

PD 25888:2011



BSI Standards Publication

PUBLISHED DOCUMENT

Business continuity management – Guidance on organization recovery following disruptive incidents

This publication is not to be regarded as a British Standard.

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 2011

ISBN 978 0 580 65641 5

ICS 03.100.01

The following BSI references relate to the work on this standard:
Committee reference BCM/1

Publication history

First published, December 2011

Amendments issued since publication

Date	Text affected
-------------	----------------------

Contents

Foreword *ii*

Introduction 1

1 Scope 1

2 Terms and definitions 2

3 The relationship between recovery management, incident management and business continuity management 5

4 Establishing an organization recovery management capability 7

5 Organization recovery planning 7

6 Actions on implementation 11

7 Return to normal operations 20

Annexes

Annex A (informative) Possible causes of restrictions to access to premises 21

Annex B (informative) Insurance 22

Bibliography 25

List of figures

Figure 1 – The incident timeline 6

Figure 2 – Example of recovery management team structure 9

List of tables

Table A.1 – Access issues arising from type of building 22

Summary of pages

This document comprises a front cover, an inside front cover, pages i to ii, pages 1 to 26, an inside back cover and a back cover.

Foreword

Publishing information

This Published Document is published by BSI and came into effect on 31 December 2011. It was prepared by BSI panel BCM/1/-/6, *BCM – Recovery*, 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 guide, this Published Document 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.

It has been assumed in the preparation of this Published Document that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

Presentational conventions

The provisions in this Published Document are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is “should”.

The word “should” is used to express recommendations of this Published Document. 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.

This Published Document is not to be regarded as a British Standard.

Introduction

This Published Document (PD) focuses on recovery management in the context of a single organization and is designed to complement the provisions BS 25999-1:2006 and BS 25999-2:2007. Recovery management provides an organization with a capability to recover (restore or reconfigure) to an agreed strategic and operational state following a single (or series of) damaging incident(s).

Recovery management has to take account of any financial, legal, regulatory, environmental, reputational and emotional consequences arising from a risk or actual incident, and the consequences of activities associated with organizational recovery.

The nature, complexity and scale of recovery management cannot be determined in advance of an incident; therefore, recovery management has to be flexible, scalable and relevant to a broad range of risks applicable to the organization and its operating environment.

Some incidents are dramatic and could change the very fabric of “normality” for the organization and its stakeholders, so lessons have to be learned from the response to any incident and the recovery management arrangements reviewed. For this reason, recovery management might need to operate under new operating norms beyond recovering to pre-recovery conditions. Recovery management has to balance predetermined recovery requirements against emerging or changing expectations.

It is necessary that an organization’s recovery arrangements interface with any incident management and business continuity management (BCM) arrangements. This PD assumes that effective BCM is already in place within the organization.

1 Scope

This Published Document (PD) gives guidance on the development and implementation of the organization recovery element applicable to an organization’s response to an incident.

NOTE 1 Successful implementation of organization recovery is mutually dependent upon effective implementation of incident management and business continuity plans.

This PD is applicable to recovery management prior to, during and after an incident that disrupts an organization’s ability to deliver its products and/or services.

This PD is generic and intended to be applicable to all organizations (or parts thereof), regardless of type, size and nature of business. The extent of application depends on the organization’s operating environment and complexity.

NOTE 2 Annex A discusses possible causes of restrictions to access to premises following an incident and Annex B discusses insurance as a means of obtaining financial compensation for loss of assets.

2 Terms and definitions

For the purposes of this Published Document, 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.

[BS 25999]

2.2 business continuity

strategic and tactical capability of the organization to plan for and respond to incidents and organization disruptions in order to continue business operations at an acceptable pre-defined level

[BS 25999]

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, may 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.

[BS 25999]

2.4 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

[BS 25999]

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 pre-defined level

[BS 25999]

2.6 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

[BS 25999]

2.7 business impact analysis (BIA)

process of analysing business functions and the effect that a business disruption may have upon them

[BS 25999]

2.8 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.

[BS 25999]

2.9 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

[BS 25999]

2.10 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

[BS 25999]

2.11 impact

evaluated consequence of a particular outcome

[BS 25999]

2.12 incident

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

[BS 25999]

2.13 incident management plan (IMP)

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

[BS 25999]

2.14 incident management team (IMT)

group of individuals responsible for confirming the nature and extent of an incident, taking control of the situation, mitigating the impact of the incident, and communicating with stakeholders

NOTE 1 The same team is also responsible for triggering an appropriate business continuity response. This is sometimes known as the "crisis management team".

NOTE 2 In small organizations the responsibility for incidents and business continuity management may be vested in a single individual. Larger organizations may use a tiered approach and may establish different teams to focus on incident management, business continuity and business recovery issues. In some cases these teams may be supported by other teams with responsibility for activities such as media communications and people issues.

2.15 invocation

act of declaring that an organization's business recovery arrangements need to be put into effect in order to continue delivery of key products or services

[BS 25999]

- 2.16 loss**
negative consequence
[BS 25999]
- 2.17 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]
- 2.18 organization recovery management**
process of rebuilding, restoring and rehabilitating the organization following an incident

NOTE This is distinct from, but usually overlaps with, response.
- 2.19 response**
actions taken to deal with the immediate effects of an emergency
- 2.20 resilience**
ability of an organization to resist being affected by an incident
[BS 25999]
- 2.21 resources**
all assets, people, skills, information technology, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that an organization has to have available to use, when needed, in order to operate and meet its objectives
- 2.22 risk**
effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected – positive and/or negative.
NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).
[ISO Guide 73]
- 2.23 risk appetite**
amount and type of risk that an organization is prepared to accept, tolerate or be exposed to at any point in time amount, and type of risk that an organization is willing to pursue or retain
- 2.24 risk assessment**
overall process of risk identification, risk analysis and risk evaluation
[ISO Guide 73]
- 2.25 risk management**
coordinated activities to direct and control an organization with regard to risk
[ISO Guide 73]

2.26 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.

[BS 25999]

2.27 top management

person or group of people who direct and control an organization at the highest level

[BS EN ISO 9000]

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

3 The relationship between recovery management, incident management and business continuity management

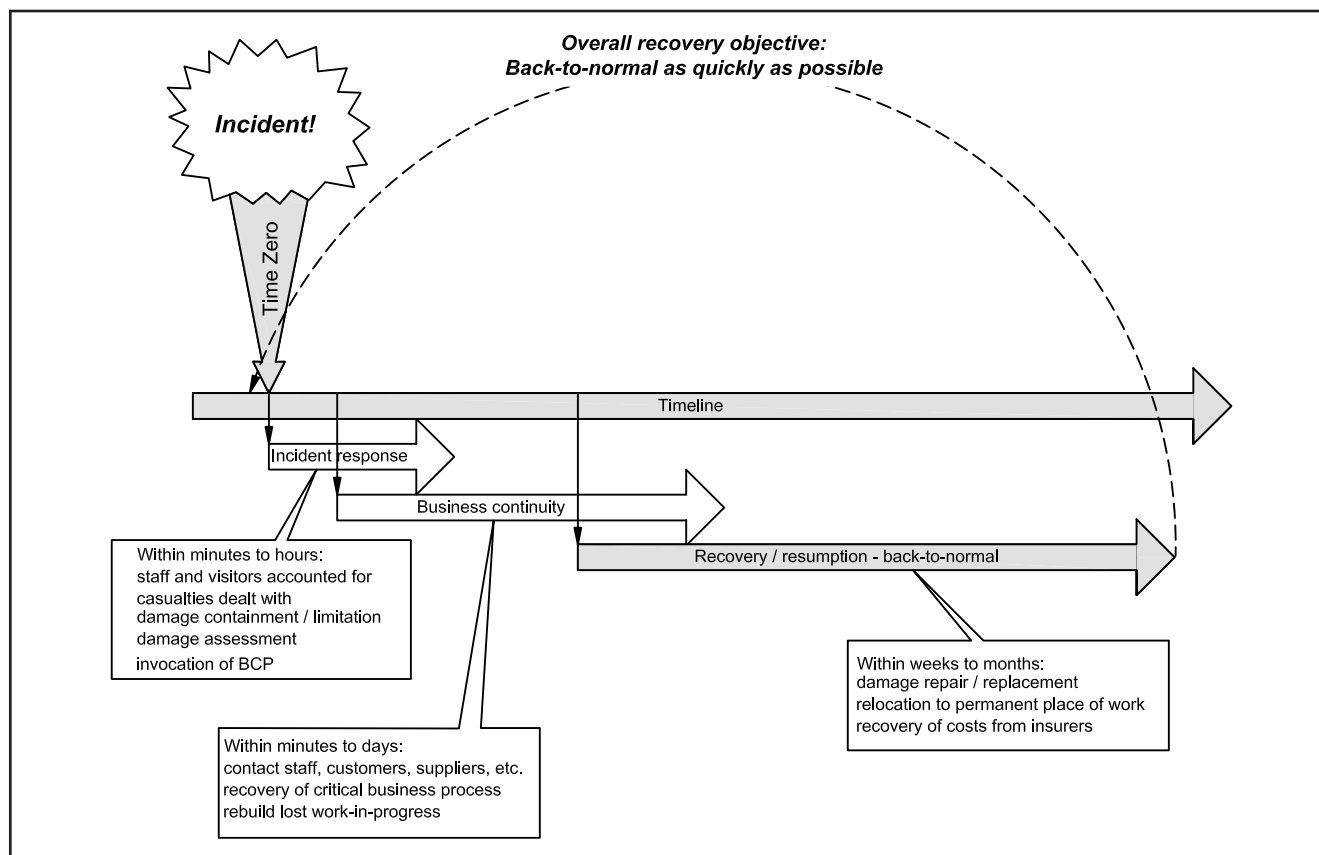
3.1 Overview

Recovery management is the third element [see items 1) to 3)] of the process by which an organization manages the impacts of a disruptive incident on its capability to delivery products and services to its customers, clients and/or patients; to effectively protect its brand, reputation and financial viability; and to ensure regulatory and legal responsibilities are met.

- 1) Incident management is used in the initial stage of an incident to ensure that staff and visitors are accounted for, casualties dealt with, damage to the organization is contained/limited, damage assessment undertaken and business continuity plans activated if appropriate.
- 2) The BCM element comprises the arrangements that ensure the organization restores, within agreed timeframes, the critical activities and processes necessary to recover key products and/or services and communicates with stakeholders.
- 3) Recovery management covers the extended period after BCM arrangements have been implemented up to the point the organization is fully restored to normal, or if appropriate a "new normality", and covers all products and services provided by the organization.

Figure 1 demonstrates the sequence of, and relationship between, the three elements.

Figure 1 The incident timeline



3.2 Recovery management policy

An organization's recovery arrangements should interface with any incident management and BCM arrangements, so there is no requirement to set out a separate policy for recovery management. This PD assumes that effective BCM is already in place within the organization.

The BCM policy statement should be at a high level and cover the basic requirements for recovery management, including:

- the set-up activities for establishing an organization recovery capability (3.3);
- the ongoing management and maintenance of the organization recovery capability during the recovery phase (3.4); and
- the arrangements for standing down the organization's recovery capability once "return to normal" has been achieved.

3.3 Set-up activities

The set-up activities should incorporate the specification, make-up of the recovery team (membership), the build, and the implementation of the business recovery capability.

3.4 Ongoing management and maintenance

The ongoing management and maintenance activities of the business recovery capability should involve updating and communicating arrangements, particularly when there is significant change in premises, personnel, process, market, technology or organizational structure.

As part of the review of its BCMS arrangements the organization should maintain and regularly review the recovery management arrangements.