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.™

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

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

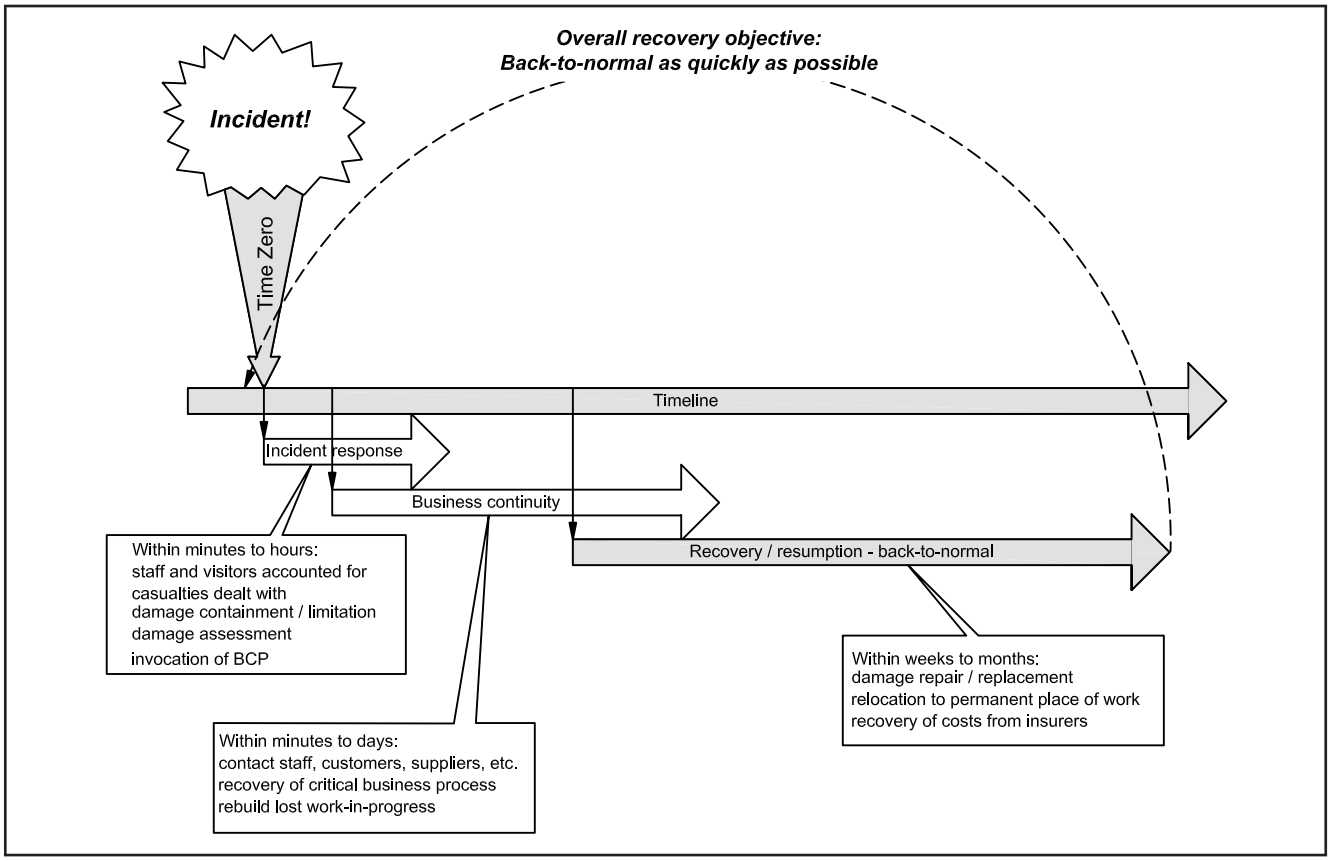
3.1 Overview

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:

a) the set-up activities for establishing an organization recovery capability (**3.3**);

b) the ongoing management and maintenance of the organization recovery capability during the recovery phase (**3.4**); and

c) 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.

4 Establishing an organization recovery management capability

4.1 Initial assessment

As the impacts of an incident on an organization can only be fully assessed after an incident, the focus for the recovery management capability cannot be determined until a full impact assessment has been undertaken. This assessment should be provided to top management, who will determine the scope and timescale of recovery required to return the organization to normal. The responsibility for establishing a recovery management capability may be vested with either the incident management or business continuity team. If this is the case, the responsibility should be included in the roles and responsibilities of the appropriate team.

NOTE Top management may decide to cease all or part of the organization's activities and not to establish a recovery management capability.

4.2 Scope of the recovery management

Top management should determine the scope of the organization recovery to be established by identifying the products and services, locations and facilities that are to be recovered. The organization's risk situation might change in light of exceptional circumstances caused by an incident and the organization could face new risks. As a result, the risk assessment might need to be revised before determining the recovery scope.

In determining this scope top management should also take into account the organization's objectives, financial position, brand and reputation obligations and statutory duties.

The scope of the organization's recovery should clearly define any limitations or exclusions that apply, e.g. geographical or service/product exclusions.

5 Organization recovery planning

5.1 Responsibility for organization recovery arrangements

The organization should identify suitable individuals with the relevant knowledge, skills and authority to develop the organization's recovery arrangements. These nominated individuals may already be members of the organization's business continuity team and it might be appropriate for those individuals to perform both functions. Alternatively, the recovery activities may be performed by a separate team of individuals. It is a matter for the organization to determine its preferred approach, but where a "two-team" approach is adopted, effective communication and coordinated activity between the teams are paramount.

5.2 Invocation

A process should be put in place for invocation as soon as possible after an incident. An important part of recovery management, in the response phase of the incident, is to develop a recovery strategy and liaise with the incident management team (IMT), BCM team, or equivalent, to ensure decisions do not compromise medium to long-term recovery. The relationship of recovery with the business continuity response is important; these should not be viewed as two separate disciplines, but two elements of the same overall response which have to work side-by-side.

A person(s) should be assigned responsibility for invocation arrangements. The most obvious group to undertake this is the IMT. Therefore, those responsible for developing the recovery management arrangements should work closely with those responsible for business continuity/incident management to ensure invocation arrangements are considered in the incident response process, e.g. a standing item on the IMT agenda.

5.3 Recovery strategies

As part of its BCP strategy, the organization ought to have considered the options for the continuity of its critical activities in the short term, e.g. for premises it may have a strategy which involves hiring a backup site from a third-party recovery site provider; for technology, the organization may have implemented remote-access working.

These strategies may still be relevant for recovery management, but they should be reviewed in light of the changing circumstances and longer timeframe of recovery management. For example, if a third-party recovery site is being used, the contract might only allow occupation for a certain period, so that a strategy has to be drawn up to cover the period after expiration.

Top management may decide that all or some of the organization's activities will not be recovered or they may take the opportunity to change the way the organization operates by changing the structure, method or operation, suppliers, etc., thereby creating a "new normality". This decision may be influenced by a number of factors, both internal and external to the organization, e.g. the organization might have learned new things about its priorities, or the risk appetite, market or legislation/guidance could have changed. The changes made by stakeholders (including competitors) might also have an influence on decision-making.

The recovery strategy should be agreed and signed off by top management before long-term recovery commences.

5.4 Recovery management team

As with incident response, the organization should define a recovery management response structure that will enable the rebuilding, restoration and rehabilitation of the organization following an incident. For the purposes of this Published Document this structure is referred to as the recovery management team (RMT) (see Figure 2 for an example recovery management team structure). Once the incident has been contained, the RMT assumes responsibility for the long-term recovery, allowing the IMT to stand down. As part of the planning process, possible representatives on the RMT should be identified and appropriately equipped to perform the role and responsibilities assigned to them.

The education and awareness of the function of the team should be incorporated into, or complement, the organization's programme of continuity management culture, education and awareness (BS 25999-1:2006, Clause **10**).

As the RMT is the strategic decision-making authority for the recovery phase, its key responsibilities include:

a) producing regular situation assessments (see **5.6**);

b) identifying areas where decisions need to be made beyond existing policies and procedures;

c) developing (and reviewing) the overall recovery strategy, including such topics as communications, finance, legal, restoration of infrastructure, staffing, brand/reputation, and changes to company strategies/objectives;

d) ensuring that relevant stakeholders are involved in the development and implementation of the strategy;

e) coordinating implementation of the strategy in a structured and timely manner and monitoring progress;

f) formulating an overall communications strategy that permits the coordination and delivery of consistent messages to stakeholders and the media;

g) establishing appropriate subgroups as required;

h) monitoring financial matters and identifying funding sources; and

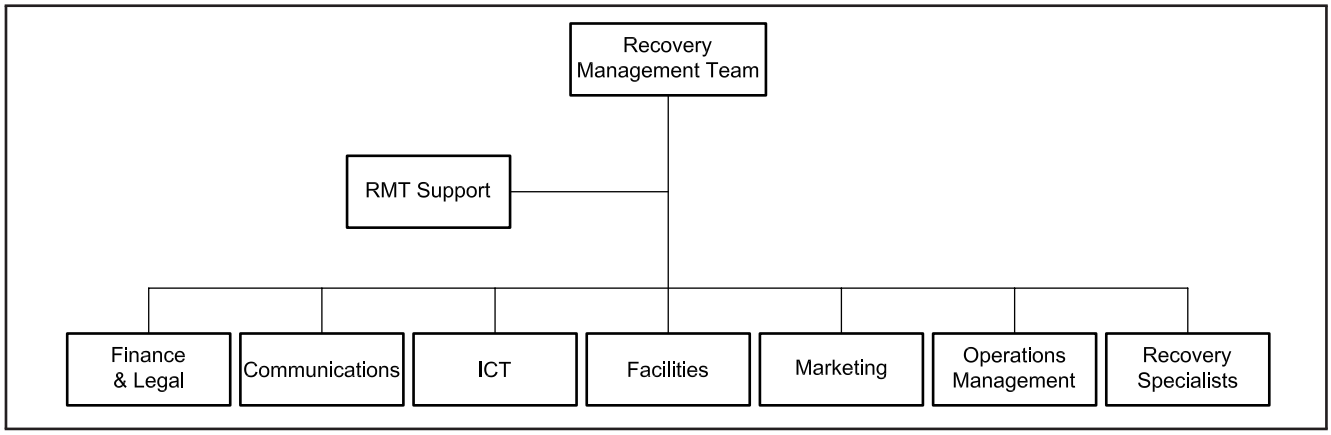
i) ensuring compliance with legal and regulatory requirements.

The size and configuration of the RMT structure depends on the organization and the nature of the disruption. The RMT may be made up of a very small number of individuals or involve numerous subgroups to aid the delivery of the recovery strategy. Possible subgroups are:

1) finance and legal;
2) communications (stakeholders and media);
3) infrastructure (premises and technology);
4) people (staffing levels, health and welfare);
5) products and services (e.g. supplies, key activities and logistics); and
6) brand and reputation.

The RMT may also include external representatives, e.g. architects, local authority planners, loss adjustors, loss assessors, restoration experts, staff counsellors and key suppliers.

Figure 2 **Example of recovery management team structure**



Given the likely length and breadth of the recovery phase effective project management is crucial, along with the visible commitment of top management.

The RMT, as the strategic decision-making authority, needs to think beyond immediate recovery troubleshooting into the medium and long-term recovery phase. To help achieve this, a framework should be put in place to ensure the RMT does not become too focused on the short-term recovery.

5.5 Record-keeping

The importance of record-keeping becomes ever more apparent in the recovery phase as the longer timeframe can lead to those involved in the initial response forgetting why actions were taken, by whom, and how. There is also a risk over time that individuals move on and their knowledge is lost. If the organization intends to make an insurance claim (see Annex B) following the incident it is essential that records and evidence are retained in order to justify any subsequent claim. Finally, but perhaps most importantly, it is possible that there will be investigations into the organization's response following an incident, and possible litigation. Good record-keeping allows the organization to provide evidence and justification for particular actions.

Those responsible for developing the recovery management arrangements should work closely with those responsible for business continuity and incident management plans, to ensure a structured and consistent approach to records management. This will largely be defined by the nature of the organization, but some of the issues to consider include:

a) the system to be used:
    1) Will this be different to the usual document management system?
    2) Who should have access to it?
    3) Are different levels of access required?
    4) Will people need to be trained on it?
b) whether template documentation is to be provided for:
    1) recording decisions taken, why, by whom and when;
    2) recording actions taken, why, by whom and when;
    3) recording minutes of meetings;
    4) recording key conversations; and
c) storage of documentation/communication received from external parties.

5.6 Situation assessment

A template should be developed so that, during the recovery phase, the RMT can undertake regular assessments to establish the current situation and identify areas where adjustments to the recovery plan might need to be made. In the planning phase, a mechanism should be established to ensure that the RMT receives regular updates on:

a) stakeholders;
b) staff;
c) premises and equipment;
d) technology;
e) information;
f) supplies;
g) finance, including insurance;
h) brand and reputation; and
i) relevant media and counterparty activities.

The questions this assessment may address include the following.

1) Is the organization meeting its duty of care?
2) Is the organization communicating with relevant stakeholders?

3) What key resources (premises, equipment, technology, information, staff and finance) support the organization's critical activities?

4) Is the availability of other resources becoming critical as the situation develops?

5) Are these all operating normally?

6) If they are not operating at full capacity are they operating at a suitable capacity given critical activity requirements?

7) If not, what immediate actions are being taken to resolve this issue?

8) Where resourcing is operating at an acceptable reduced level, how long can this continue before it begins to impact on critical deliverables? What actions are being taken to mitigate the impact of this?

9) Where resourcing is operating at full capacity, are there risks that this could be impacted in the near future, and what action is being taken to mitigate this or any negative consequence?

10) Are current continuity arrangements sustainable? If not, what action is being taken?

11) What has been reported/said in the media?

12) Considering the preceding points, are there any:

    i) knock-on impacts (either now or that are likely to arise in the near term) to other areas of the organization?

    ii) wider implications for the organization?

    iii) wider implications for stakeholders?

The situation assessment should inform the strategic decisions that need to be taken by the RMT. Some of these may include:

- redirection of resources;
- re-evaluation of priorities;
- re-evaluation of policies/strategies; and
- communication decisions.

6 Actions on implementation

6.1 Strategic implementation

In implementing the recovery strategy as agreed by top management the RMT should consider the following.

a) *Products and services.* Do products/services need to be discontinued and/or new ones brought in?

b) *Reassembling infrastructure.* Do new sites need to be acquired? Does new technology need to be implemented?

c) *Reassembling staff.* Do new staff/skills need to be acquired? Do staff need to be moved? Are changes to staff levels required?

d) *Logistics.* Do new supplies need to be sourced? Do new methods and routes of transportation need to be developed?

e) *Continuity arrangements.* Do new continuity arrangements need to be put in place?

f) *Finance.* How are actions going to be financed?

g) *Legal.* What are the legal and regulatory implications of any changes?

6.2 Tactical implementation: Issues for consideration following an incident

6.2.1 People

Any incident which results in the implementation of business continuity arrangements will cause disruption to people, including the organization's staff, customers, contractors, partners and the community in general. The greater and longer the disruption, the greater the impact upon people.

The organization should be aware of duty of care and statutory/contractual requirements to protect people.

To achieve an effective recovery the organization should ensure that appropriate human resource (HR) policies and procedures are developed as part of the overall recovery management arrangements.

The HR policies and procedures should cover two distinct areas:

a) managing people during the recovery phase; and

b) supporting people after the organization has recovered.

a) Managing people during the business recovery phase

On invocation, it is important to ensure that the HR policies and procedures recognize and address the impact disruption will have on people affected by the incident. Failure to acknowledge and manage the issues can lead to resentment and demotivation, and hence a fall in the organization's capability at the time when it is most vulnerable.

The following issues should be considered:

1) changes to working environment and social spaces;

2) disruption of "social working" groups;

3) impersonal working space and difference in technical presentation;

4) disrupted travel arrangements;

5) disrupted and extended working hours;

6) catering arrangements;

7) stress of working away from normal location;

8) changes to, or sudden introduction of, home working arrangements;

9) access to support areas, such as Personnel, etc.;

10) problem resolution: work and personal;

11) increased pressure above that normally experienced;

12) communications to keep staff informed;

13) legal arrangements:

    i) flexibility of employment contracts;

    ii) pay and compensation arrangements; and

    iii) health and safety arrangements;

14) maintaining employees' support during a lengthy period of disruption;

15) liaising with staff representatives/associations;

16) cultural and religious requirements; and

17) disability access and requirements.

b) Supporting people after recovery (business as usual)

The effects on people of a major incident and subsequent disruption do not end at the point when the organization has fully recovered, albeit to a new normality. For many the affects will last for a considerable time. It is therefore essential that the HR policies and procedures are put in place to respond to the needs of employees over an extended period.

Policies and procedures should be developed which take account of:

1) the effects of trauma on staff:
    i) identifying the signs;
    ii) prevention;
    iii) treatment (counselling);
2) ongoing employee support;
3) families support; and
4) memorials and donations.

It is important to recognize that members of the incident, continuity and recovery teams will be under considerable stress. This will be greatest during the early stages of the incident. The HR policies and procedures should therefore address the specific needs of these team members.

All policies and procedures developed for recovery have to comply with the appropriate legal and regulatory requirements, and have to continue to recognize equality and diversity issues.

NOTE PD 25111 provides detailed advice on managing people during and following a disruptive incident.

6.2.2 Premises

6.2.2.1 General

Following an incident that affects the organization's premises, there are a number of areas to consider, including access to premises and equipment.

6.2.2.2 Access to premises after an incident

Access to premises (including sites and buildings) after an incident might be disallowed by the authorities, or could be restricted due to structural problems, contamination or emotional and other considerations (see Annex A). An organization's buildings can be affected by smoke and fumes from fires on other organizations' premises, especially if the fumes are deemed toxic and require evacuation measures. Recovery management arrangements should take this into consideration. It might be necessary to seek expert advice and to provide appropriate personal protective equipment.

Any change to the premises during restoration could require planning permission from the appropriate authorities and this can be subject to considerable delay. Planning permission might even be needed to restore a building to its previous state if the zoning of the area has changed since the building was built.

Temporary accommodation may be provided under business continuity arrangements, but the RMT has to determine if the type and size of temporary accommodation available can sustain the organization's activities over the period of recovery. It is possible that contractual arrangements with third party suppliers are time-limited. In this case, the RMT has to ensure that suitable alternative accommodation is identified and made available before the third-party contract expires.

The use of alternative accommodation, temporary or permanent, can impact staff [see **6.2.1**a) and PD 25111]. Other issues to consider when using alternative accommodation include the following.

a) Is the location suitable for the organization's activities (e.g. easy access for customers)?

b) Are there restrictions on what type of business can operate from the premises?

c) Can supplies be delivered to the new location?

d) Can local businesses meet the organization's requirements (e.g. site maintenance, catering)?

e) Are there other tenants on the site?

f) What physical security arrangements are required?

g) Are there appropriate levels of fire protection in place?

h) What hazards exist in the neighbourhood (e.g. flooding, chemical plants)?

i) What are the arrangements for mail delivery/collection?

j) Is there sufficient telecommunications network capacity?

k) Is there sufficient utility provision/capacity at the premises?

l) Are existing software licences restricted to a specific location?

6.2.3 Equipment

6.2.3.1 Salvaging damaged equipment

There are several significant areas to be considered with regard to salvaging damaged equipment and ensuring that urgent protective action is taken to minimize adverse effects on affected items. Swift action is required to protect equipment from the immediate effects of the damage.

Key points to remember include:

a) restoration, where possible, can be much quicker and less expensive than obtaining new items;

b) restored equipment is already set up and configured for the organization's exact uses;

c) insurance for written-down value could cover restoration, but not replacement;

d) high humidity can result in fungal attack (e.g. rot and mould) as a wet building slowly dries;

e) after a fire, the materials used in fighting the fire (water, halon, foam, dry powder) will need to be dealt with;

f) air conditioning intakes close to the top of stacks can draw fumes back into the building and circulate them to parts which were previously undamaged;

g) corrosion and contamination can travel and persist inside the air conditioning system and the ceiling and floor voids;

h) hydrochloric acid produced by the combustion of PVC in a fire readily corrodes exposed metal surfaces; removal of the acid is enough to prevent further corrosion; and

i) ongoing damage from wind and rain.

6.2.3.2 Control

Control of any recovery and restoration operation is essential, whether it is big or small. Leaving equipment in a contaminated state or in environmentally unfriendly conditions, even for a short time, can preclude the equipment ever being restored to a satisfactory condition. Similarly, inappropriate handling of equipment can preclude its restoration.

There are likely to be several parties in attendance at an incident, and the question of who should do what, how and when has to be determined at an early stage. Whatever incident has occurred, immediate measures should be taken to limit material damage as soon as access is granted to the site. Measures to limit business interruption can begin even before access is granted.

Besides the reclamation of equipment, there is the reclamation of structures, mechanical plant, electrical/electronic plant, data and documents, for which various specialist cleaners or recovery and restoration experts may be appointed. The control of individual functions, and the coordination between functions, is complex but absolutely necessary.

No single individual is likely to have adequate knowledge of all business activities, all aspects of the physical site and all reclamation techniques, and it is unlikely that any one person will have a mandate to take all decisions.

A person with the appropriate skills and knowledge should be appointed to oversee and control all salvage operations. This person should be in daily contact with all relevant parties, such as insurance loss adjusters, specialist cleaners, contractors, builders, site security, police, forensic scientists and, of course, the organization which has suffered the damage. Each of these other parties should nominate a contact person having appropriate authority. On a very big recovery it may be appropriate to have a daily management meeting.

It is not essential for the person responsible for salvage operations to be from the organization which suffered the damage, though the site building services manager may be a good candidate.

Some organizations pre-appoint a specialist restoration company to provide professional restoration measures in the event of a damaging incident occurring. Their services can cover:

a) damage assessment;

b) decontamination;

c) drying of buildings;

d) cleaning of buildings and equipment;

e) odour neutralization; and

f) documentation of damage.

6.2.3.3 Recording

It is important to implement a process for recording work undertaken and equipment removed from the earliest moments of the recovery to prevent loss and deliberate theft. Details of the equipment, data and documents taken to and returned from off-site recovery and restoration specialists have to be recorded in full.

If appropriate premises can be obtained, e.g. a vacant warehouse, it might be possible to group the items recovered from damaged premises on a room-by-room basis. This enables easier identification and restoration of equipment and other resources by the appropriate department or employee.

6.2.4 Information

6.2.4.1 IT-related assets

The recovery process should identify the status of IT assets. Critical information will generally be covered by the routine backup procedures performed as part of the organization's business continuity arrangements, but important information might need to be recovered from other media. Examples include:

- legal documents;
- staff members' personal documents (e.g. personal contact lists); and
- transient documents, such as invoices, delivery notes and orders.

There are different recovery considerations for different types of documents.

a) It is very difficult in practice to safeguard or recover personal documents, but their loss could impede recovery. Information about such documents should be dealt with by personal continuity methods.

b) For transient documents, it is worth structuring the normal workflow to capture the information in electronic form as soon as possible after these enter the organization (and, of course, to back up the electronic data). Counterparties to contracts might be able to provide copies.

c) Microfiche and microfilm are susceptible to softening through contact with water and to smoke or chemical attack, as well as fire. The main hazard is mechanical damage suffered as a result of unsupervised transfer. This is especially true after softening and/or sticking has occurred through water damage.

Certain general observations can be made:

1) recovery from clean, undamaged media is easy;
2) recovery from damaged media is expensive and slow;
3) unskilled attempts to recover data cause more harm than good;
4) data stored on magnetic and optical disks are often recoverable even when the computer equipment is severely damaged; and
5) magnetic tapes are almost always readable if the tape itself is intact.

Issues that the RMT has to consider include the following.

i) Do-it-yourself recovery efforts causing further damage. Do external experts need to be brought in to assist the recovery?

ii) Knowing which items of media contain the data needed. Can the backup schedule be found to indicate where the backups are held?

iii) Physically retrieving the media from a damaged building. Provide the salvage team with instructions for location of backup tapes and keys to the fire-proof safe.

iv) Access to data can be restricted by:

- deliberate or accidental erasure;
- off-site backup being incomplete or out-of-date;
- malfunction of the equipment which controls access to the data;
- physical distortion of tapes or disks caused, for example, by heat or age; and
- contamination of recording surfaces by chemicals or dust.

v) Problem of being able to run, for example:

- application hardware key linked to application software key;
- software protected by dongles;
- old computer models;
- obsolete media formats.

vi) Scrambling of the information, where the information is still recorded but the index to where it is stored has been lost.

vii) Access and ownership rights.

6.2.4.2 Paper documents

6.2.4.2.1 Recovery considerations and priorities

The major issue with document recovery and restoration is that the initial handling determines the degree of success of recovery work.

It is necessary to obtain professional advice and help as soon as practicable.

Whatever the category, the aim behind all document recovery is to produce documents which can be read, handled and stored.

For all of the forms of paper documents, the RMT should decide which parts of the organization they are going to recover first. Decisions on what products and services to recover first should be based on:

a) BIA data;

b) the BCP which should identify those documents whose recovery is vital to the organization and those which are not; and

c) the priorities agreed through the business continuity phase of the incident.

The RMT should confirm that the BCP list of vital records is up-to-date and instruct the salvage team to recover these items.

This ensures that the salvage team can concentrate on vital documents only and that the organization does not waste money on the recovery of non-vital documents. When there is a large volume of paperwork to deal with, then bound documents should be tackled before loose documents.

It might not be possible to access the building, in which case it will be necessary to instruct a recovery and restoration organization (so that office plans are vital).

Recovery is an unpleasant job, as the documents to be recovered can be dirty, wet and smelly. In addition, there are potential health risks for people performing a recovery role, including:

1) polluted water;

2) dangerous dust, e.g. toxic chemicals;

3) spores; and

4) glass fragments from explosions can be captured in the folds of paper, particularly loose papers left lying on desks.

This means that protective equipment is needed for the salvage team and anyone else who will be handling damaged paper.

6.2.4.2.2 Sources of damage to paper documents

a) Fire

The particular issues surrounding papers damaged or contaminated by fire are:

1) charred documents are fragile and need very careful handling;

2) documents can absorb water used in firefighting, so there could be water damage;

3) both paper and ink are attacked by the chemicals present in or near a fire and this can stain documents; and

4) smoke particles are likely to cause staining and warping, if not removed, because of the acids which can be absorbed by the paper surface.

b) Flooding and water damage

The particular issues surrounding papers contaminated by water are:

1) wet paper is heavy and easily damaged;

2) sheets have to be dried individually;

3) mould can appear within 48 hours in moist conditions if the temperature is above 6 °C, and this will cause marks, so quick decisions are needed as to recovery;

4) it is easy to reassemble documents incorrectly; and

5) water-soluble ink can be washed away.

6.2.4.2.3 Recovery considerations for particular documents

There are different recovery considerations for different types of documents.

a) Legal documents need to be retained, e.g. contracts should be held in hard and electronic formats.

b) A library could contain valuable books and art.

6.2.5 Supplies

The organization should understand how the business recovery phase of an incident will impact upon the supplies required to support the delivery of activities.

Supply requirements during a recovery can differ from those needed to maintain the delivery of the organization's activities during normal operations. New supplies or sources of supply might be required, additional resources drawn upon, or existing supplies cancelled or allowed to become exhausted against a timescale different to that to which organization usually operates. The organization should be aware of these issues in preparing its business recovery arrangements.

The organization should ensure that any supply requirements are met to achieve an effective recovery of the business in the event of an incident. Some of the questions an organization needs to address include the following.

a) What supplies does the organization need to continue to receive following a disruption to support the continued delivery and recovery of critical activities?

b) Will the recovery create a need for any new supplies? Where and how can the organization source and finance these new supplies?

c) Will the organization be required to provide training to staff to ensure they are able to use any new supplies effectively?

d) Will the use of new supplies or suppliers have implications for the organization's quality management arrangements?

e) Will a change in the amount and type of supplies stored by the organization lead to a shift in the organization's duties under Health and Safety regulations [e.g. the Control of Substances Hazardous to Health

Regulations 2002 (COSHH), as amended [1], and the Control of Major Accident Hazards Regulations 1999 (COMAH) [2]].

f) Is there an alternative address to which supplies are to be delivered?

g) What existing supplies can be exhausted or cancelled? Will the organization run into any contractual issues if the services of a current supplier become unnecessary as a result of the incident?

h) Will interim supply arrangements have permanency following the successful conclusion of the recovery?

i) Will safe disposal arrangements need to be developed to discard unwanted or unused supplies?

6.2.6 Communication with stakeholders

The organization should ensure that it maintains the confidence of all its stakeholders through communication updates highlighting successful progress in maintaining and resuming business operations after an incident.

The organization should ensure that all communications are current.

The organization's communication should be supported with evidence.

Staff communication should also be timely as many employees have access to television news or the internet at work. If the communication is delayed they will become more concerned. In addition, having a current, accurate internal news source enables staff to maintain confidence in the organization, its management and the process it is using to handle the incident.

6.2.7 Resource allocation

The organization should ensure that it has appropriate plans for the allocation of any additional resources to cover its needs during recovery and its initial production resumption phase. It should ensure that it has easy access to any hard-to-acquire resource, either by stockpiling or by dedicated contractual arrangements. After resumption to "normality" the organization should assess its resource deployment to validate the allocations specified in the plans and to update them based upon its experience.

In addition, the organization should ensure that it has a purchasing capability, which may be made up of staff not required for initial operation resumption, in order to buy any items the organization requires but has omitted from its plans.

6.2.8 Cash flow: receipts and payments

Examples of the documents the organization might have to obtain during the recovery phase include the cheque book, paying-in book, manual purchase order forms, pro-forma key suppliers letter, pro-forma staff advances letter and list of business-essential creditors.

The organization should also maintain invoice and payment management; ensure that all purchases are recorded; retain bank account reconciliations; and set up a manual accounting and petty cash process.

It is essential for the organization to keep track of any expenditure incurred as a result of an incident as some insurance policies might reimburse such costs. This also allows the organization, as part of the post-incident process, to understand the true cost of the incident.

6.2.9 Finance and liquidity

Recovery of an organization's activities following a major disruption can place considerable strain on the financial viability of the organization. Those responsible for the organization's finances need to ensure they have access to sufficient funds to support the recovery. It is important to contact the organization's banks and investors to apprise them of its financial status

It should be recognized that insurance payouts can be delayed if there is any dispute surrounding a claim.

It is important to determine the value and liquidity of the organization's investment and other assets to evaluate its ability to continue to fund the organization's operations and remain in capital compliance. If it is determined that the organization is unable to meet its obligations to those counterparties or otherwise continue to fund its operations, the organization should request additional financing from its bank or other credit sources to fulfil its obligations to its customers and clients. If the organization cannot remedy a capital deficiency, it should file appropriate notices with its regulators, etc.

7 Return to normal operations

Once the organization has returned to normal or to a "new normality" the requirement for recovery management capability ends. In standing down the capability the organization should ensure that appropriate records and documents are retained and a debrief should be undertaken to identify lessons from the recovery process which can be used to improve recovery management arrangements.

Consideration should be given to publicly acknowledging the work done by the recovery team to enabling the organization to return to normal.

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

a) **Structural problems**

If a building appears to be dangerous, access could be denied by the authorities until emergency strengthening work is carried out.

High wind can pull window panes and cladding from a damaged building. Access might be denied during high wind and anyone entering the building will need appropriate personal protective equipment.

b) **Contamination**

Potential contamination on the premises needs to be taken very seriously. Cutting corners with decontamination can be a very expensive mistake.

- **Asbestos.** Asbestos-containing materials are used in many buildings for cladding, insulation, partitions or roofing, and these can be broken up and spread around by fire and the water used to extinguish a fire. It is then necessary to test for asbestos contamination, particularly if the buildings were built or re-clad between 1965 and 1985, and to clear any trace of blue (crocodilite) or brown (amosite) asbestos before anyone enters the premises. It takes at least three or four days for a registered asbestos removal contractor to tent a contaminated area, remove the asbestos and have it independently analysed.

  Note that in some places there could be a legal duty to notify the Health and Safety Executive about any asbestos found.

  Expert advice might be taken on whether it is better to remove the asbestos or leave it undisturbed.

  It might also be appropriate to check the asbestos register.

- **Polychlorinated biphenyls (PCBs).** PCBs were extensively used as coolants in electrical switchgear and transformers, so might well be present in older equipment. If the equipment is damaged in a fire, the PCBs can be spread all over the building with the smoke. PCBs are highly carcinogenic, so decontamination is essential before anybody enters.

- **Other chemicals/substances.** Tests need to be made for traces of any dangerous chemicals and substances which are known (or suspected) to be on-site. Also, many ordinary chemicals can produce dangerous cocktails in a fire after mixing through damage, breakage or leakage of containers.

- **Dirty water.** There are a number of water-borne hazards to health, particularly if water is contaminated by chemicals or sewage, e.g. Hepatitis A, Typhoid or Weil's disease (leptospirosis icterohaemmhagica). It is almost inevitable that flood water will become dirty or foul; therefore, people working in these conditions have to be protected by personal protective equipment.

c) **Death or serious injury**

If there is widespread distress in the organization as a result of deaths or injuries, it can appear insensitive to be too eager to restart operations.

d) **Utilities**

The organization's staff could be denied access to the site if gas leaks or downed power cables present a danger to the public until the utility company has dealt with the problem.

e) **Type of building**

The type of building occupied by the organization can result in some special access risks (see Table 1).

Table A.1 **Access issues arising from type of building**

High-rise buildings	Industrial buildings
Multiple occupancy. The organization's staff might have to queue with other tenants for a short time slot in which to retrieve essential items	**Asbestos.** Asbestos cement sheeting is very common on factory roofs and cladding, and can become friable after fires.
Falling glass. There is a higher risk of falling glass with high-rise buildings, and a bigger problem replacing glass before the organization can use the building again. Anti-shatter film can reduce the potential for damage and injury.	It is also particularly important to look for asbestos insulation and lagging on pipework, especially in places which are hard to reach, such as inside service ducts.
Power failure. If there is no power the lifts cannot be used. How will staff walk up 20 floors or more? What can they carry down, and how?	

Annex B (informative) Insurance

B.1 Business interruption insurance

Insurance can provide financial compensation for loss of assets, increased costs of working, business resumption and protection for associated legal liabilities. However, it will never compensate for all of the losses associated with a disruption, such as the loss of customers and opportunities, reduction in shareholder value or loss of reputation and brand image. It is important, therefore, that the continuity options selected by the organization are consistent with the covers available in the marketplace and with its insurance purchase decisions.

Business Interruption (BI) insurance is most closely associated with BCM, but it is important to note that, typically, this only provides protection for the loss of profits and continuing fixed expenses resulting from a break in the commercial activities of the organization due to the occurrence of an already insured material damage loss. The indemnity periods in such BI policies are the periods during which cover is provided for disruption to the organization following the occurrence of an insured event, and are usually determined by the length of time that an organization believes it will take to recover effectively from such an event (or the affordability of such cover). Invariably, organizations with effective BCM in place are capable of returning to normal operations more rapidly than those without BCM and are therefore able to choose shorter (and less expensive) indemnity periods and/or reduced sums insured.

A frequently overlooked component of BI insurance is "increased cost of working" (ICOW). This provides cover for additional expenses incurred in order to mitigate the loss. Typical BI policies contain clauses which include some ICOW up to an "economic limit", but additional ICOW cover is often added so that the costs of implementing a planned recovery (such as temporary accommodation, transportation, additional payroll, invocation charges) can be reclaimed. Thus, ICOW can be viewed as a means of funding certain costs associated with the implementation of a BC response to a disruption.

Some insurers offer cover for a range of BI extensions, such as failure of a supplier to provide contracted products or services and utilities failures. However, such covers are quite limited in scope and their availability and cost could prove problematic.

Generally, insurers are concerned about the resilience of an organization and, as such, take into account the existence of a BCM programme, but this is only one factor in determining a risk profile and insurance costs.

For small to medium-sized enterprises (SMEs), insurance can also provide some useful financial support following the loss of named key individuals due to death, injury or other forced absence from the business.

B.2 The role of the loss adjuster

Loss adjusters are independent claims specialists employed to investigate, negotiate and agree the conclusion of insurance claims on behalf of insurers and policyholders.

B.3 The initial stages of a claim

Once a loss adjuster has been appointed, either by the insurer or by the broker on behalf of the insurer, their role is as follows.

a) Establish the exact cause of the loss, instructing forensic scientists to carry out detailed investigations, if appropriate. The cost of this is borne by insurers.

b) Advise the insurer and the policyholder about policy coverage and whether or not the loss is covered by the policy terms and conditions, and seek to establish whether or not policy terms, conditions and warranties have been complied with.

c) Check the adequacy of sums insured.

d) Identify and protect the position and rights of both the insured party and the insurer in respect of any potential recovery against a third party.

e) Provide advice and guidance about the claims process and the steps to be taken to progress a claim. This may include the appointment of other specialists such as architects or structural engineers.

f) Establish a reserve, the loss adjuster's realistic expectation of the likely extent of all costs following the initial investigation. As the claim progresses, the reserve might alter.

B.4 Assisting a loss adjuster

It is in the best interests of the insured party to provide a loss adjuster with full cooperation and assistance. This allows a claim to be settled in a quick and effective manner.

Where there has been structural damage to the premises and equipment, it greatly assists the loss adjuster if they are provided with:

a) drawings/plans/maps of the site;

b) asset registers and equipment locations;

c) if there is a landlord/lessee relationship in place, a copy of the lease; and

d) any pre-incident photographs of the premises.

Where there has been damage to stock and work in progress the loss adjuster ought to be provided with:

1) schedules of work in progress;

2) order books;

3) lists of materials and finished goods held in stock; and

4) stock values: copy purchase invoices and additional labour/plant costs for work in progress.

B.5 Next steps

Following the initial investigation, the loss adjuster agrees with the insured the next steps. These usually involve:

a) the compilation of a specification for the scheme of repair/reinstatement works;

b) obtaining competitive tenders based upon the agreed specification; and

c) a review of tenders and confirmation of which company is to be used.

If the works are complex and likely to take a number of months to complete, the loss adjuster usually submits interim reports to the insurer and requests that staged payments be made. If it is appropriate, the loss adjuster can arrange for the insurance company to pay the contractor directly, provided that the insured party agrees to this and completes a mandate authorizing this.

B.6 Recoveries

If investigations reveal that a third party is either partially or wholly responsible for damage, the insurer collates the details and considers whether or not there is a sufficiently strong case to pursue an action. The policy provides the insurer with the right to pursue recovery from negligent third parties in the insured party's name. If the insurer chooses to exercise the right to pursue recovery from negligent third parties, the insured party will be kept informed of progress. It is also possible that the insured party could have the opportunity to join the action if they have suffered an uninsured loss. The insured party ought to provide insurers with as much assistance as possible if they choose to subrogate a claim. This is partly because any recovery gained will ultimately be offset against the total settlement amount. This will, in turn, improve the insured overall claims experience and loss ratio.

B.7 The role of the loss assessor

A loss assessor may be appointed by the insured party when they need to submit a substantial or complex claim. In certain instances the assessor's fees might be recovered as part of the claim settlement, but only when the policy has been extended at the outset (at extra cost) to deal with this contingency.

Loss assessors handle all aspects of the claims process, including;

a) meeting with insurance company representatives or their appointed loss adjusters;

b) preparing the claim;

c) negotiating the best possible settlement of the claim; and

d) dealing with cases where a claim has initially been declined by the insurance company or where problems or delays have occurred in agreeing settlement.

Bibliography

Standards publications

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

PD 25111, *Business continuity management – Guidance on human aspects of business continuity*

BS EN ISO 9000, *Quality management systems – Fundamentals and vocabulary*

ISO/IEC Guide 73, *Risk management – Vocabulary*

Other publications

[1] GREAT BRITAIN. The Control of Substances Hazardous to Health Regulations 2002 (COSHH), as amended. London. The Stationery Office.

[2] GREAT BRITAIN. The Control of Major Accident Hazards Regulations 1999 (COMAH). London. The Stationery Office.

This page deliberately left blank

This page deliberately left blank

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™