

BS 25777:2008



BSI Standards Publication

Information and communications technology continuity management — Code of practice

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© BSI 2008

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

Foreword *ii*

Introduction *1*

1 Scope *5*

2 Terms and definitions *5*

3 ICT continuity programme management *9*

4 Understanding the ICT requirements for business continuity *13*

5 Determining ICT continuity strategies *15*

6 Developing and implementing ICT strategies *20*

7 Exercising and testing *26*

8 Maintenance, review and improvement *31*

Annexes

Annex A (informative) ICT continuity management milestones *34*

Bibliography *36*

List of figures

Figure 1 – Relationship between ICT continuity management and business continuity management *3*

Figure 2 – Elements of ICT service recovery *28*

Figure A.1 – Key ICT continuity management timescales *35*

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 services¹⁾ 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:

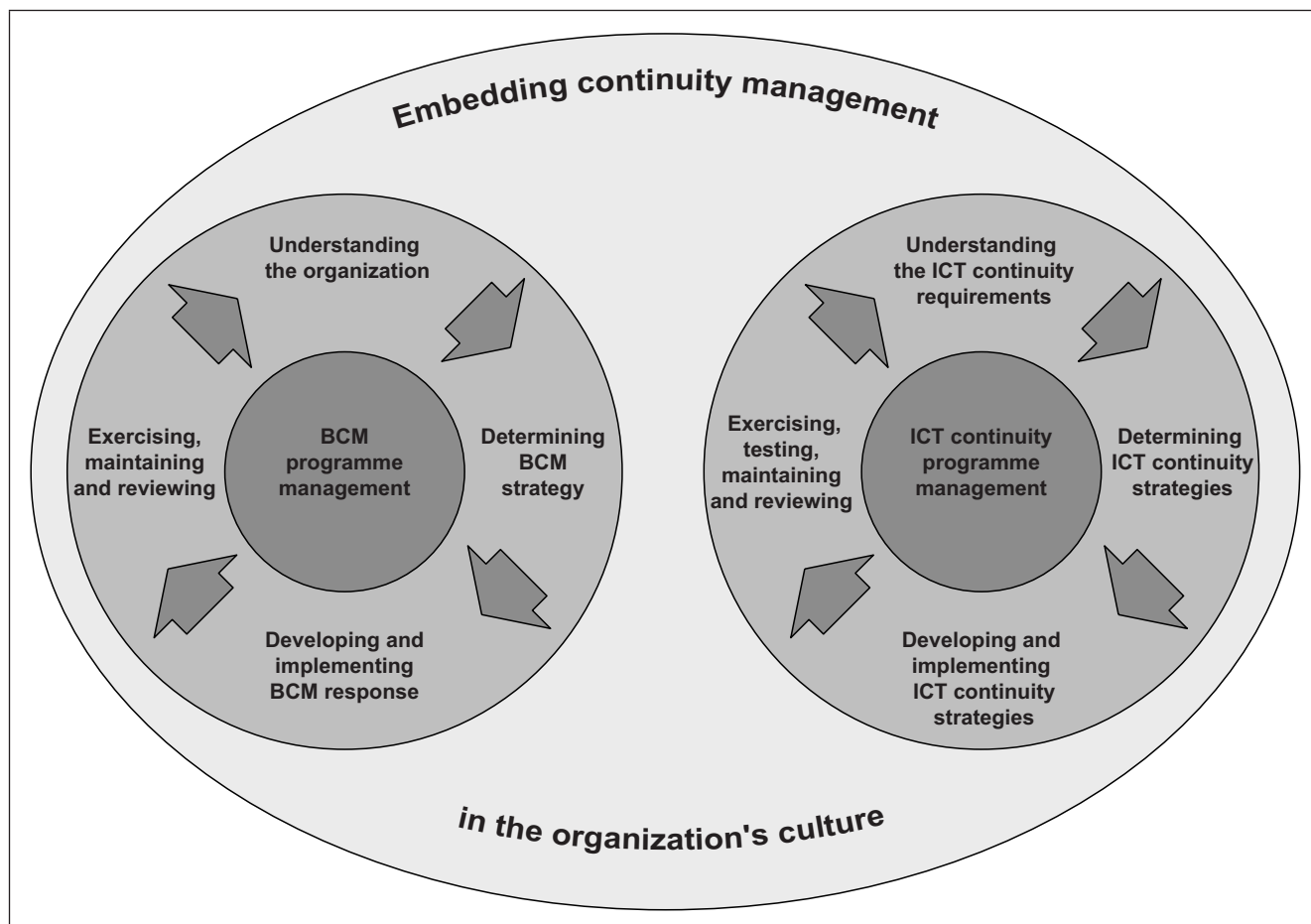
- they are resilient and recoverable at the appropriate level;
- any unexpected event within a service is detected, addressed and investigated in a timely manner;
- the dependencies between ICT services and external factors²⁾ are known and used in assessing risk and the impact of change; and

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

- dependencies on the technical components³⁾ 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:

- 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.
- Detect:** Detecting incidents at the earliest opportunity will minimize the impact to services, reduce the recovery effort, and preserve the quality of service.
- 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 services⁴⁾ 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]

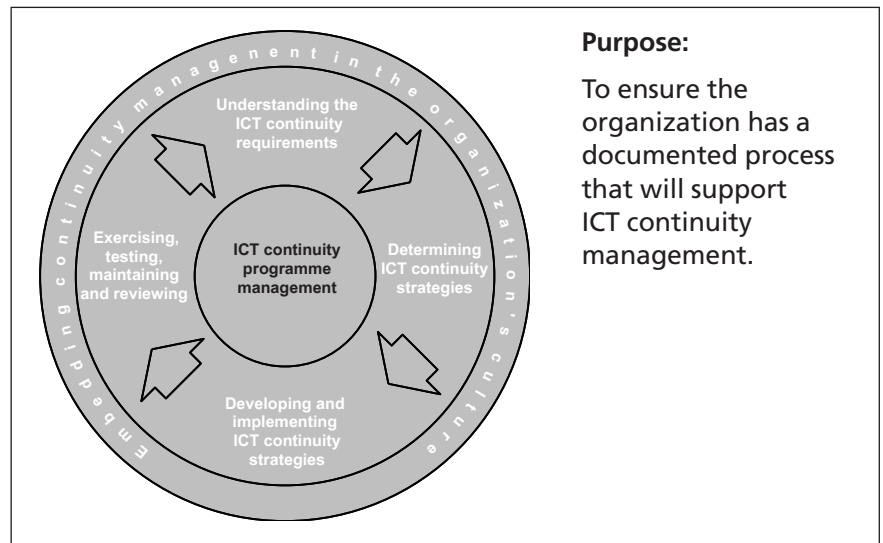
NOTE Top management, especially in a large multinational organization, might not be directly involved; however, top management accountability through the chain of command is manifest. In a small organization, top management might be the owner or sole proprietor.

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



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.