or the effects of such events. In risk management it is important to make a clear distinction between these various usages of the word "risk".

NOTE 2 Risk is defined relative to a particular objective; therefore, concern for several objectives implies the possibility of more than one measure of risk with respect to any source of risk.

NOTE 3 Risk is often quantified as an average effect by summing the combined effect of each possible consequence weighted by the associated likelihood of each consequence, to obtain an "expected value". However, probability distributions are needed to quantify perceptions about the range of possible consequences. Alternatively, summary statistics, such as standard deviation, may be used in addition to expected value.

2.26 risk appetite
total amount of risk that an organization is prepared to accept, tolerate or be exposed to at any point in time

2.27 risk assessment
overall process of risk identification, analysis and evaluation

2.28 risk management
structured development and application of management culture, policy, procedures and practices to the tasks of identifying, analysing, evaluating, and controlling responding to risk

2.29 stakeholders
those with a vested interest in an organization's achievements

NOTE This is a wide-ranging term that includes, but is not limited to, internal and "outsourced" employees, customers, suppliers, partners, employees, distributors, investors, insurers, shareholders, owners, government and regulators.

2.30 testing
forced failure of all or part of an ICT system, under specific conditions, to verify that recovery is properly performed

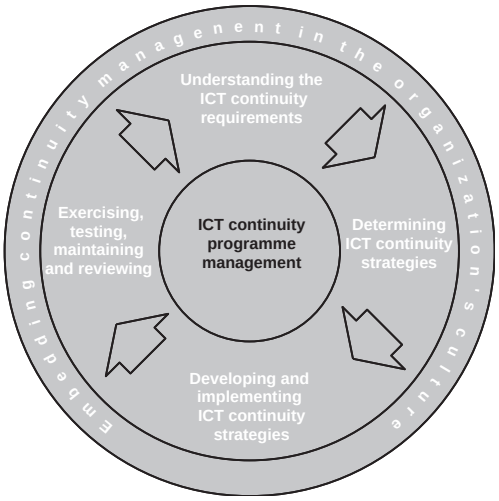
2.31 top management
person or group of people who direct and control an organization at the highest level [BS EN ISO 9000:2005]

NOTE Top management, especially in a large multinational organization, might not be directly involved; however, top management accountability through the chain of command is manifest. In a small organization, top management might be the owner or sole proprietor.

2.32 vulnerability
weakness within the ICT asset or activity that might, at some point, be exploited by threats

NOTE Examples of vulnerabilities are inadequate fire protection, poor utility supply and weak security protection.

3 ICT continuity programme management



Purpose:

To ensure the organization has a documented process that will support ICT continuity management.

3.1 Establishing ICT continuity management

The organization should develop, implement, maintain and continually improve a management system which will support ICT continuity management.

ICT continuity management should ensure that:

a) the ICT continuity management objectives are clearly stated, understood and communicated;

b) top management's commitment to ICT continuity management as part of business continuity management is demonstrated;

c) necessary resources are allocated; and

d) those with ICT continuity management responsibilities are competent to perform their roles.

3.2 Scope of ICT continuity management

3.2.1 General

The organization should define the scope of ICT continuity management and set ICT objectives, with due regard to the:

a) requirements for ICT continuity;

b) business continuity scope, objectives and obligations, including statutory, regulatory and contractual duties;

c) acceptable level of risk and ICT risks;

d) business continuity requirements; and

e) interests of its key stakeholders.

The organization should identify the ICT systems within the scope of business and ICT continuity.

3.2.2 ICT continuity policy

Top management should establish and demonstrate commitment to an ICT continuity management policy as part the overall BCM policy.

The policy should include or make reference to the:

a) organization's ICT strategy; and

b) scope of ICT continuity management, including limitations and exclusions.

The policy should be:

i) approved by top management;

ii) communicated to all persons working for or on behalf of the organization; and

iii) reviewed at planned intervals and when significant changes occur.

3.2.3 Provision of resources

The organization should determine and provide the resources needed to establish, implement, operate and maintain ICT continuity management.

ICT continuity management roles, responsibilities, competencies and authorities should be defined and documented.

Top management should:

a) appoint a person with appropriate seniority and authority to be accountable for ICT continuity management policy and implementation; and

b) appoint one or more persons with responsibility for implementing and maintaining ICT continuity management.

3.3 Embedding ICT continuity management into the organization's culture

Purpose:

To ensure that the organization embeds ICT continuity management into its routine ICT operations and management processes, so that it becomes one of the core values of the overall BC ICT management system through raising awareness and training appropriate staff.

3.3.1 Raising awareness

The organization should:

a) raise, enhance and maintain awareness through an ongoing education and information programme for relevant staff;

b) establish a process for evaluating the effectiveness of the awareness delivery; and

c) ensure that staff are aware of how they contribute to the achievement of the ICT continuity objectives.

3.3.2 Competency of ICT personnel

The organization should ensure that all personnel who are assigned ICT continuity management responsibilities are competent to perform the required tasks by:

a) determining the necessary competences for such personnel;

b) conducting training needs analysis on such personnel;

c) providing training;

d) ensuring that the necessary competence has been achieved; and

e) maintaining records of education, training, skills, experience and qualifications.

3.4 ICT continuity management documentation and records

The organization should have documentation covering the following aspects of ICT continuity management:

a) the ICT continuity management policy;

b) a list of critical ICT services, with the recovery time objective (RTO) and recovery point objective (RPO) for each, agreed by top management;

c) results of the business impact analysis;

d) results of the risk assessment;

e) the continuity strategy for each ICT service;

f) the continuity and incident management plans for ICT;

g) up-to-date contact and mobilization details for personnel and any relevant agencies, organizations and resources that might be required to support the response strategies;

h) training and awareness;

i) test/exercise programme, results and preventive and corrective actions (see **8.3**);

j) post-incident reviews; and

k) a description of the ICT components and how they are configured or linked to deliver each service.

Records should be established, maintained and controlled to provide evidence of the effective operation of ICT continuity management.

Documented procedures should be established in order to identify the controls over ICT continuity management documentation and records.

3.5 Monitoring and reviewing ICT continuity management

The person with accountability for ICT continuity (see **3.2.3**) should monitor and review ICT continuity management to ensure its effectiveness and efficiency. The review should ensure the appropriateness of the ICT continuity policy, objectives and scope, and determine and authorize actions for correction and improvement.

3.6 Preventive and corrective actions

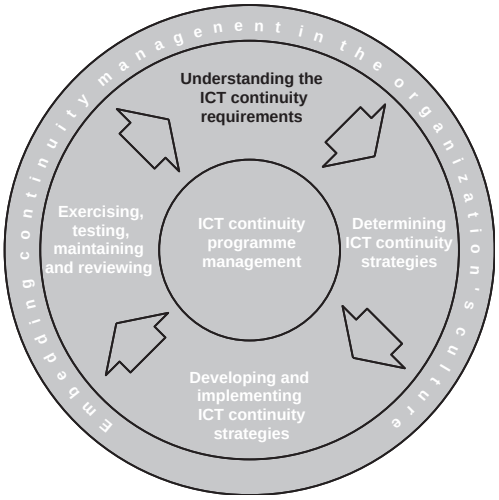
The organization should improve ICT continuity management through the application of preventive and corrective actions. These actions should be appropriate to the potential impact of the problems, as determined by the organization's business impact analysis (BIA) and its risk appetite.

Changes arising from preventive and corrective actions should be reflected in ICT continuity management documentation.

3.7 Continual improvement

The organization should continually improve the effectiveness of ICT continuity management through the review of the policy and objectives, audit results, preventive and corrective actions and management review.

4 Understanding the ICT requirements for business continuity



Purpose:

To determine the ICT continuity services that are required to support the organization's business continuity requirements, to understand how these ICT services are normally configured, both physically and logically, and to identify the gaps between current ICT continuity capability and business continuity requirement for each critical ICT service.

4.1 Defining ICT continuity requirements to meet business continuity requirements

4.1.1 As part of its BCM programme, the organization should categorize its activities according to their priority for recovery and define the minimum level at which each critical activity needs to be performed upon resumption. Top management should agree the organization's business continuity requirements. This should result in a documented RTO for each critical activity and minimum level at which each ICT continuity activity needs to be performed. This may include ICT service delivery, such as help desk.

4.1.2 The organization should define and document its ICT services. ICT service names should be meaningful to the organization. A brief description of each ICT service listed may be produced as business and ICT staff sometimes use different names for the same ICT service or have a different understanding of the service scope. Each ICT service listed should identify the organization's product or service that it supports.

4.1.3 The organization should identify and document the ICT services that are required to support the business continuity requirements. Some indication of the ICT service minimum capacity required at reinstatement and how quickly this capacity might need to be increased may also be necessary.

NOTE The ICT service RTO is generally less than the RTO for the critical activity it supports. (This might not be the case where the business continuity strategy calls for an interim measure, such as a manual procedure, instead of depending entirely upon the ICT service.)

4.1.4 Top management should agree the list of critical ICT services in **4.1.2** and their associated ICT continuity requirements in **4.1.3**.

4.2 Understanding critical ICT services

4.2.1 For each critical ICT service listed and agreed by top management, all the ICT components of the end-to-end service should be described and documented, showing how they are configured or linked to deliver each service. Both the normal ICT service delivery environment and the ICT continuity service delivery environment configurations should be documented.

4.2.2 For each critical ICT service the current continuity capability should be reviewed from a prevention perspective to assess risks of service interruption or degradation, e.g. single points of failure. Opportunities should also be sought to improve ICT service resilience and thereby lower the likelihood and/or impact of service disruption. It may also highlight opportunities to enable early detection and reaction to ICT service disruption. The organization can decide if there is a business case to invest in identified opportunities to improve service resilience. This service risk assessment may also provide a business case for enhancing ICT service recovery capability.

4.3 Identifying gaps between critical ICT continuity capability and business continuity requirements

4.3.1 For each critical ICT service the current ICT continuity arrangements should be compared with business continuity requirements and any gaps should be documented.

4.3.2 Top management should be informed of any gaps between critical ICT services continuity capability and business continuity requirements. Such gaps might indicate risks and the need for additional resilience and recovery resources, such as:

a) staff, including numbers, skills and knowledge;

b) premises used to house ICT facilities, e.g. computer room;

c) supporting technology, plant, equipment and networks (technology);

d) information applications and databases; and

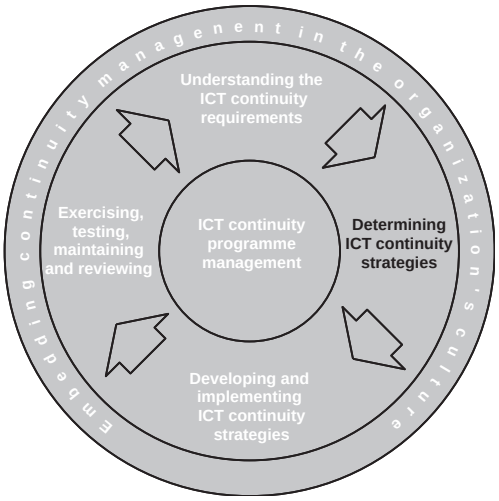
e) external services and suppliers (supplies).

Such additional resilience and recovery resources might require further finance or budget allocation.

4.4 Sign-off

Top management should sign off the ICT service definitions, the documented list of critical ICT services and the risks associated with gaps identified between critical ICT services continuity capability and business continuity requirements. This should include, where appropriate, the sign-off of identified risks (as outlined at **4.2.2**). The options for addressing the gaps and risks identified should then be explored by determining ICT continuity management strategies.

5 Determining ICT continuity strategies



Purpose:

To evaluate and recommend for acceptance by top management an overall ICT continuity management strategy and an ICT continuity management strategy per ICT service that closes the gaps between ICT continuity capability and business continuity requirements.

5.1 General

An ICT continuity management strategy should define an approach to implementing the required resilience, protection and recovery processes.

A full range of ICT continuity management options should be evaluated. The ICT continuity strategies chosen should be capable of supporting the business continuity requirements of the organization.

The organization should take into account the implementation and ongoing resource requirements when developing the strategy. External suppliers may be contracted to provide specialist services and skills that play an important role in supporting the strategy.

ICT continuity management strategy should be flexible enough to cater for different business strategies in different markets. In addition, the strategy options should take into account internal constraints and factors, such as:

- budget;
- resource availability;
- potential costs and benefits;
- technological constraints;
- the organization's risk appetite; and
- the organization's existing ICT strategy.

5.2 ICT continuity options

The organization should consider a range of options for the continuity of its ICT services. The options should consider increasing protection and resilience, as well as provision for recovery from an unplanned disruption, and may include provision made within the organization; services delivered to the organization; and services provided externally by one or more third parties.

The options should take account of the various components required to ensure the continuity and recovery of ICT services. Continuity may be achieved in many ways, and should address:

- skills and knowledge;
- premises;
- technology;
- data;
- suppliers.

5.3 Skills and knowledge

The organization should identify appropriate strategies for maintaining core ICT skills and knowledge. This may extend beyond employees to contractors and other stakeholders who possess extensive ICT specialist skills and knowledge. Strategies to protect or provide those skills may include:

a) documentation of the way in which critical ICT services are performed;

b) multi-skill training of ICT staff and contractors;

c) separation of core skills to reduce the concentration of risk (this might entail physical separation of staff with core skills or ensuring that more than one person has the requisite core skills); and

d) knowledge retention and management.

5.4 Premises

The organization should devise strategies for reducing the impact of the unavailability of the normal ICT premises. This may include one or more of the following:

a) alternative premises (locations) within the organization, including displacement of other activities;

b) alternative premises provided by other organizations;

c) alternative premises provided by third-party specialists;

d) working from home or at other remote sites;

e) other agreed suitable working premises;

f) use of an alternative workforce in an established site; and

g) alternative premises that can be transported to the site of the disruption and used to provide direct replacement of some of the physical assets involved.

In considering the use of alternative premises the following should be taken into consideration:

- site security;
- staff access; and
- proximity to existing premises.

NOTE 1 Strategies for ICT premises can vary significantly and a range of options might be available. Different types of incident or threat might require the implementation of different or multiple strategies. The correct strategies will in part be determined by the organization's size, sector and spread of activities, stakeholders, geographical base, technology available and other key constraints.

NOTE 2 Communications and network capability and security arrangements need to be considered to perform IT specific duties at these locations.

5.5 Technology

NOTE The provision of technology solutions to satisfy ICT continuity requirements depends on the nature of the ICT employed, the critical activities it supports, and the timescales and level of service required for its recovery.

ICT continuity strategies should be established to ensure the availability of those ICT services that support the recovery of the critical business activities within the RTOs defined as part of the organization's BIA process.

Additionally, critical business activities might depend on the provision of up-to-date or near-up-to-date data. Data continuity solutions should be designed to meet the RPOs of the organization as they relate to the critical business activities.

The technologies that support ICT services frequently need complex arrangements to ensure continuity, so the following should be considered when selecting ICT strategies:

- RTOs and RPOs for ICT services which support the key activities identified by the BCM programme;
- location and distance between technology sites;
- number of technology sites;
- remote access to systems;
- cooling requirements;
- power requirements;
- the use of un-staffed (dark) sites as opposed to staffed sites;
- telecoms connectivity and redundant routing;
- the nature of "failback" (whether manual intervention is required to activate alternative ICT provision or whether this needs to occur automatically);
- level of automation required;
- technology obsolescence; and
- outsourced service providers connectivity and other external links.

5.6 Data

The chosen continuity options should ensure the ongoing confidentiality, integrity, availability and currency of critical data that support critical activities (see BS ISO/IEC 27001 and BS ISO/IEC 27002).

Data storage and continuity strategies should meet the organization's business continuity requirements, and should take account of:

- RPO requirements;
- how data are securely stored, e.g. disk, tape or optical media; appropriate backup and restoration mechanisms should be in place to ensure the data are secure and in a safe environment;
- where information is stored, transported or transmitted, distance, location, network links, etc. (onsite, offsite or third party), and expected timescales for the retrieval of backup media; and
- restore timescales, driven by the volume of data, how they are stored and the complexity of the technical restore process, along with the requirements of the service user and the needs of organizational continuity.

NOTE An understanding of the "end-to-end" use of data throughout the organization, including information feeds to and from third parties, is a critical input in developing and ICT continuity management strategy.

The nature, currency and value of data will vary enormously within an organization.

5.7 Suppliers

The organization should identify and document external dependencies which support ICT service provision and take adequate steps to ensure that critical equipment and services can be provided by their suppliers within predetermined and agreed timeframes. Such dependencies may exist for hardware, software, telecoms, applications, third party hosting services, utilities, and environmental issues, such as air conditioning, environmental monitoring and fire suppression.

Strategies for these services may include:

- storage of additional equipment and software copies at another location;
- arrangements with suppliers for the delivery of replacement equipment at short notice;
- rapid repair and/or replacement of faulty parts in the event of an equipment malfunction;
- dual supply of utilities such as power and telecoms;
- emergency generating equipment; and
- identification of alternative/substitute suppliers.

The organization should include ICT and business continuity management requirements in contracts with its partners and service providers. Contract schedules should include reference to each party's obligations, agreed service levels, response to major incidents, cost assignment, exercising frequency and corrective actions.

5.8 Sign-off

ICT continuity options should be presented to top management, with recommendations for a decision based on risk appetite and cost.

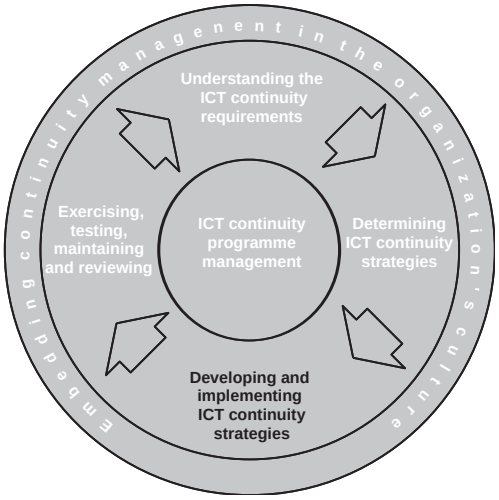
Top management should be advised if ICT continuity options are unable to meet the business continuity requirements, in which case they may be informed of current capability.

Top management should choose the ICT continuity strategies from the options presented to them, and approve and sign off the documented options to confirm that the continuity options have been properly undertaken and that they support the overall business continuity requirements.

The agreed ICT continuity management options should:

- cater for likely risks and effects of disruption;
- integrate with the organization's chosen business continuity strategies; and
- be appropriate to meet the organization's overall objectives within its risk appetite.

6 Developing and implementing ICT strategies



Purpose:

To implement the organization's chosen ICT continuity management strategies, along with the necessary organization structure, plans and procedures required to support the implementation.

6.1 Implementing ICT management strategies

The ICT continuity management strategy should only be implemented when approved by top management.

Each strategy should be implemented as part of an ongoing project/lifecycle through the organization's formal project management controls, change control process and BCM programme management in order to ensure full management visibility and reporting.

6.2 Skills and knowledge

Successful implementation may include:

- documentation of processes and procedures;
- documentation of ICT-related knowledge;
- cross training to ensure skills/knowledge gaps are minimized;
- succession planning; and
- the avoidance of a concentration of skilled staff at one location.

6.3 Processes

Continuity and recovery processes should be documented, clear and in sufficient detail to enable competent staff to execute them (these may differ from processes within the business-as-usual environment).

These documented processes may include procedures at an alternative location to their normal place of operation. In practice, such procedures may be required to be adapted according to the precise circumstances of the disruption (e.g. degree of loss or damage), the operational priorities of the organization and the demands of external stakeholders.

6.4 Technology

ICT technology strategies may include:

- Hot Standby, where ICT infrastructure is replicated across two sites;
- Warm Standby, where recovery takes place at a secondary site where ICT infrastructure is partially prepared;
- Cold Standby, where infrastructure is built or configured from scratch at an alternative location;
- Ship-in arrangements, under which external service providers provide hardware; and
- Composite arrangement of the preceding strategies: a "pick-and-mix" approach.

6.5 Data

The arrangements for the availability of data should be aligned with the requirements identified within the ICT continuity management strategies, and may include:

- additional storage for data in a format that ensures their availability within the timescales identified in the business continuity programme; and
- alternative locations for data storage, which may be physical or virtual, provided the security and confidentiality of the data are maintained; thus, appropriate access procedures should be in place and, if arrangements are made through third parties for the storage of that information, the information owners should satisfy themselves that appropriate controls are in place.

6.6 ICT incident response

For any ICT incident there should be an incident response to:

- confirm the nature and extent of the incident;
- take control of the situation;
- contain the incident; and
- communicate with stakeholders.

The incident response should trigger an appropriate ICT continuity management response. This response should integrate with overall BCM incident management, and may constitute an incident management team (IMT) or, in a small organization, a single individual with the responsibility for incident and business continuity management.

A larger organization may use a tiered approach and may establish different teams to focus on different functions. Within ICT, this may be based on technical or service-related issues.

NOTE In some cases the potential impact of a disruption to ICT services might require a wider incident management response in the context of the organization's business continuity plan, and actions such as media communications and welfare management.

Those responsible for incident management should have plans for the activation, operation, coordination and communication of the incident response.

6.7 Plans

6.7.1 General

The organization should have plans to manage potentially disruptive incidents to enable ICT continuity and recovery of critical activities.

The organization's ICT incident management, business continuity and technical recovery plans may be activated in rapid succession or simultaneously.

The organization may develop specific plans to recover or resume ICT services back to a "normal" state (recovery plans). However, as it is not always clear what "normal" looks like until some time after an incident, it might not be possible to implement recovery plans immediately. The organization should therefore ensure that the ICT continuity plans are capable of extended operation in support of the wider business continuity, giving time for the development of recovery ("back-to-normal") plans.

6.7.2 Content of plans

A small organization may have a single plan that encompasses all activity to recover the ICT services of its entire operations. A very large organization may have many plans, each of which specifies in detail the recovery of a particular element of its ICT services.

All plans, whether incident management plans or ICT continuity plans, should be concise and accessible to those with responsibilities defined in the plans. Plans should contain the following elements.

a) Purpose and scope

The purpose and scope of each specific plan should be defined, agreed by top management, and understood by those who will invoke the plan. Any relationship to other relevant plans or documents within the organization, particularly to BC plans, should be clearly referenced and the method of obtaining and accessing these plans described. Each plan should state clearly what it does not intend to achieve and why.

Each incident management and ICT continuity plan should set out prioritized objectives in terms of:

- the critical ICT service activities to be recovered;
- the timescales in which they are to be recovered;
- the recovery levels needed for each critical ICT service activity; and
- the situation in which each plan can be invoked.

Plans may also contain, where appropriate, procedures and checklists that support the post-incident review process.

b) Roles and responsibilities

The roles and responsibilities of the people and teams having authority (both in terms of decision-making and authority to spend) during and following an incident should be clearly documented.

c) Plan invocation

NOTE Time lost during a response can never be regained. It is almost always better to initiate an ICT response and subsequently stand it down than to miss an opportunity to contain an incident early and prevent escalation.

Organizations therefore need to use the incident management escalation and invocation protocols contained within their wider business continuity incident management plans to form the basis for managing potential ICT-related service disruptions.

The method by which an ICT continuity plan is invoked should be clearly documented. This process should allow for the relevant plans or parts thereof to be invoked in the shortest possible time, either in advance of a potentially disruptive event or immediately following the occurrence of an event.

The plan should include a clear and precise description of:

- how to mobilize the ICT continuity management team;
- immediate rendezvous points;
- subsequent team meeting locations and details of any alternative meeting locations (in a larger organization these meeting places may be referred to as "command centres"); and
- circumstances under which the organization deems an ICT continuity response is not necessary (e.g. minor faults and outages, perhaps to critical ICT services, but which are managed by normal helpdesk and support arrangements and agreements).

The organization should document a clear process for standing down the ICT continuity management team(s) once the incident is over, and returning to business-as-usual.

d) Plan owner and maintainer

The organization should nominate the primary owner of the plan and identify and document who is responsible for reviewing, amending and updating the plan at regular intervals.

A system of version control should be employed, and changes formally notified to all interested parties with a formal plan distribution record maintained.

e) Contact details

NOTE The contact records may include "out of hours" contact details. However, where plans reference such private details, respect for data protection has to be a paramount consideration.

Each plan should contain or provide a reference to the essential contact details for all key stakeholders.

6.7.3 The ICT continuity plan

Purpose:

To allow the organization to manage an ICT incident.

The ICT continuity plan should:

i) be flexible, feasible and relevant;

ii) be easy to read and understand; and

iii) provide the basis for managing serious issues that are deemed by the organization to merit an ICT continuity response (typically following a significant disruption event).

The ICT continuity plan should define the overarching framework within which the recovery plans are organized, covering:

- overall strategy;
- critical services (with RTO/RPO);
- timelines for recovery; and
- recovery teams and their responsibilities.

The recovery plans should be documented such that competent personnel can use them in the event of an incident. The recovery plans should include:

a) **Objectives:** a short description of the objectives of the plan;

b) **Scope:** covering the following, with reference to the results of the BIA:

   - the criticality of services: description of the relevant services and identification of their criticality;
   - technology: overview of the main technology that supports the services, including where it is housed;
   - organization: overview of the organizations (departments, vital persons and procedures) that manage the technology;
   - documentation: overview of the main documentation for the technology, including the (offsite) locations where it is stored;

c) **Availability requirements:** business-defined requirements for the availability of services and related technology;

d) **Technology recovery procedures:** description of the procedures to be followed to recover the ICT service, including the following:

   - a list of activities, e.g. desktop support and restore contact information;
   - a list of activities to recover network, systems, applications, databases, etc., to an agreed level at an alternative location, taking into account the changed environment (e.g. this could affect line capacity, system-to-system communications, etc.);
   - a list of activities to restore basic functionality, such as security, routing and logging;
   - coordination within the application, or between applications, data synchronization, and potential automated procedures for handling a backlog of information;

- the process needed to restore the ICT services and turn them over to their users to operate in recovery mode;
- backup procedures;
- where and how people can get further information, instructions, etc., e.g. hotline numbers; and
- steps to take to return to normal.

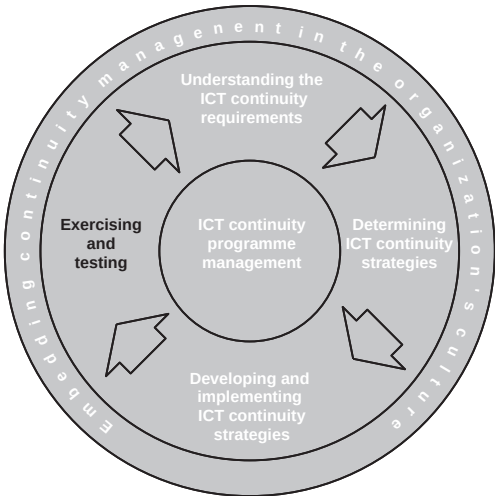
e) **Appendices**

- inventory of information systems, applications and databases;
- overview of network infrastructure and server names;
- inventory of hardware and systems software; and
- contracts and service level agreements.

f) **Key ICT suppliers**

- business-as-usual suppliers; and
- recovery service suppliers.

7 Exercising and testing



Purpose:

To ensure that the chosen strategies and plans will work as anticipated and when required, providing assurance and knowledge and raising awareness within the business

7.1 Exercising the elements of an ICT service

NOTE An organization's ICT continuity plans cannot be considered reliable until exercised. An exercise programme may involve a number of different exercises and tests that, taken together, validate the whole of ICT resilience and recovery capabilities for services that support the organization's overall business continuity.

The organization should exercise, not only the recovery of the ICT service but also its resilience elements in order to determine whether:

a) the service can be protected, maintained and/or recovered regardless of the incident severity;

b) the ICT continuity management arrangements can minimize the impact to the business; and

c) the procedures for return to business-as-usual are valid.

7.2 Exercising

7.2.1 Exercise programme

NOTE The exercise is a business-wide activity and not just the domain of the ICT department. It may extend to suppliers and other third parties. The ICT department may retain the planning and execution aspects of the exercise, but the organization still has a key role to play.

In most instances, the whole ICT recovery cannot be proven in one exercise. A progressive exercising regime might therefore be appropriate to build towards a full simulation of a real incident. The programme should include different levels of exercise from familiarization to computer room resilience, as defined in Figure 2 (see **7.2.2**), and should consider all aspects of the end-to-end ICT service delivery.

The risk associated with exercising and the exercise programme should be understood. The exercise programme should not expose the organization to an unacceptable level of risk. Top management

sign-off on the exercise programme should be obtained and a clear explanation of the associated risks documented.

The ICT continuity exercise programme objectives should be fully aligned to the wider business continuity management scope and objectives and complementary to the organization's broader exercise programme. Each exercise should have both business objectives (even where there is no direct business involvement) and defined technical objectives to test or validate a specific element of the recovery or resilience strategy.

Exercising individual elements in isolation at the component level is complementary to full systems exercising and should be maintained as part of an ongoing exercise programme.

The ICT continuity exercise programme should define the frequency, scope and format of each exercise. The following are high level examples of exercise scopes:

- data recovery: recovery of a single file or database following corruption;
- recovery of a single server (including a full rebuild);
- recovery of an application (this may consist of several servers, sub-applications and infrastructure);
- failover of services hosted on a high availability platform (for example, clustering: simulating the loss of one of the pair in a cluster);
- data recovery from backup (recovery of single files or series of files from offsite tape storage);
- network testing; and
- communications infrastructure failover tests.

Exercises should be progressive to include an increasing test of dependencies and inter-relationships and relevant end-user communities.

7.2.2 The scope of exercises

Exercising should be carried out to:

- build confidence throughout the organization that the resilience and recovery strategy will meet the business requirements;
- demonstrate that the services can be maintained or recovered within agreed service levels or recovery objectives regardless of the incident;
- demonstrate that the services can be restored to pre-test state in the event of an incident at the recovery location;
- provide the opportunity for staff to familiarize themselves with the recovery process;
- identify any improvements that are required to the strategy, architecture or recovery processes; and
- provide the basis for an audit trail and organizational competence.

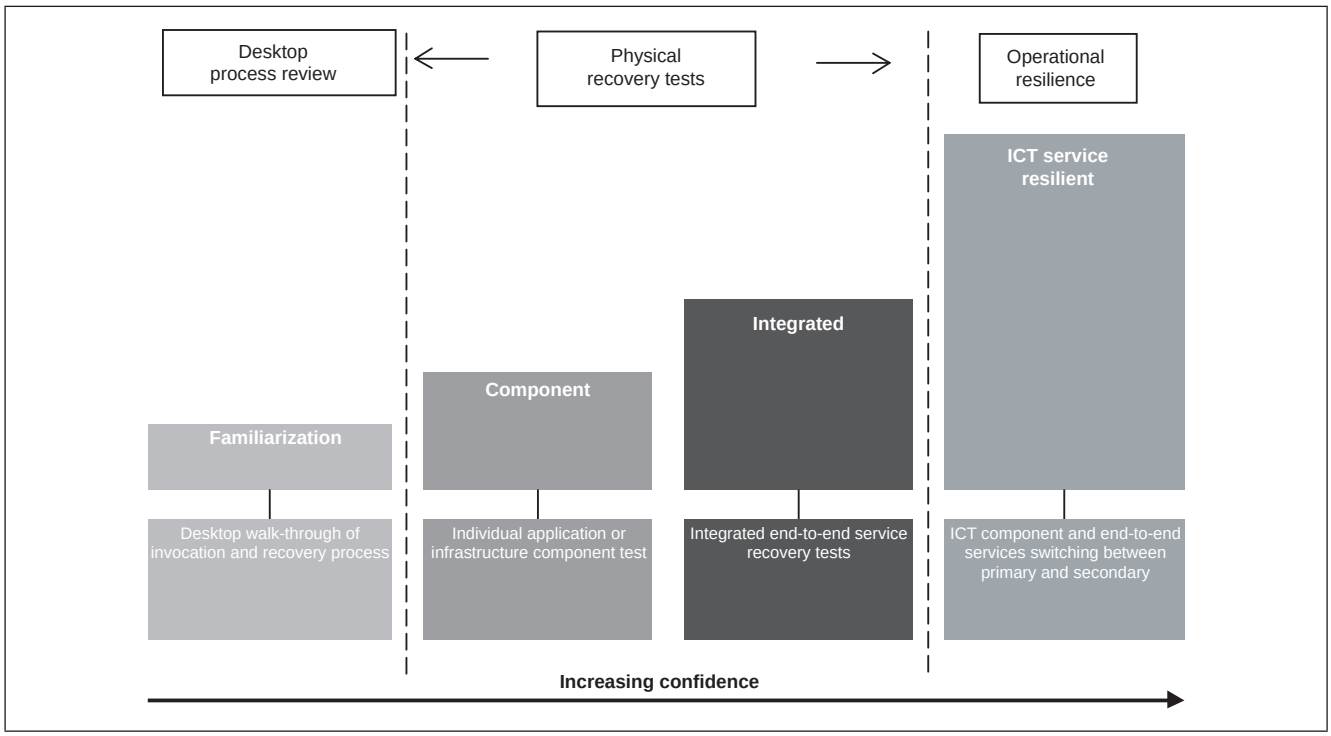
Exercising should apply to the ICT environment and all the components that deliver the end-to-end service from the computer room through to the user desktop or any other service delivery channel.

7.2.3 Elements of service recovery

The organization should exercise all elements of the ICT service recovery as appropriate to its size, complexity and business continuity management scope. The exercising should not focus solely on service recovery and resumption, but should include the reliability of the resilience capability, system monitoring and alert management.

The organization should exercise at component level through to full location-based system testing in order to achieve high levels of confidence and resilience (see Figure 2).

Figure 2 **Elements of ICT service recovery**



The following elements should be exercised:

- computer room, such as physical security; fire and water leak detection systems; evacuation process; heating, ventilation and air conditioning; environmental monitoring; and alert protocols and electrical services;
- infrastructure, including the overall resilience of the network connectivity; network diversity; and network security, including anti-virus protection and intrusion prevention and detection (see BS ISO/IEC 27001);
- hardware, including servers, telecommunications equipment, storage arrays and removable media;
- software;
- data; and
- services.

7.3 Planning

To ensure that it does not cause incidents or undermine the service capability, an exercise should be carefully planned to minimize the risk of an incident occurring as a direct result of the exercise.

This risk management should be appropriate to the level of exercise being undertaken (i.e. component or computer room), and may include:

- ensuring that all data are backed up immediately prior to the exercise;
- conducting exercises in isolated environments; and
- scheduling exercises "out of hours" or during quiet times in the business cycle, with the knowledge of the end users.

Exercises should be realistic, carefully planned and agreed with stakeholders, so that there is minimum risk of disruption to business processes. They should not, however, be carried out during incidents.

The scale and complexity of exercises should be appropriate to the organization's recovery objectives.

Each exercise should have a "terms of reference", agreed and signed off in advance by the exercise sponsor, which may include the following:

- description;
- objectives;
- scope;
- assumptions;
- constraints;
- risks;
- success criteria;
- resources;
- roles and responsibilities;
- high-level timeline/schedule;
- exercise data capture;
- exercise/incident logging;
- debriefing; and
- post-exercise actions (follow-up and reporting).

Planning an exercise should enable the organization to achieve the success criteria identified.

7.4 Managing the exercise

A clear exercise command structure should be developed with roles and responsibilities allocated to appropriate individuals. The exercise command structure may include:

- exercise command;
- exercise communications;
- confirmation that there are enough staff available to undertake the exercise with safety;

- sufficient observers and/or facilitators to capture the exercise proceedings and maintain an issues log;
- key exercise milestones;
- end of exercise protocols; and
- emergency stop exercise protocols.

The exercise should be run through the exercise command structure to ensure that:

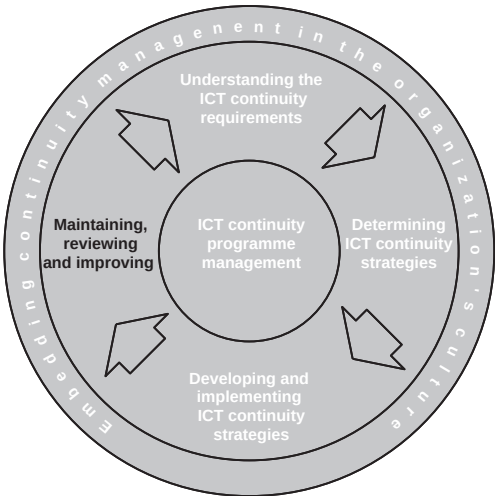
- objectives and key milestones are met;
- all exercise materials and activities have appropriate levels of confidentiality;
- any ongoing risks are monitored and mitigated;
- any visitors/observers are authorized;
- exercise proceedings are captured in a consistent manner; and
- all participants are debriefed and feedback is collated.

7.5 Review, report and follow-up

At the end of an exercise its findings should be reviewed and followed up promptly. This should include:

- gathering the results and findings;
- analysing the results and findings against the exercise objectives and success criteria;
- identifying any gaps;
- assigning action points with defined timelines;
- creating an exercise report for formal consideration by the exercise sponsor; and
- consolidating and following up exercise report actions.

8 Maintenance, review and improvement



Purpose:

To permit the organization's ICT continuity management strategy to remain resilient and adaptable in a dynamic operating environment.

8.1 Change control

8.1.1 Dealing with change

With change comes risk; not only the risk of failure, but the risk of destabilizing existing policies and strategies. The ICT continuity management strategy should therefore be resilient and adaptable.

No change to the ICT service should be implemented until the implications of the change have been assessed and addressed from both a technical and a business perspective.

To ensure that the ICT continuity management strategy and plans remain appropriate for the organization:

a) top management should ensure that the ICT continuity management strategy continues to support the organization's BCM requirements;

b) the change management process should include all parties responsible for the ICT continuity management strategy, both its compilation and its delivery;

c) the development process for new ICT services should include sign-off that resilience has not been compromised;

d) due diligence on merger and acquisition activity should include a resilience assessment; and

e) ICT component decommissioning should be reflected within related ICT continuity management.

8.1.2 Control of ICT continuity management records

Controls should be established over ICT continuity management records in order to:

a) ensure that they remain legible, readily identifiable and retrievable; and

b) provide for their identification, storage, protection and retrieval.

8.1.3 Control of ICT continuity management documentation

Controls should be established over ICT continuity management documentation to ensure that:

a) documents are approved for adequacy prior to issue;

b) documents are reviewed and updated as necessary and re-approved;

c) changes and the current revision status of documents are identified;

d) relevant versions of applicable documents are available at points of use;

e) documents of external origin are identified and their distribution controlled; and

f) the unintended use of obsolete documents is prevented and that such documents are suitably identified if they are retained for any purpose.

8.2 Review of ICT continuity management

8.2.1 Timing and content of review

Top management should ensure that ICT continuity management is reviewed at planned intervals. This review may take the form of internal or external audits, or self-assessments.

The review should include assessing opportunities for improvement and the need for changes to ICT continuity management, including the ICT continuity management policy and ICT continuity management objectives.

The results of the review should be clearly documented and records should be maintained.

8.2.2 Review input

The input to a management review should include information on:

a) internal service levels;

b) external service providers' ability to maintain appropriate levels of service;

c) results of relevant audits;

d) feedback from interested parties, including independent observations;

e) status of preventive and corrective actions;

f) level of residual risk and acceptable risk;

g) follow-up actions from previous management reviews and recommendations;

h) lessons learned from exercises, incidents and the education and awareness programmes;

i) emerging good practice and guidance.

8.2.3 Review output

The output from the review should be signed off by top management and include:

a) varying the scope of ICT continuity management;

b) improving the effectiveness of ICT continuity management;

c) modifying ICT continuity management strategy and procedures, as necessary, to respond to internal and/or external events that could impact on ICT services, including changes to:

   1) business requirements;

   2) resilience requirements; and

   3) levels of risk and/or levels of risk acceptance;

d) resource needs; and

e) funding and budget requirements.

8.3 Improving ICT continuity management through preventive and corrective actions

8.3.1 General

The organization should improve ICT continuity management through the application of preventive and corrective actions which are appropriate to the potential impacts determined by the organization's business impact analysis (BIA) and its risk appetite.

Changes arising from such preventive and corrective actions should be reflected in ICT continuity management documentation.

8.3.2 Preventive actions

The organization should identify potential weaknesses in ICT services, and establish a documented procedure for:

a) identifying potential failures;

b) identifying the causes of failures;

c) determining and implementing preventive action needed;

d) reviewing and recording results of action taken; and

e) informing appropriate individuals or groups of the potential failures and preventive action put in place.

8.3.3 Corrective actions

The organization should take action to correct any actual failure of ICT service. The documented procedures for corrective action should define the requirements for:

a) identifying the failures;

b) determining the causes of failures;

c) evaluating the need for actions to ensure that failures do not recur;

d) determining and implementing the corrective action needed;

e) recording the results of action taken; and

f) reviewing the corrective action taken.

Annex A (informative)

ICT continuity management milestones

Figure A.1 illustrates key ICT continuity management milestones along a time line starting at Time Zero when an ICT service disruption event occurs.

The Recovery Point Objective (RPO) indicates the amount of data loss that can be expected following a disruption, given the ICT service recovery strategy employed. This is represented on the time line as the amount of time between the last good backup and when the disruption occurs.

The first milestone after the ICT service disruption occurs is detection of service loss (or degradation), for which there will be an elapsed time before the notification; for example, in some instances notification might come via a call to the IT helpdesk from a user.

Further time could elapse while the ICT service disruption is investigated, analysed, communicated and a decision taken to invoke ICT continuity. It might take several hours from the onset of ICT service disruption until a decision is taken to invoke ICT continuity once communication and decision-making time is taken into account. The invocation decision might require careful consideration in some situations, for example where the service has not been entirely lost or there seems to be a strong prospect of imminent service reinstatement, because invoking ICT continuity often impacts upon normal business operations.

Once invoked, ICT service recovery can commence. This can be divided into infrastructure (network, hardware, operating system, backup software, etc.) and application recovery (database, application, batch processes, interfaces, etc.).

Once the ICT service has been restored and some systems testing has been conducted by ICT staff the service can be made available for user acceptance testing before it is released to staff for use in business continuity operations.

From a business continuity perspective there is an RTO for each product, service or activity. This RTO starts from the point at which the disruption occurs and runs until the product, service or activity is resumed. A number of ICT services might be required to enable this and each of these ICT services could comprise a number of ICT systems or applications. Each of these component ICT systems or applications will have its own RTO as a subset of the end-to-end ICT service RTO and this ought to be less than the business continuity RTO, taking into account the detection and decision-making time and the user acceptance testing time (unless the business continuity product, service or activity can be supported without ICT for a period, for example using manual procedures).

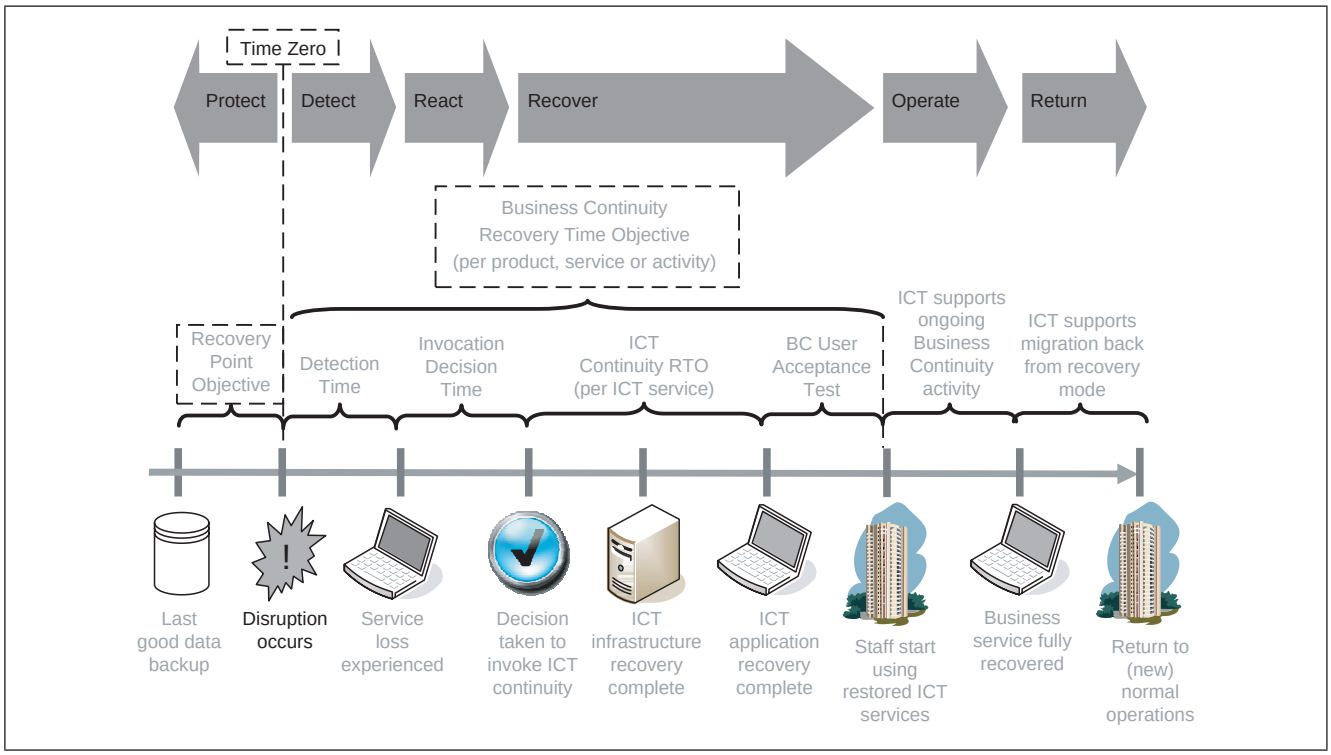
Recovered ICT services typically operate for a period of time supporting business continuity activity. If this is an extended period, then recovered ICT services might need to be scaled up to support an increasing volume of activity, potentially up to the point at which the product, service or activity is fully recovered to normal transaction volumes.

At some point in the future business will want to migrate back from business continuity to "normal" operations. While ICT staff have the opportunity to carefully plan this migration and schedule it to take place during a natural lull in operations, this is nevertheless a substantial task in its own right. Returning to normal operations

might better be termed returning to (new) normal operations as the disruption might have forced a permanent change upon the business.

The arrows across the top of Figure A.1 indicate how the principles of ICT continuity detailed in BS 25777 align with the disruption time line.

Figure A.1 **Key ICT continuity management timescales**



Bibliography

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 25999, *Business continuity management*

BS EN ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*

BS ISO/IEC 20000-1, *Information technology — Service management — Part 1: Specification*

BS ISO/IEC 20000-2, *Information technology — Service management — Part 2: Code of Practice*

BS ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

BS ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security management*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 9000 Fax: +44 (0)20 8996 7400

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

You may also buy directly using a debit/credit card from the BSI Shop on the website **www.bsigroup.com/shop**

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library.

Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre.

Tel: +44 (0)20 8996 7111
Fax: +44 (0)20 8996 7048 Email: info@bsigroup.com

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com**

Copyright

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™

British Standards