Business and IT Continuity:

Overview and Implementation Principles

(Parts of this report constitute the deliverable defined in the ENISA Work Programme 2007 as "Report on Business Continuity risk analysis methods for SMEs")

Conducted by the
Technical Department of ENISA
Section Risk Management

in cooperation with:
Janet Beattie et al. - Glen Abbot Ltd.

February 2008

Executive Summary

This report is an ENISA deliverable in the area of Risk Management as foreseen in the ENISA Work Programme 2007 (item 2.2.4). The report elaborates on continuity risks and contains an overview of numerous Business Continuity models. The report addresses open issues identified in previous ENISA reports on Risk Management [ENISA RM]. Moreover in various events and discussions the need for an overview on Business Continuity has been communicated by both experts and non-experts.

The field of Business Continuity has been attracting increasing attention because it greatly contributes to the quality of services and to the resilience of systems and processes. Many good practices, regulations and recommendations underline the importance of Business Continuity for all organisations, especially for those which rely on IT systems to implement their business processes.

The purpose of this document is to provide information on and generate awareness of the important topic of Business and IT Continuity. Our main objective is to offer solutions to the following general problems encountered in the area of Continuity Management:

- missing overview on the contents and structure of methods, tools and good practices;
- absence of a "common language" in the area of IT Continuity Management to facilitate communication among stakeholders and
- lack of surveys on existing methods, tools and good practices.

Based on the overview presented in this report ENISA is going to:

- *Generate an inventory of methods, tools and good practices*: similar to the work on Risk Management / Risk Assessment inventory, this deliverable is the basis for an inventory in the area of Business Continuity methods and tools. A first version of the inventory will be generated during 2008.
- *Perform a survey on the usage of continuity measures in e-communication*: during 2008 ENISA plans to survey e-communication providers in order to assess continuity controls and technologies used to guarantee the resilience of networks.
- *Develop an approach to IT continuity that can be used within micro enterprises and SMEs*: in the future ENISA plans to develop an approach to Business and IT continuity that can be utilized by non experts within small enterprises.

Contact details: ENISA Technical Department – Section Risk Management
Dr. Simone Balboni, National Expert Seconded by the University of Bologna and
Dr. Louis Marinos, Senior Expert Risk Management
e-mail: RiskMngt@enisa.europa.eu

Contents

Figures

Tables

1 Introduction

This report has been written to fulfil the objective of the European Network and Information Security Agency (ENISA) to: "Promote Risk Assessment and Risk Management methods to enhance the capability of dealing with network and information security threats" [ENISA Regulation]. As continuity risks are considered to be amongst the most important faced by many organisations and businesses, ENISA decided to invest its efforts in the promotion of methods, tools and good practices for continuity management. As the main focus of the Agency is on Network and Information Security, the context of this work will be on Information Technology and closely related areas.

Business processes are increasingly linked together via information and communication technology. This is accompanied by increases in the complexity of the technical systems and with a growing dependence on the correct operations of the technology (BSI Standard 100-2: 2005) [IT Grundshutz].

Through an organisation's Risk Management process[1] it is likely that continuity risks will be identified. These risks can be managed to reduce their likelihood and/or impact, but it may be necessary to have plans in place to deal with the effects of the risk should it occur.

Business Continuity is the term applied to the series of management processes and integrated plans that maintain the continuity of the critical processes of an organisation, should a disruptive event take place which impacts the ability of the organisation to continue to provide its key services. ICT systems and electronic data are crucial components of the processes and their protection and timely return is of paramount importance.

Business Continuity (BC) is now recognised as an integral part of good management practice and corporate governance.

The need for Business Continuity has expanded in recent years following incidents (malicious, terrorist attacks and environmental disasters) which have disrupted large enterprises and forced many smaller ones to cease trading. Government legislation e.g. Sarbanes-Oxley [SOX] in the US, Bill 198 in Canada [BILL 198] (both target the private sector), the Civil Contingencies Act (2004) [CC ACT] in the UK and the Presidential Decision Directive 67 [PDD 67] in the USA (necessitating the need for Continuance of Government), state the requirement for Business Continuity although they do not detail a particular methodology.

Regulatory bodies also influence the requirement for BC, for example the regulations of the Finance Services Authority [FSA] in the UK state the acceptable period for call centres to be unavailable, letters unanswered, etc. There are many similar financial bodies throughout the world, each have their own regulatory requirements. In Australia this led to the requirement for APS232 [APS 232].

Financial benefits are also evident as an incentive to widen the practice of BC. In some parts of the western world, insurance companies offer discounts when BC plans are in place. With Business Continuity Management (BCM) penetration lower than 20% in Japan, despite the frequent natural disasters, the Development Bank of Japan offer a Disaster Prevention Loan with reduced interest rates, to be used to plan BC programmes, to prepare facilities to reduce the effects of a disaster or to provide backup ICT services.

[1] See [ENISA RM] and in particular http://www.enisa.europa.eu/rmra/rm_process.html

Reflecting this upsurge in interest there are a number of emerging standards (and overlapping standards) in the area of Business Continuity Management. With a choice of different terminologies and areas of overlap a company must adopt one specific methodology and apply it throughout the organisation.

Factors such as human resources, financial and technological limitations and regulatory constraints will shape the strategy and drive the eventual solution. With an increasing reliance on ICT in all areas of our lives this becomes an important part of the solution. The term "Disaster Recovery (DR)" has over many years migrated from its true meaning within business to a response to an ICT problem or failure. ICT departments provide DR Plans to recover important systems within a reasonable timescale in accordance with a Service Level Agreement but this rarely meets the end-user's expectations based on their BC requirements.

These issues and overlaps are being addressed in the latest standards and frameworks but this evolves into a complex web of procedures and policies e.g. ITIL [ITIL] is a Framework for Information Technology (IT) infrastructure with v2 being divided into 9 areas; while the idea is to utilise the areas relevant to the organisation, the existence of relationships among the areas means that taking one and not another could create deficiencies. This is also reflected in standards, where the relationships are now starting to be defined. For example, PAS77 IT Service Continuity Management [PAS 77] acknowledges the need for Business Continuity Management (BCM) before IT Services Continuity (ITSC) plans can be developed. It also states that if there is no BC in place then a subset of the Business Impact Analysis (BIA) must be completed in order to understand the business requirements and to align IT services to business requirements.

Emerging standards (and existing ones which are evolving) reflect their roots and so the target audience for each must be known to best understand their basis. The American standard NFPA 1600 comes from the National Fire Protection Association [NFPA] and is the standard on Disaster and Emergency Management and Business Continuity Programs. Early versions are more about saving the environment than IT but the latest version (2007) moves towards BC. This contrasts with BS 25999-1, which was written purely as a BC standard to enable businesses to recover from incidents ranging from minor (outage of a few hours) to a major incident requiring relocation of services [BS 25999-1].

A number of frameworks in this area identify a purely IT aspect of BCM referred to as IT Service Continuity. IT Service Continuity Management (ITSCM) is a discipline which has evolved from IT Disaster Recovery (ITDR) but is more customer-centric. The paradigm is similar, but the underlying assumptions made by ICT as to priorities, timescales and important components are replaced with accurate data from the business units. ITSCM is the control which transforms ICT into a pro-active service organisation, meeting the needs of its customers, understanding their requirements and fulfilling these requirements. In the event of an incident the plans and systems in place should ensure a resumption of service within the agreed Service Level Agreements (SLAs) ensuring compliance and customer satisfaction as well as aiding in Business Continuity.

This report utilises knowledge of many different methods, represents them on a Business Continuity overview process diagram and then compares the methods through individual process diagrams and entries in an inventory. This allows the readers to assess their suitability for use within their own organisation. Moreover, it provides an orientation for the target audience who would like to have an overview on the state of art of methods and good practices for continuity and who would like to properly apply existing approaches to their organisation.

2 Scope

This report will provide an introduction to establishing a Business Continuity Management process within an organisation in order to mitigate the technology and information continuity risks identified as part of Risk Management.

In order to maintain availability of IT and information the organisation needs to understand:

- which processes are critical;
- how quickly they must to be restored;
- what are the IT and information required in order to keep these critical processes running.

Using this information, ICT and Information Security (IS) professionals are able to determine the actions that must be performed to ensure that the IT and information requirements of the critical processes can be met, despite a disruptive event. This includes ensuring that the ICT and IS staff are available within the required timeframes and the identification of an alternative site(s) from which to work should it become necessary. This information is detailed within the Business Continuity Plan (BCP).

Once ICT and IS are operational again, the operational teams will be able to work from their IT Service Continuity Plan to restore the critical IT components and information required to support the critical processes.

This report does not address the continuity of the critical processes themselves but rather the continuity of ICT and IS that is needed to provide the critical processes with their technology and information requirements following an incident. This is represented in the figure below.

Error! Not a valid link.
Figure 1 - Scope of this document

Critical Processes are shown within their Business Units. These feed Recovery Time Objective (RTO) and Recovery Point Objective (RPO) requirements to the ICT and IS departments according to requirements dictated by the processes; the processes themselves are outside the scope of this report. Within ICT and IS there is a significant issue concerning their continuity response. Their own Business Continuity requirements (this is often a very difficult concept for actors in this field to understand and accept) are shown as the lower section on the left[2]. IT Service Continuity Management (ITSCM) is determined purely by the requirements of Critical Processes. This involves a number of systems (hardware, applications, databases and pre-requisite software). The chain of dependencies determines the prioritised order of recovery and timescales for recovery. If outages are recovered within the approved timeframe, IT outage events will not trigger Business Continuity events.

Specific technical procedures for IT system recovery – usually contained in the IT Service Continuity Plan - are not developed in detail in this report, and more information can be

[2] Not all of these critical processes have IT requirements e.g. a process to change backup tapes and ensure they are stored in a secure, off-site location will not require software and therefore has no RTO/RPO requirements from the underpinning technology.

found within standards and guidelines such as PAS 77, NIST 800-34, ITIL v3 and COBiT v4 [COBIT].

The interfaces between the Business Continuity Plan and the IT Service Continuity Plan are extensively covered in this report.

While this report focuses on Business Continuity, it concentrates on ICT, on the relationship of IT Service Continuity to Business Continuity, and on the importance of considering both together (and not each in isolation) to achieve a successful, integrated recovery from an incident. The methodologies described in PAS 77, ITIL v3 and COBiT v4 all state that BCM should be in place before ITSC can be achieved. If it is not, then BIAs must be performed by the Business Units in order to provide ICT with a business view of the IT requirements. The results of the BIA study are recorded in a report which is then transferred from BCM to ICT. This report is referred to in the present document as the IT Requirements document.

Error! Not a valid link.

Figure 2 - The Information Technology Service Continuity process

The present document shows the relationship between BCM and RM, where BC is seen as a method of Risk Treatment to mitigate continuity risks. These risks are either treated in a proactive or reactive manner. **Proactive controls** implement agreements and systems in place to deal with the effects of a disruption. These can take the form of an agreement with a Work Area Recovery Facility (WARF), a clustered server with UPS and RAID disks or simply having a second telephone line installed. Business Continuity Plans are developed for a **reactive response**.

HB 292-2006, the Australian Handbook for Business Continuity practitioners [HB 292-2006], advocates a proactive approach to Business Continuity where the BCM practitioner works closely with the risk managers so that much of the Risk Assessment for BCM is undertaken by others, providing more quality input into the process. This means that treatment of disruption events become a focus and 'the (BCM) practitioner can lead the creation of proactive improvements in capabilities in resilience'. It goes on to state that the contents of the standard have a strong emphasis on conducting a robust Risk Management process as part of BCM.

A number of standards use a proactive and reactive approach to Risk Management and the mitigation of continuity risk e.g. NIST 800-34, BS 25999-1 and Business Continuity Institute Good Practice Guide [BCI GPG]. In this report we consider only the reactive controls as the proactive ones are mitigated in the classical Risk Management activity leaving Business Continuity to address the risks which cannot be successfully mitigated or treated as well as those that arise as a result of an incident. More detail is given in Section 7.1.

3 Assumptions

In writing this report, the following assumptions have been made:

- Any Disaster Recovery Plan contains the procedures for restoring IT components, telephony and information following a disruptive event.
- Information refers to electronic information e.g. application files, data within databases, data on CD, DVD or memory stick etc.
- ICT and Information Security are functions. As such, they are not necessarily managed by a single department (ICT).
- Preventative risk controls (proactive measures to reduce the likelihood of a disruptive event) are outside the scope of this document. Instead, they are fed back into the classical Risk Management model.

4 Approach

To ensure that no standard has been given an unequal priority within the review process for this document the following methodology was adopted:

- Evaluate a number of standards from different parts of the world to see how they relate to BC and ITSC;
- Develop a generic Continuity Management process to show activities including how they flow;
- Integrate this result with the existing ENISA process model on Risk Assessment and Risk Management.

In compiling this report, various standards, handbooks and good-practice guides related to Business Continuity, Information Technology Service Continuity, Risk Management and Information Security were evaluated (see Bibliography).

An overview Business Continuity process (see Figure 7) was developed which represents most of the Business Continuity methods available at present, while remaining independent. The language used fits all current methods rather than being aligned with any one method in particular.

It was felt that the existing Risk Assessment model [ENISA RM] could be utilised for BCM since it is important to show the relationship between Business Continuity and Risk Assessment. Since Business Continuity is risk-based the model appears to fit at many levels. The block diagram was then developed and the interfaces and overlaps were discussed (see Figure 8).

5 Structure and target groups of this document

The structure of the present document is illustrated in Figure 3.

The intended target group for the present document is Information Security and Information Technology experts. It focuses on how to write a Business Continuity Plan (BCP) to protect ICT or Information Security in the event of an incident which threatens their ability to provide their services to the rest of the organisation. The general overview of BCM also provides background to anyone writing a Strategy/Plan. In addition it addresses the interfaces among Business Continuity and Risk Management.

Error! Not a valid link.

Figure 3 - Structure of the document

The structure of the document is not intended to be used as step by step instructions for conducting any of the activities described herein, but it is intended to provide an overview of a complete process.

The main body of the report draws on various worldwide standards, good practices and the experience of the authors to describe the main principles of Business Continuity Management. These main principles are summarised in an overview process diagram while the various standards that can be used to assist individuals in writing a BCP are illustrated in the process maps appended to the document.

Also appended to this report are two templates that will serve as a basis for the generation of an inventory of methods, tools and good practices for Business Continuity. They will be used later on to generate a survey on existing methods, tools and good practices in this field. The purpose of each template is to represent all necessary information required for the inventory entries. This information includes the main features of the methods and tools available and how they may best be used to assist an organisation in writing a BCP. Each method and tool has its own particular strengths. Accordingly the inventory compares and contrasts these tools and methods to ensure that those most appropriate to the organisation's needs will be selected.

A GLOSSARY provides an explanation of the BC terminology used both in this document and in the standards and good practices used as a basis for this document. Where there is more than one term for the same entity it is cross-referenced.

To assist further with Business Continuity planning a list of useful web-site links has been appended in addition to the Bibliography (see Section Websites).

Although the document appears to be aimed at larger organisations with separate ICT and IS departments, and several sites, it is equally relevant for firms defined as Small to Medium Enterprises (SMEs). Their plans will obviously be simpler since the roles and responsibilities and membership of the Operational Team may well amount to a single person rather than several individuals. Some plans may also be combined and sections irrelevant to the organisation deleted.

Appendix A outlines an initial framework for the BCM approach for SMEs. ENISA will elaborate on this document to develop it into a full fledged approach for SMEs.

Appendix B provides a simple example of a BCM Policy.

6 Business Continuity and its interface with related disciplines[3]

Corporate Governance is concerned with improving the performance of companies for the benefit of shareholders, stakeholders and economic growth. It focuses on the conduct of, and relationships among, the Board of Directors, Managers and Shareholders. It generally refers to the processes by which organisations are directed, controlled and held to account. It encompasses authority, accountability, stewardship, leadership, direction and control exercised within the organisation [HB 254-2005].

The Australian Stock Exchange has developed ten core principles which underlie sound corporate governance, one of which is recognising and managing risk. According to HB 254-2005, the integration of a Risk Management processes into an organisation's corporate governance framework has the following advantages:

- More effective strategic and operational planning
- Greater confidence in achieving planned operational and strategic objectives
- Greater confidence in the decision-making process
- Greater stakeholder confidence and enhanced capital-raising
- Director protection
- Enhanced operational resilience (and continuity)

Risk is present in all decisions and activities undertaken by organisations and a number of these will present continuity issues. The approach to managing these continuity risks is twofold:

1 Pro-actively manage the risk, as part of the organisation's Risk Management process on an ongoing basis to lessen the likelihood or impact of an incident. The Business Continuity process itself can highlight further risks, which will themselves become part of the Risk Management process.

2 Implement a Business Continuity Management process to treat residual risk. Business Continuity Management should be conducted as one of the required outcomes of the Risk Management programme. Both BS 25999-1 and the Draft for Public Comment BS 31100 – Code of Practice for Risk Management [BS 31100] – states that Business Continuity is one of the ways of modifying risk to lessen the impact if the risk occurs; especially in cases where avoiding, transferring or accepting the risk are not appropriate risk treatments. This could be considered a reactive method of managing risk.

ISO 27001:2005 - Annex A [ISO 27001] calls for Business Continuity Management, as a method of risk treatment, to be considered as a measure to counteract interruptions to business activities and to protect critical business processes from the effect of major failures of information systems or disaster as well as to ensure their timely resumption.

[3]It is very difficult to isolate all the disciplines related to planning for and recovering from an incident which threatens an organisation either from an internal or external source. All the disciplines are closely related and there are areas of cross-over, where it is difficult to implement one plan without the other. For instance if an external incident resulted in a large-scale evacuation, the BCP would not be effective in helping to restore critical activities if the Emergency Plan had not been put into action, staff were not accounted for, the area made secure and the damage assessed.

Error! Not a valid link.

Figure 4 - Key functional elements of BCM (from HB 292-2006)

A further comparison of Risk Management and Business Continuity Management is given in Table 1.

	Risk Management	**Business Continuity Management**
Key Method	Risk Analysis	Business Impact Analysis
Key Parameters	Impact and Probability	Availability and Impact
Type of incident	All types of events	Events causing significant business disruption
Size of events	All events affecting the organisation	Those threatening availability of organisation's core processes
Scope	Focus primarily on management of risks to core business objectives, to prevent or reduce incidents	Focus mainly on incident management and recovery of critical business processes following an incident
Intensity	All, from gradual to sudden	Sudden or rapid events (although response may also be appropriate if a creeping incident suddenly becomes severe)

Table 1 - Comparison of Risk Management and Business Continuity (based on BCI Good Practice Guidelines 2007)

Business Continuity Management is concerned with managing risks to ensure that at all times an organisation can continue operating at least to a pre-determined minimum level. The BCM process involves reducing the risk to an acceptable level and planning for the recovery of business processes should a risk materialise and a disruption to the business occur.

Disaster Recovery Planning is concerned with the actual technical recovery of the IT components and details the procedures to be used to restore the IT components following a failure. As the plan is devised by ICT without the knowledge and understanding of business units as to their IT requirements, it is an orderly but non-prioritised recovery process. The Disaster Recovery Plan will not be discussed in this document, but its existence is mentioned for completeness.

Information Technology Service Continuity Management (ITSCM) ensures that information technology technical and services facilities (including computer systems, networks, applications, telecommunications, technical support and service desk – referred to as IT components throughout the remainder of this document) can be recovered within required and agreed business timescales. ITSC Management should be part of the overall BCP and not dealt with in isolation (PAS 77: 2006). The major difference between DR planning and ITSCM is that the user requirements drive ITSCM - their recovery time objectives and agreed recovery sequence (taken from dependencies and RTO for applications). This enhances the service as it focuses the recovery effort on the Business Continuity requirements and reduces disruption to the critical processes.

Definitions of the various risk-related disciplines are given in Table 2.

Risk discipline	Description
Corporate Governance	The system by which entities are directed and controlled [HB 254-2005]
Risk Management	Process of enhancing an organisation's likelihood of success in achieving its objectives [HB 254-2005], [BS 31100]
IT Risk Management	The process, distinct from Risk Assessment, of weighing policy alternatives for the safeguard of data assets and IT systems in consultation with interested parties, considering Risk Assessment and other legitimate factors, and selecting appropriate prevention and control options. (ENISA)
Business Continuity Management	BCM assures the availability of processes and resources in order to ensure the continued achievement of critical objectives [HB 293-2006]
IT Service Continuity Management	Supports the overall Business Continuity Management process by ensuring that the required information technology components can be recovered within required, and agreed, business timescales and in the agreed order of priority, from data extracted from the BIAs. The underlying recovery procedures can then be prioritised to effect recovery in a timely fashion [PAS 77]
Disaster Recovery Planning	Disaster Recovery Planning refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility. The scope may overlap that of an IT Service Continuity Plan; however, the DR Plan is narrower in scope as it does not address the requirements of the business (based on [NIST])

Table 2 - Related Risk Management disciplines

The relationships among Corporate Governance, Risk Management, Business Continuity Management, IT Service Continuity Management and Disaster Recovery Planning are complex since some can exist without the others. Figure 5 on the following page tries to explain the relationships, should they co-exist.

Error! Not a valid link.

Figure 5 - Proposal for a nested relationship of the related risk disciplines

BCM overlaps with Risk Management (see Figure 5), and one of the areas of convergence is Business Impact Analysis. If ITSCM is in place, it utilises some of BIA's information in order to achieve Continuity Management and align it with the needs of the business. That is the only information which BCM and ITSCM have in common. ITSCM uses this information in order to prioritise the plans developed through DR Planning.

If ITSCM does not exist within the organisation then DR Planning is the pro-active risk mitigation function of Risk Management and although it impacts BCM and can be invoked by a BCM event it is not part of BC. Similarly, ITSCM can exist without BCM but requires a subset of BIA information so the Business must conduct BIAs in order to ascertain the necessary information. If there are no DR Plans then these must also be developed. DR Planning is an essential part of ITSCM. Although it may not exist when originally

developed it must be in operative if ITSCM is to be considered complete. In a similar way, BCM cannot exist without BIA information.

Risk Management and Business Continuity need to be considered as an integrated whole together with IT Service Continuity and Information Security. The successful implementation of a robust Business Continuity Plan is dependent upon having a tried and tested ITSC Plan in place which improves the technological resilience of the organisation. This requires the presence of procedures for restoration should any part of the IT infrastructure fail.

Not only should the Business Continuity Plan consider the IT requirements of the business processes within the organisation, and how ICT will organise themselves to restore services to meet the business requirements following an incident, but the Business Continuity Plan must consider the information requirements. BS 7799-3 [BS 7799-3] states that one of the most valuable assets of an organisation is its information which needs to be protected whatever its form. Information assets, which can be databases, contracts, user manuals and training materials, or other types of information, are stored on or used by other assets and these may be defined as:

- Processes and services
- Software
- Physical items
- Personnel

Information Security (IS) must be able to recover its own processes following an incident in order to be able to restore the business processes' information requirements. Interdependencies will exist between ICT and IS and the two will need to work together to ensure an integrated approach which meets business needs.

There are other security disciplines related to Business Continuity which are described in the following paragraphs and illustrated in Figure 6.

Emergency Planning: Emergency planning is a process resulting in a set of agreed procedures to prevent, reduce, control, mitigate and take other actions in the event of a civil emergency which impacts the organisation [BS 25999-1].

Incident Response: Incident response is the immediate response to an incident usually within the first few hours of occurrence. It is an important phase in which control should be gained of the incident, the impact assessed, personnel made safe and key communications made to staff, public, stakeholders and the media. If control is not gained at this stage it is extremely difficult to implement effective incident management thereafter (Glen Abbot).

Incident Management: Incident Management is the process of taking central command and control of an incident which threatens the operations, staff, stakeholders or reputation of an organisation. The incident management team ensures that staff are able to restart their critical processes and communications are made internally and externally (Glen Abbot).

Error! Not a valid link.
Figure 6 - Incident timeline

7 The Business Continuity Process

7.1 Overview of the Business Continuity Process

Error! Not a valid link.

Figure 7 - The Business Continuity Process

The presentation of Business Continuity Management processes in this chapter is a consolidated overview of relevant content found in the corresponding literature (see Bibliography). As mentioned above (see Approach), various standards, handbooks and good-practice guides related to Business Continuity, Information Technology Service Continuity, Risk Management and Information Security were evaluated to derive the process model overview. It then presents most of the Business Continuity methods available at present, while remaining neutral. The language used fits most current methods rather than being aligned with any one method in particular.

In the present document Business Continuity is considered to be the umbrella under which take place several processes/activities related to the identification, mitigation, management and control of continuity risks, as well as the governance of such a project inside an organisation. For the sake of the presentation, an integrated view of Business Continuity is presented in terms of a "big picture", i.e. the six processes and their activities (see Figure 7). Furthermore, this figure shows possible interfaces among the processes presented.

In practice, any of the processes depicted can be used as an entry point to the Business Continuity process or can be performed in isolation. Many organisations, for example, perform Risk Treatment without the performance of an exhaustive and documented Risk Assessment or without the prior establishment of a Corporate Business Continuity Strategy.

The ideal sequence for the performance of the processes of Business Continuity is to start with the definition of a Business Continuity Framework inside the organisation for the Programme Governance and proceed as indicated in the figure above by the orange cyclic arrow.

Business Continuity Management is considered as consisting of the six main processes shown in the figure above: *Define a Business Continuity Management framework, Conduct of Business Impact Analysis, Design of a Business Continuity Management approach, Deliver Business Continuity Plans, Test of Business Continuity Plans, Sustain Business Continuity Management Programme*.

The content of these processes is outlined below with a short description. A more detailed description can be found in Section 8-13.

7.1.1 Define BCM framework

In order to implement successful Business Continuity Management within an organisation, it must first be initiated as a project, including well defined project structure, scope, objectives and deliverables aligned with the business strategy and the risk appetite. It is essential for the success of the project that the senior management team endorse the project and provide support to it at all times.

Once the Business Continuity project has been established, and in order to be able to commence development of the suite of Business Continuity Plans, it is essential to

understand completely the organisation with respect to its critical business processes, technology risks, loss impacts and resource requirements. This understanding aids the development of continuity plans that will support the strategic needs of the organisation, ensure that key internal and external customer needs can be met and also protect the safety and welfare of staff.

7.1.2 Conduct Business Impact Analysis

Once the business critical processes of the organisation have been identified, the purpose of Business Impact Analysis (BIA) is to correlate specific IT components with the critical processes that they support and based on that information, to characterise the consequences of a disruption to the components.

The technology risks thus identified will contain enough information to produce the IT Requirements report. This should include not only the technological components (specific hardware, applications and peripherals which in turn point to infrastructure, servers, databases and networking components) but also the specific Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) required by the business units for their critical business processes. The definition above relates to two different objectives. The BIA gathers '*process RTO'*, the recovery time objective for the process as a whole. In order to achieve this objective there is a critical path of underpinning components. The latter must be recovered in a shorter timeframe in order to achieve the process RTO. Throughout the remainder of this document the timeframe to recover such underpinning components will be referred to as the '*component RTO*'.

The process RTO specifies the critical processes' desired recovery time and the ITSC Plan will need to consider the actual RTOs for all dependent components (e.g. infrastructure, server build, network connections, data restore) in determining how or whether it is possible to achieve an overall RTO which meets the requirements of the business.

The RPO specifies the recovery period for data, e.g. no more than 24 hours of data can be lost. This is a trickier metric since it is a checkpoint in time which may require that database checkpoints, transaction logs or write-through disk data, more frequent backups, and all the associated recovery procedures are carried out in a timely and consistent fashion.

7.1.3 Design BCM approach

Once the processes have been prioritised and the critical technology infrastructure, hardware, software and information resource needs of the processes which depend upon IT have been identified, it is necessary to design the way in which recovery from an incident can be effectuated. Given the requirements and the various methods of recovery, decisions must be made as to how recovery may be best achieved. Factors such as budget, manpower and compliance will drive the decision making process. A list of options can be drawn up and weighted to aid decision making. For this reason, the management of the organisation will be asked to accept both the risks treated and the ones that will not be treated. This can happen within the activity "Risk Acceptance" of the IT Risk Management process (see Figure 8).

7.1.4 Deliver BCP

A Business Continuity Plan is not one document but rather a whole suite of documents which integrate to form the organisation's response to an incident from the moment of impact to near normal recovery of the organisation. Everyone who is responsible for recovery actions will work according to their specific recovery plan.

7.1.5 Test BCP

This area of BC ensures that the Business Continuity Plan is adopted by the whole organisation and is viable and workable. Testing verifies that the plan actually meets its objectives whilst training allows staff involved in the recovery of the business to gain experience in their roles. Plans must be kept up to date and regularly reviewed and re-tested.

7.1.6 Sustain BCM programme

BCM is not a static or point-in-time solution. In order to ensure that it is current, it will be necessary to implement an on-going maintenance regime and internal communication. BCM cannot be effective if staff are unaware of the existence of plans or if those with roles to play are unsure of their roles, of what is expected of them and where to find information. This requires the training of BCM staff and awareness by all.

It is important that strict change control and maintenance regimes are in place and that the identified updating tasks are performed regularly and in a regulated manner.

7.2 Relationship between IT Risk Management and Business Continuity

As mentioned previously, Business Continuity Management has an inseparable relationship with Risk Management. Traditional thinking has positioned Risk Management as a tool to be used within Business Continuity, whereas more contemporary thinking sees Risk Management as a broad philosophy looking at understanding uncertainty, informed decision making and managing surprise in the achievement of objectives. This thinking also views BCM as an integral part of the broad field of Risk Management, a part that considers the management (both pre- and post-incident) of those risks which may result in disruption to the organisation [HB 292-2006].

HB 292-2006 goes on to include the following among the benefits of this more contemporary approach to Risk and Business Continuity:

- a more comprehensive consideration of risk within the BCM process
- improved integration between BCM and Risk Management activities which in turn includes:
  - improved flow of risk related information;
  - a better understanding of the requirements of both activities;
  - a reduction in repeated demands for the same sets of information;
  - an organisational focus on priority risks including those related to Business Continuity;
  - a more cost effective use of resources;
  - an improved focus of BCM activity on business improvement rather than reactive planning only.

Figure 8 shows the overlap between the Risk Management process and the Business Continuity process, where the definition of the framework for the Business Continuity Management could be carried out as part of the definition of the Risk Management framework. Conducting a Business Impact Analysis is an extension of assessing risk and the two tasks can be carried out simultaneously as a way of gaining complete insight into the risks faced by the organisation, the likelihood of them occurring and the impact upon the organisation's ability to continue to operate. However, further work is required during this stage of Business Continuity to determine the resources required by the critical processes and the timescales for recovery should there be an incident which prevents normal operation.

When determining the strategy for recovery it is likely that further risks relating to continuity of operation will be highlighted. These are then fed back into the Risk Management process (see pink arrow labelled "Acceptance of continuity risks"). Decisions are taken whether to accept the risks or develop an action plan to treat the risk. This may then feed back into the Business Continuity process.

The stage of Risk Treatment in the Risk Management process determines the action to take to avoid, share, retain or modify the risk. One method of modifying risk is to lessen its impact by implementing a plan for continuity: this is shown in the pink arrow labelled "Controls for Continuity".

Figure 8 represents the classical approach to Business Continuity, where Business Continuity is seen as a way to cover residual (continuity) risk only and is therefore not seen as a preventative control. This view is presented in BS 25999-1 and FEMA 141 [FEMA] and is discussed further in this report.

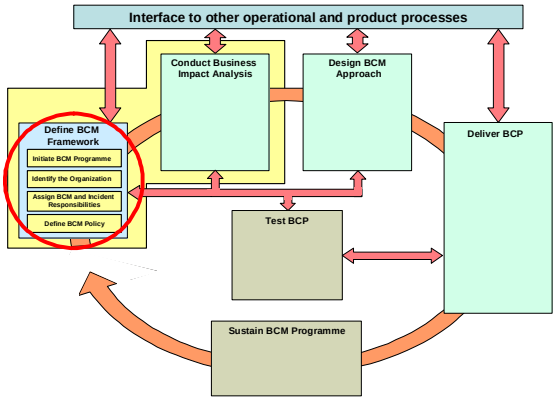
Other standards present a more integrated approach to Risk Management and Business Continuity, where preventative controls are part of Business Continuity Management. These standards include HB 292-2006, NIST 800-34 and NFPA 1600.

Error! Not a valid link.

Figure 8 - Integration of Business Continuity with Risk Management[4]

[4] The figure depicting the Risk Management process has been taken from a previous ENISA deliverable [ENISA RM].

8 Define BCM framework



BCM is an ongoing management process undertaken on a continuous basis to safeguard the interests of key stakeholders, as well as the reputation, brand and value-creating activities [TR 19:2005] of an organisation.

Where BCM is being implemented for the first time in an organisation, it is advisable to treat the implementation as a project. The project should be managed in line with the organisation's normal project management methodology [COBiT].

In order to manage and maintain BCM within the organisation, personnel must be appointed who will be responsible for defining and managing the complete BCM programme.

The next step is to ensure that a BCM Policy is defined which is appropriate to the nature, scale, complexity, geography and criticality of the business processes and that it reflects the culture, dependencies and operating environment. The Policy should also consider budget availability, time constraints, regulatory aspects, deadlines and the source of the Business Continuity expertise [HB 221:2004] Definition of the BC Policy is essential before the development of the BCP can commence since it forms the foundation for the rest of the work and for the continued viability of BCM (see example in Appendix B).

The BCM capability should be integrated into the organisation's change management process so that it is incorporated into the growth and development of the organisation's products and services [BS 25999-1].

During this stage of the BCM programme consideration should be given to the personnel who will form part of the organisation's response and recovery teams during and after an incident.

8.1 Initiate a BCM programme

When implementing a BCM programme for the first time in an organisation, project management disciplines should be adopted, which define clear deliverables, budgets and timescales.

Once the BCM programme has been established and the key elements are in place, further work programmes are likely to develop as the maintenance, testing, training and review cycle get under way and the BCP evolves.

Initiating the programme should include:

- Goals and objectives of strategic and operational activities of BCM
- Identification of deliverables and outcomes
- Timescales and deadlines
- Constraints
- Budget and work effort control
- Resourcing capabilities

There are several project management methods, some of which have software support. The method selected should be appropriate to the size and complexity of the organisation.

8.2 Identify the organisation

So that ICT and IS can prioritise and manage their recovery activities they need to understand the requirements of the rest of the organisation. The scope of the BCM programme will assist in identifying the key business areas that need to be questioned about their use of technology and information as well as about the likely impact of its loss. The most effective staff members for contributing to the BIA are the managers or team leaders of the business units since they not only understand how their business area operates from day to day, but they also have the authority to define the required recovery objectives.

A clear understanding of the key responsibilities and position inside the organisation is also required to appoint the teams that will be responsible of the BC project in all the different phases, as described below.

Once the business areas have been identified it is necessary to identify the business processes within those areas. It is more effective to recover an organisation at process level following an incident as it ensures that non essential areas are not recovered before essential ones.

8.3 Assign BCM responsibilities

The senior management team should appoint or nominate a person with appropriate seniority and authority to be accountable for BCM policy and implementation and appoint one or more individuals to deliver and maintain the BCM programme.

Essentially, responsibility for the implementation and ongoing day to day management of the Business Continuity project is undertaken by two teams; the Business Continuity Management Team and the Business Continuity Steering Committee.

In addition to it, specific teams will be appointed to deal with incidents, as described in Section 8.4.

The detailed team structure proposed in the following paragraphs – derived from some leading standards - better suits the need of larger organisations; in smaller organisations, many roles and responsibilities (strategical as well as operational) may be bundled together and covered by fewer teams. This holds true both for strategic teams and teams in charge of operations following an incident (see below).

Appendix A outlines a framework for the BCM approach for SMEs.

8.3.1 Business Continuity Management Team

The Business Continuity Management Team will be led by the Business Continuity Manager, who will be responsible for the delivery of the BCP, embedding BC within the organisation and ongoing maintenance of the BCP. Depending on the scope of the programme the BC Manager might be assisted by a Business Continuity Analyst. In large organisations there may also be Business Continuity Co-ordinators within each business unit, who are responsible for assisting with the gathering of the impact data (see Section 9) and for writing and maintaining their own business unit recovery plans under the guidance of the Business Continuity Manager.

Error! Not a valid link.

Figure 9 - Structure of the Business Continuity Management Team

The Business Continuity Manager does not necessarily become a member of the Incident Management Team during an incident (see Section 8.4). Rather, this role is often used in a consultative capacity owing to its extensive knowledge of the organisation.

8.3.2 Business Continuity Steering Committee

It is imperative for the governance of the BC programme that a Business Continuity Steering Committee (BCSC) is appointed. Because Business Continuity Management is concerned with infrequent but potentially catastrophic events, it can be overlooked as individuals within the organisation are pressed by their day-to-day responsibilities. When this occurs the Business Continuity Plan can decay and become increasingly irrelevant to the organisation. The implementation of a Business Continuity Steering Committee ensures that the organisation's Business Continuity Plans are regularly considered, reviewed, tested and updated when organisational change occurs.

This group comprises the most senior managers from the organisation and each key department must be represented. The BCSC should be lead by the senior manager with responsibility for BCM. NIST 800-34 suggests that this might be the Chief Information Officer. BS 25999-1 states that the responsibility for BCM should be assigned to the owner, a board director or elected representative. The profile of a typical BCSC is shown in Figure 10, which also shows the relationship between the BCSC and the Senior Management Team (strategic/gold level *incident* team - see Section 8.4.1). Each box represents a role rather than a management position, therefore more than one role may be held by the same person.

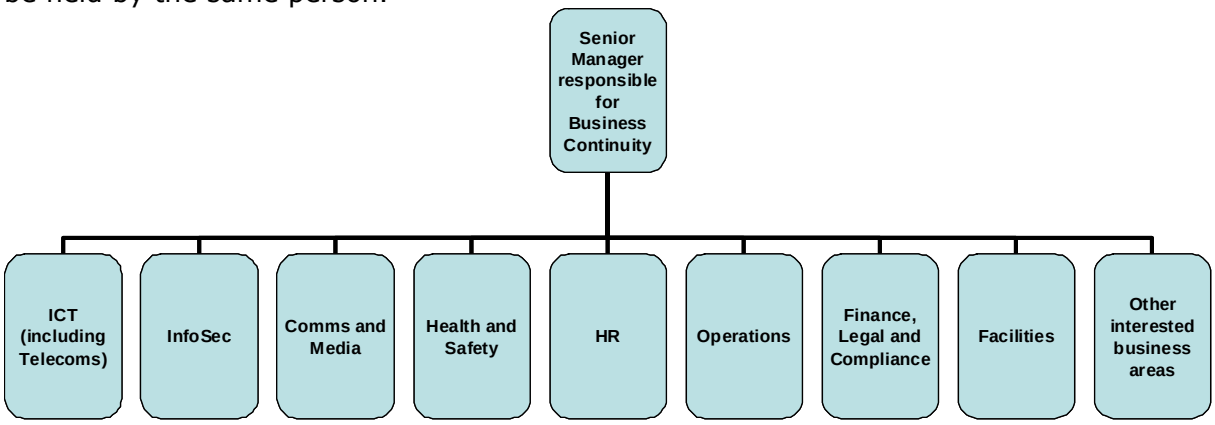


Figure 10 - Structure of a typical Business Continuity Steering Committee

The Business Continuity Steering Committee are tasked with making strategic recovery and continuity planning decisions for the organisation and will sign off on each stage of the programme. Unlike the usual project management steering committee, which is disbanded on completion of the project, this committee is permanent [TR 19:2005].

The BCSC should meet regularly at suitable intervals during and after the implementation programme. It is likely that the meeting interval would lengthen once the BC programme has been completed. Suggested meeting frequencies are monthly during the implementation phase of the programme and quarterly once the BCP has been delivered and BCM is part of everyday organisational management.

Most experienced Business Continuity Managers would state that implementation of successful BCM is dependent upon having senior management "buying in" from the very start of the programme.

Strategic management of an incident is carried out by the Senior Management Team (strategic/gold level incident team – see Section 8.4.1). It is very likely that some or all of the members of the BCSC or their deputies would become members of the Senior Management Team during an incident. Given the seniority of the members of the BCSC, it is unlikely that they would become members of the Incident Management Team (tactical/silver level incident team – see Section 8.4.2).

8.4 Assign Incident Teams

PAS 77 suggests a three-tiered approach to manage an incident. The three tiers are referred to as Strategic or Gold, Tactical or Silver and Operational or Bronze and this approach is in line with the approach the emergency services use. This is illustrated below in Figure 11. Early identification of the personnel who will comprise these teams is recommended so that they may become involved in the BC programme from the beginning and become familiar with Business Continuity and all that it involves.

These teams are only formed during an incident and do not have a line management relationship to each other. During day to day operation of the organisation, the members of these teams will be undertaking their normal duties, while attending incident management briefings and training as required.

8.4.1 Senior Management Team (Gold Team)

The Senior Management Team leads the incident strategically. They do not carry out recovery tasks, but are more concerned with strategic decisions such as longer term planning for normal business resumption from the incident, liaising with the stakeholders and giving media interviews.

Many members of the Business Continuity Steering Committee are also automatically members of this team which is in charge of strategic decisions following an incident, i.e. the ICT, the Information Security and the Communication and Media members. Other members such as HR, Facilities and other interested business area managers are called upon as necessary, depending on the incident.

8.4.2 Incident Management Team (Silver Team)

The Incident Management Team is responsible for central command and control of the incident and assists the critical processes in implementing their recovery plans. The team works to the procedures within the Incident Management Plan and liaises both with the Business Unit Management Team and the Senior Management Team.

8.4.3 Business Unit Management Team (Bronze Team)

The Business Unit Management Team is responsible for recovery of their critical processes in accordance with their Business Recovery Plans. Each department will have a Recovery Manager who will liaise with the Incident Management Team.

8.4.4 Incident Response Team

The Incident Response Team will be involved in the management of an incident if there is a need to call out the emergency services and/or evacuate one or more buildings. Their responsibilities fall mainly in the first few hours after an incident. Once the incident is stabilised, and once it is established that the staff and anyone else who is affected (e.g. customers and public) are safe, then at that point they will handover the situation to the Incident Management Team.

Error! Not a valid link.

Figure 11 - The three tier Incident Management structure and the relationship with Incident Response (from [PAS 77])

NIST 800-34 [NIST] states that the specific types of teams required to manage an incident are based on the system affected. The functional teams are described below and some or all of these teams may be needed to effect a Business Continuity response:

Roles/Teams[5]	**Responsibility**	**Incident Level**	**Relevant Plans**
Senior Management Official/Team	Strategic management of the incident	Gold Team	Gold Incident Management Plan Long Term Resumption Project Plans
Management Team	Tactical management of the incident	Silver Team	Silver Incident Management Plan
Administrative Support Team	Administrative support for the Gold and Silver Teams	Gold Team Silver Team	Silver Incident Management Plan
Damage Assessment Team	Assessment of the damage caused by the incident	Bronze Team	Recovery Support Plan IT Service Continuity Plan
Operating System Administration Team	Recovery of operating system	Bronze Team	Business Recovery Plan IT Service Continuity Plan
Systems Software Team	Recovery of systems	Bronze Team	Business Recovery Plan IT Service Continuity Plan
Server Recovery Team	Recovery of servers	Bronze Team	Business Recovery Plan IT Service Continuity Plan
LAN/WAN Recovery Team	Recovery of LAN/WAN	Bronze Team	Business Recovery Plan IT Service Continuity Plan
Database Recovery Team	Recovery of database	Bronze Team	Business Recovery Plan IT Service Continuity Plan
Network Operations Recovery Team	Recovery of network	Bronze Team	Business Recovery Plan IT Service Continuity Plan
Application Recovery Team(s)	Recovery of user applications	Bronze Team	Business Recovery Plan IT Service Continuity Plan
Telecommunications Team	Recovery of telecommunications system	Bronze Team	Business Recovery Plan IT Service Continuity Plan
Hardware Salvage Team	Salvaging hardware for restoration and repair	Bronze Team	Business Recovery Plan IT Service Continuity Plan
Information Systems Team	Ensuring access to vital records and data. Ensuring compliance with the Data Protection Act	Bronze Team	Business Recovery Plan IT Service Continuity Plan
Alternate Site Recovery Co-ordination Team	Co-ordination of staff and resources at alternate site. Escalation of issues	Bronze Team	Recovery Support Plan IT Service Continuity Plan
Original Site Restoration/Salvage Team	Salvaging equipment and documents	Bronze Team	Recovery Support Plan IT Service Continuity Plan
Test Team	Testing the IT system once it has been restored	Bronze Team	Business Recovery Plan IT Service Continuity Plan
Transportation and Relocation Team	Transporting staff to alternate sites or home	Bronze Team	Logistics/Facilities Recovery Support Plan

[5] In a smaller organisation, some of the bronze roles may be rolled up together and covered by fewer teams. The same holds true for Gold Team and Business Continuity Steering Committee.

Roles/Teams[5]	Responsibility	Incident Level	Relevant Plans
Media Relations (Communications) Team	Issuing communications briefings	Bronze Team + Silver/ Gold Team members	Business Recovery Plan Communications and Media Plan
Legal Affairs Team	Managing legal aspects of the incident especially where insurance claims will be made or where there are casualties	Bronze Team	Business Recovery Plan
Physical /Personnel Security Team	Ensuring the security of the abandoned site and the alternate sites	Bronze Team	Incident Response Plan Business Recovery Plan
Procurement Team	Procuring items required for recovery e.g. servers, cabling, IT specialists, electricians	Bronze Team	Business Recovery Plan

Table 3 - Responsibilities of each of the Incident Teams (from [NIST 800-34])

8.4.5 Example of how the three-tier incident response would operate

This section provides an example of the way in which each team would operate and each plan would be used during an incident.

The organisation, River Bank, is a bank which provides mortgages. The main office, Riverside House, is situated on Tay Street, which runs alongside the River Tay.
In this example ICT and IS work in Riverside House, together with the bank's Mortgage Application Call Centre, the Finance department and the Credit Control office.

The main Communication Room (which unfortunately is in the basement) is flooded, causing several servers to be damaged and also compromising the electrical safety of the whole of Riverside House.

Error! Not a valid link.

Figure 12 - Three tier incident management example

The Facilities Manager advises the ICT and IS Manager, the Call Centre Manager, the Finance Manager and the Credit Control Office Manager that they should evacuate the building in accordance with the Incident Response Plan and then informs the Health and Safety Manager and the Business Continuity Manager of what has happened and the extent of the damage. The Business Continuity Manager contacts the members of the Incident Management Team who meet at the Incident Room in Glenalmond House and start implementing the Incident Management Plan.

ICT and IS are relocated to Gleneagles House in accordance with their Business Recovery Plan where everything needed has been set up. The management team will establish their own Incident Management Team to manage the operational teams and to liaise with the organisational Incident Management Team. The ICT and IS operational teams can then implement the IT Service Continuity Plan to restore the technology and information service to the affected Business Units.

The critical processes from the Call Centre, Finance and Credit Control teams will relocate to the alternate sites referenced in their Business Recovery Plans (which could include another bank site, working from home, relocating to a Work Area Recovery Facility – WARF) and once there will start working in accordance with their Business Recovery Plans. This might necessitate using the procedure for manual operation while ICT and IS restore service.

As the incident affects the bank's ability to answer customer telephone calls and release mortgage funds a gold team is established in order to cope with relevant managerial decisions related to the incident. The ICT Director would be part of this team.

8.5 Define BCM Policy

The BCM Policy provides the framework around which the BCM capability is designed and built. The BCM Policy is the key document which sets out the scope and governance of the BCM programme.

8.5.1 Define scope

It may be that an organisation wishes to include the whole of the organisation in the BCM programme or that it wishes, in the first instance, to cover only certain key areas such as the data centre or the processes which support key services. Alternatively the scope of

the BCM programme may be to cover certain customer groupings, essential plant or geographical locations.

BS 25999-1 allows for this approach, since compliance may be achieved for parts of an organisation rather than the whole organisation. However the BCI Good Practice Guidelines 2007 urge caution: "the limitation of scope should be seen as a tactical approach that allows a staged development to the introduction of BCM across an organisation. If a product or service is defined as being within scope then all activities which support its delivery must be included in the BCM programme".

8.5.2 Define BC drivers

The drivers against which the BCM is implemented should be defined so that the requirements of the organisation are met. The Australian standard HB 292:2006 suggests that key components of determining the organisational need for BCM should include:

- Understanding key imperatives of the organisation including:
  - critical objectives, critical success factors and key performance indicators
  - major current and emerging risks exposures
- Critical organisational dependencies and interdependencies both within and external to the organisation, including:
  - critical business activities
  - critical plant, property assets and other infrastructure
  - third party relationships such as with the community, suppliers, customers and partners
  - regulators (e.g. financial regulators such as FSA in the UK [FSA], APRA in Australia [APRA], Bundesanstalt für Finanzdienstleistungs in Germany)
- Analysis of past incidents and disruptions that indicate a propensity for future disruption, including:
  - occurrences in the area of the organisation under consideration (e.g. ICT and IS)
  - occurrences in the organisation as a whole
  - prior involvement of customers, suppliers, strategic alliances and other stakeholders
  - experiences of others within the same market sector, industry, geographical location etc

The information gathered from this activity can be used to answer the three following questions:

'What is important to my organisation and why?'

'What does my organisation depend upon to continue operating?'

'What might prevent my organisation from achieving its key objectives?'

The answers to these fundamental questions will allow the organisation to determine what BCM objectives it wishes to achieve and the areas to concentrate upon when developing the BCP.

8.5.3 Define stakeholders

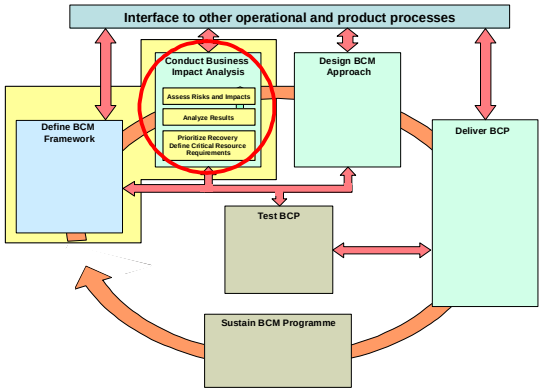
It is important to understand the stakeholders in the organisation in order to ensure that all aspects of Business Continuity planning have been addressed and all concerned

parties have been accounted for in the BCP. A stakeholder in any particular organisation is any party that has an interest in the success and ongoing operation of an organisation such as employees, directors, shareholders, regulators and customers. Each stakeholder, while sharing a common interest in the ongoing health of an organisation, can and will have slightly different perspectives:

- Employees will have expectations relating to security of employment and a safe working environment (the latter often being a regulatory requirement also)
- Directors will have expectations and responsibilities for ensuring growth, protection of revenues and profits and reputation management
- Shareholders will be concerned with the financial performance of the organisation, its commercial prospects and, particularly in the case of institutional investors, the overall systems of control and governance that are in place
- Regulators, depending on their remit, will have specific concerns regarding workplace safety, environmental issues, financial and/or operational controls
- Customers will be primarily concerned with availability and quality of goods and services provided

An organisation's Business Continuity arrangements should encapsulate all of these considerations when setting both its Business Continuity strategy and its specific recovery approaches.

9 Conduct Business Impact Analysis



The Business Impact Analysis (BIA) is a key step in the continuity planning process. The BIA enables the Business Continuity Manager or Business Continuity Co-ordinator to fully characterise the systems requirements, processes and interdependences and use this information to determine continuity requirements and priorities.

The purpose of the BIA is to correlate specific IT components with the critical processes that they support and based on that information, to characterise the consequences of a disruption to the components. Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the IT Disaster Recovery Plan, Business Recovery Plans and the Incident Management Plan [NIST 800-34].

9.1 Assess risks and impacts

Once the business critical processes of the organisation have been identified (see Section 8.2), the Business Continuity Manager may interview the managers of each business area at process level. The interview should ascertain for each process the impacts of losing technology or information in the following areas [BS 25999-1]:

- Impact on staff or public wellbeing
- Impact of breaches of statutory duties or regulatory requirements
- Damage to reputation
- Damage to financial viability
- Deterioration of product or service or service quality
- Environmental damage

HB 221:2004 adds the following impacts:

- Intellectual property, knowledge and data
- Stakeholder confidence and goodwill
- Political interest and comment

Additional methods to identify impact may be used. To this extent, qualitative or quantitative impact statements can be formulated. Such impact-measurement methods can be actually found in many Risk Management methods [ENISA_RM].

The technology required to operate each critical process should subsequently be identified and a Recovery Time Objective for that technology should be defined. This is the translation from process RTO (the RTO of the critical process as a whole) to component RTO (the RTO agreed for the various IT components required to operate the critical process itself). From the BIA data the ICT department must determine the supporting components. This may be a complex network (see Figure 1) as it may include several components (network, multiple servers, databases, data feeds from disparate

systems, pre-requisite applications, security settings, web server, etc) or it may be simple (Finance departments typically have a standalone PC with a single application, modem and smartcard reader in order to authorise bank payments). ICT must list the components and recovery sequence.

It may be helpful at this stage to start with a list of known technology so the list is not being re-created when it already exists. The ICT department may already have this information on their asset list, or IS may have this information if they have recently conducted a Risk Assessment. If this information is not already held, it would be a good idea to co-ordinate the efforts of ICT and IS. In this way, that not only are the details for the BIA collected, but any other information the ICT or IS departments may wish to gather about the business areas' use of technology and information are also obtained.

ICT will then be in a position to map the recovery process for components and relate the combined component RTO to the process RTO. If the sum of the components cannot be recovered within the process RTO then there is a gap (Figure 16).

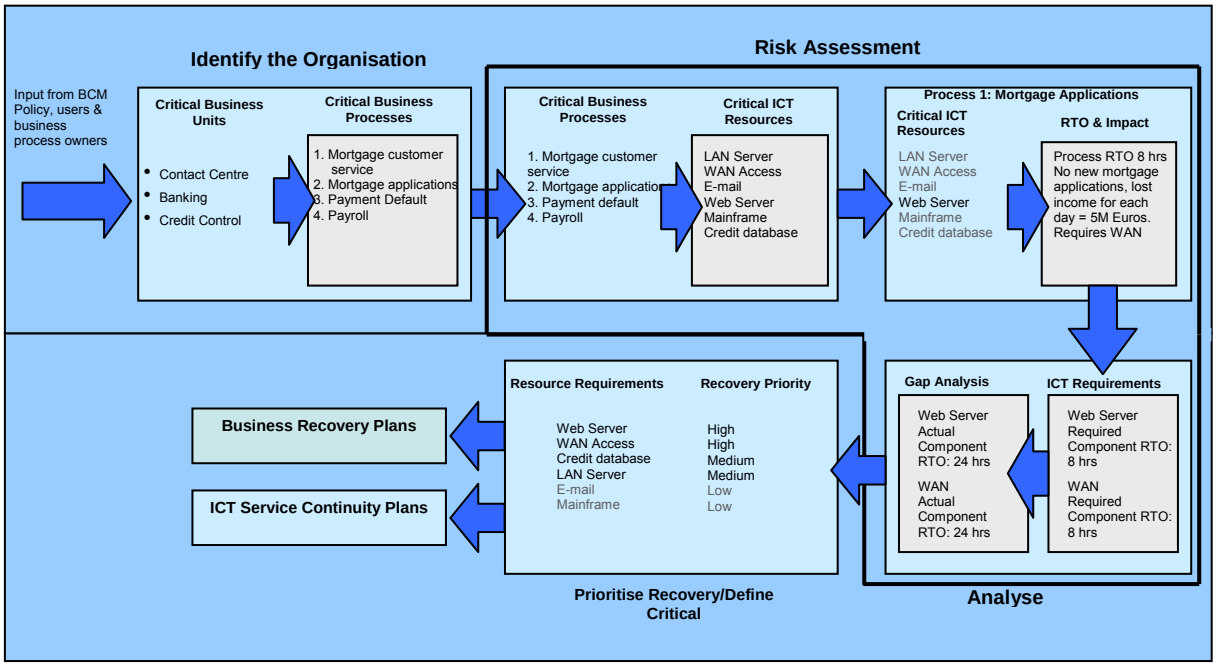


Figure 13 - Business Impact Analysis for the hypothetical River Bank plc (based on NIST 800-34)

For a BIA the minimum information which the Business Continuity Manager needs to gather from the business process manager is:

- business area and process names
- Recovery Time Objective for the process (based on the criticality ratings and recovery timescales defined in the BCM Policy)
- type of software used
- acceptable levels of downtime for the software
- information required (electronic and paper)
- acceptable levels of downtime for the information
- type of hardware used (can include workstations, printers, faxes, exception PCs, modems etc...)
- number of items of each hardware type normally used

- minimum number of items of each hardware type which could be used during an incident
- acceptable levels of downtime for the hardware
- telephony used
- acceptable levels of downtime for the telephony
- Service Levels agreed with hardware, software and service providers and within any IT support contract

The BIA should also be carried out on ICT and IS as an incident may require them to operate from an alternative location, and it is essential that they understand how they will support the organisation should they be affected by an incident.

If it has not already been carried out as part of the organisation's Risk Management, a Risk Assessment should be carried out on ICT and IS to assess areas of risk that may lead to a disruption. This Risk Assessment should be carried out in accordance with any of the relevant Risk Management methods as the ones described [ENISA RM].

The outcome of the Risk Assessment will provide the information with which to assess ICT and IS' vulnerabilities and allow them to develop an action plan to mitigate the risks. It is likely that some of the risks cannot be eliminated and the Business Continuity Plan must address them and provide a course of action should a disruption occur.

9.2 Analyse results

Once the information regarding technology usage, information requirements and acceptable downtimes has been gathered from the business processes, it is necessary to collate all the results and analyse them to determine the Recovery Time Objectives for each item of software, hardware, information and telephony used by the critical processes and the Recovery Point Objectives for the information requirements (critical data).

HB 292-2006 suggests one approach to consolidating and summarising this information is to construct a resource matrix which allows for mapping of the requirements over the whole or parts of the organisation.

Depending on the size of the organisation and the complexity of the resource requirements, there may be one resource matrix, which collates all the requirements identified in the BIA, or there may be several resource matrices, which individually show the required resources for staffing, technology, information/data, premises, equipment and materials. An example of a single Resource Matrix is shown in Table 4.

Critical Business Process	**Location**	**Process RTO (Days)**	**Additional Critical Applications, showing their Required RTO (days)**					**Critical Data**	**RPO for Data (Days)**
			Workflow	**MAD**	**CIS**	**Pay Master**	**GLedger**		
Mortgage Applications	Glenalmond House	1	2	1	0	0	0	Customer Details	1
Mortgage Customer Services	Riverside House	0.5	2	1	1	0	0	Customer Details	1
Payroll	Riverside House	5	0	0	0	10	5	Financial Accounts	1
Mortgage Payment Defaults	Gleneagles House	3	0	0	5	0	3	Customer Details	1

Table 4 - Technology resource matrix

From this Technology Resource Matrix an Application Resource Matrix could be constructed which only shows the applications and displays the information a different way. This representation highlights the discrepancy between the RTO required for that particular IT component (Required Application RTO) and the actual RTO (Required Application RTO):

Application	Critical Business Process Dependency	Required Application RTO (days)	Actual Application RTO (days)
Workflow	Mortgage Applications	2	3
	Mortgage Customer Service	2	3
MAD	Mortgage Applications	1	1
	Mortgage Customer Service	1	1
CIS	Mortgage Customer Service	1	3
	Mortgage Payment Defaults	5	3
Paymaster	Payroll	10	5
GLedger	Payroll	5	2
	Mortgage Payment Defaults	3	2

Table 5 - Application resource matrix

An Application Recovery Profile can then be determined which shows the order of priority of restoration of the critical applications, to meet the requirements of its most critical dependent process(es). The information is presented in Table 6 and as a graph in Figure 14.

If more than one process is dependent upon an application, the needs of the least critical process will be met by restoring the application to meet the requirements of the most critical application (e.g. Payroll and Mortgage Payment Defaults are both dependent upon GLedger. By restoring GLedger within 3 days for Mortgage Payment Defaults, Payroll's requirement of 5 days has also been met).

Shortest required application RTO (days)	Number of processes depending upon each application				
	MAD	CIS	Workflow	GLedger	PayMaster
1	2	2	0	0	0
2	0	0	2	0	0
3	0	0	0	2	0
10	0	0	0	0	1

Table 6 - Application recovery matrix

This is a very simplified Recovery Profile for illustrative purposes only: other factors may need to be considered such as inter-dependencies between applications, use of IT resource over different locations, prioritisation when several applications need to be restored at the same time or existing Service Level Agreements (SLAs) both internally and with third-party suppliers.

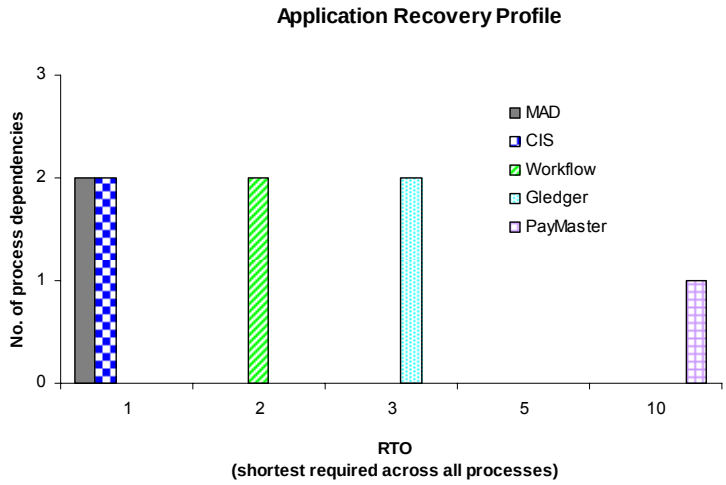


Figure 14 - Application recovery profile for the hypothetical River Bank

There may be instances when the actual RTO for an application (this is the minimum length of time within which ICT can restore it) is greater than the application RTO required by the process. This is illustrated in Figure 15. A further explanation of gap analysis is given in the next paragraph.

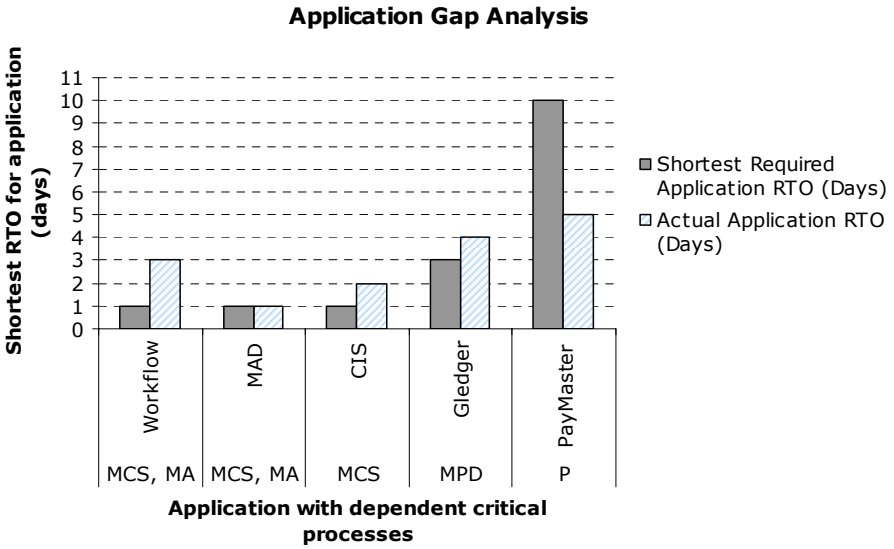


Figure 15 - Application requirements gap analysis for the hypothetical River Bank

Very often there are several interdependencies between the various IT components (applications, infrastructure, servers, databases), and if all the different component RTOs and RPOs do not match the process requirements these gaps constitute a risk and are highlighted in the IT Requirements Gap Analysis (see Section 11.8.1). The relationship between the different RTOs and the potential gap between actual component RTOs and the process RTOs are illustrated in Figure 16 and Figure 19.

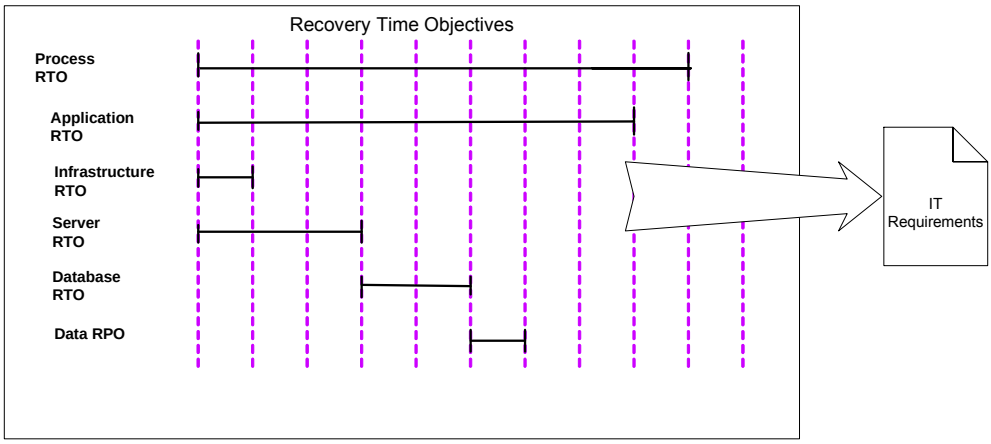


Figure 16 - Component RTOs meet critical process requirements

However the process RTO and component RTOs can vary wildly. Processes may require applications to be restored in order to commence work within their RTO, but because of the complexity of today's technology, this may involve restoration of a number of components (e.g. application server, file server, operating systems, infrastructure and data) in order to be able to recover the application for the business unit. An illustration of how the various component RTOs can impact availability of the critical process is shown in Figure 17. The discrepancies between the process RTO and the component RTO should be highlighted in an IT Requirements Gap Analysis which should be escalated to the BC Steering Committee, for gaps where there is a significant risk to be included in the Risk Register (see Section 11.8.2). In these cases a decision must be taken by the BCSC as to whether the affected business processes should develop manual workarounds, or increase their recovery timescales or whether, alternatively, the ICT or IS departments implement should a solution to improve their response times.

The gap between the process' requirements and the IT capability is illustrated below in Figure 17.

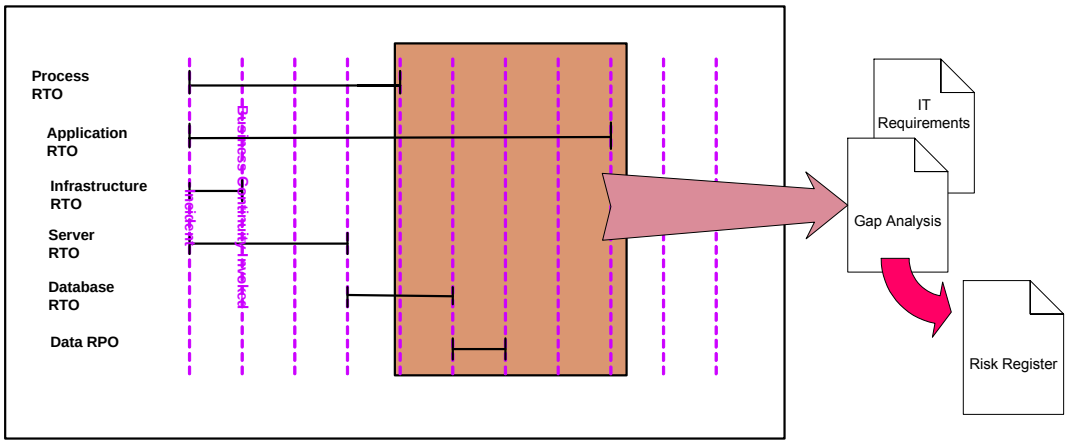


Figure 17 - Gap between the critical process RTO and the component RTOs

ICT and IS should also conduct a BIA on their own processes to understand their own needs for recovery so that the needs of the business and ICT can be weighed together.

9.3 Prioritise recovery/define critical resource requirements

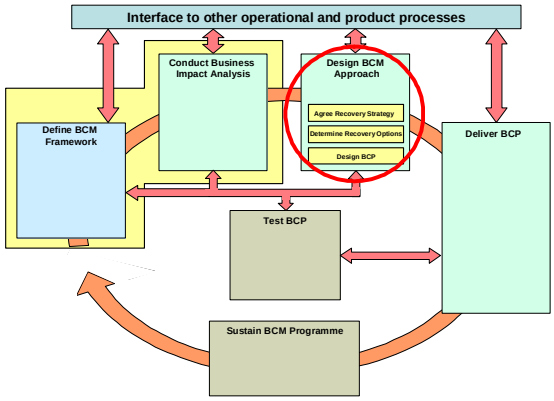
Drawing on the analysis of the results from the BIAs and in consideration of all the factors involved, the Business Continuity Manager can define the priorities for recovery of

the IT and IS components. This assessment will be based upon the criticality of each process, the required RTOs and RPOs, restoration capability, the component/process location and component interdependencies. This is essential information since in turn it helps ICT and IS define their own staffing levels and resource requirements over time, in order to be able to support the recovery effort following an incident.

The end result will be a finalised recovery profile which shows over time what is being recovered and the specific resource (technical, staff, premises, equipment or materials) that is required at any time to support the recovery. The recovery profile will allow the identification of a number of possible recovery options; the choice of recovery option will determine the BCM strategy and subsequently the development of an appropriate IT Service Continuity Plan and the Business Continuity Plan.

Should discrepancies occur between the required process RTO and the component RTO, as highlighted in the IT Requirements Gap Analysis, these must be addressed before the BCP can be completed.

10 Design BCM approach



The recovery approach is developed from the analysis of the results of the BIA and provides guidance on the way in which recovery can be effected. The first stage is to develop the possible recovery options which outline what the organisation could do to meet its BC Objectives as stated in the BCM Policy

The strategy is developed once the most appropriate recovery option(s) has been chosen and this will enable the key components of the suite of BCP documents to be identified.

10.1 Determine recovery options

The possible options for recovery should be documented and presented to the BC Steering Committee. The options will build on the BIA results and will outline how ICT and IS can continue to meet the organisation's objectives, obligations and statutory duties in a cost-effective manner, despite an incident which affects their ability to operate at normal levels.

Options should be determined for the following areas:

- Staff (including skills and knowledge)
- Premises (location(s) of work and locations where information is held)
- Technology (telephony, data, applications, systems)
- Supplies (materials and equipment)
- Stakeholders

It is quite likely that various issues will be identified as a result of Risk Assessment, Business Impact Analysis, hazard identification or from operational experience which, if not addressed, may represent continuity risks. These risks should be recorded in the Business Continuity Risk Register (see Section 11.8.2) and highlighted to the Business Continuity Steering Committee.

Examples of continuity risk might include:

- Records management – an issue regarding poor storage, archiving and retrieval of vital records has been identified which could lead to vital information not being available when it is required and leading to a regulatory or reputational risk
- Staff training - issues have been identified regarding low levels of multi-skilling, cross-training or succession planning. This could lead to a continuity risk if there were above average levels of sickness, industrial action or a key member of staff was unavailable for several weeks or months
- Back-up plan (where risks have been identified with respect to the back up of data and the recovery and restoration of that data)

Activity plans to address the continuity risks should be implemented and related work integrated to ensure that the deadline for the delivery of the BCP is achieved.

The options will depend on:

- Recovery Time Objectives for the critical processes
- Recovery Point Objectives for the critical data
- Interdependencies of components
- Costs of implementation of various options
- Consequences of inaction

It must be noted that the organisation should minimise the likelihood of implementing a solution which could be impacted by the same incident that caused the business disruption. For example relocating to a WARF which is only a few hundred metres down the road and which could be affected by the same power cut, telephony outage or flood as the organisation.

The strategies adopted for ICT and IS are often quite complex and will typically be one or a combination of the following alternate site options [BS 25999-1]:

- Provision made within the organisation (Budge Up, Displacement, Remote Working, Reciprocal Agreements)
- Services delivered to the organisation (mobile facilities or prefabricated units)
- Services provided externally by a third party e.g. Work Area Recovery Facilities (WARF) (dedicated, syndicated or shared seats)
- Mirrored sites which are identical to the primary sites in all technical aspects

There are several options available depending upon the organisation's technology strategy, and the solution can be complex. These options can be classified according to whether they are cold, warm or hot sites and their relative advantages and disadvantages can be seen in the following table:

Site	Cost	Hardware Equipment	Telecoms	Setup Time	Location
Cold	Low	None	None	Long	Fixed
Warm	Medium	Partial	Partial	Medium	Fixed
Hot	Medium/ High	Full	Full	Short	Fixed
Mobile	High	Dependent	Dependent	Dependent	Not Fixed
Mirrored	High	Full	Full	None	Fixed

Table 7 - Merits of different types of alternate site

In turn, the choice of these options will depend upon:

- RTOs for processes which support the critical activities identified in the business area BIAs
- a process RTO of several months may allow the organisation to chose to leave any decisions until after the event
- a process RTO of over a day or two may allow time for staff to be relocated to another site
- a process RTO of less than a day will require tactics that enable the activity to be taken on by staff at other locations, or quick relocation of affected staff
- Location and distance between technology sites
- Number of technology sites

- Remote access
- Unstaffed (dark) sites or staffed sites
- Telecoms connectivity and redundant routing
- The nature of failover (automatic or manual)
- Back up strategy (e.g. daily, weekly, monthly, CDs, tape, DASD[6] or RAID[7])
- Third party connectivity and external links

Further options may be selected to reduce the likelihood of an IT disruption and could include the following strategies:

- Geographical spread of technology
- Holding older equipment as emergency replacements or spares
- Additional risk mitigation for unique or long lead time equipment
- Cross training to ensure that there is more than one member of staff with key skills
- Succession plans so that the loss of a senior manager or the IT Director does not present a risk.

10.2 Agreement on recovery strategy

The chosen options will then be signed off by the BCSC and the BC Strategy will have been chosen. Any proactive measures put in place to mitigate the risk are fed back into the Risk Management strategy[8].

The strategies which are adopted for Business Continuity will, for some processes, be dependent upon the strategy for IT Service Continuity. For example if ICT Operations has decided that the best strategy for backing up and restoring the critical systems is to do a mirrored back up to a WARF, the business processes who use those systems will then recover to desks in the WARF if their building becomes unavailable or access to the systems is denied. The strategy for staff in ICT Operations will also be to recover to the WARF, as they will be required to restore the data back ups and provide workstations for use by the staff recovering to the WARF site to maintain and to provide ongoing support.

A Help Desk facility may have to restore to another site within the organisation if they have complex telephony which makes it difficult or expensive to relocate to a WARF, and this in turn will govern where some of the Telephony Team will relocate following an incident.

As discussed by Thomas Carroll in The Definitive Handbook of Business Continuity Management [DH BCM], all organisations are careful about expenditure and budget will nearly always be a limiting factor on the solution or options that are implemented to protect the organisation. It does not make sense to implement an expensive solution for a loss which may have little value to the business or a solution which enables an RTO of minutes when days are required.

The following graph shows the relationship between RTO and cost and when determining the strategy for recovery an acceptable combination between the cost to recover, the

[6] Direct Access Storage device
[7] Redundant Array of Independent Disks
[8] In order to maintain readability, we do not show graphically this relationship within Figure 8.

cost of impact and RTO should be determined, so the chosen solution can be justified on a cost/benefit basis.

Error! Not a valid link.

Figure 18 - Recovery cost vs RTO[9]

The next step is to prepare a project plan for implementing the strategy and to design the BCP.

10.3 Design BCP

Once the strategies have been determined and any continuity risks have been addressed, the organisation should decide how it wishes to present the BCP.

The BCP should at a minimum cater to three sets of activities, which correlate to the three phases of an incident, as shown in Figure 19.

- ***Respond*** to an incident, emergency or disaster;
- ***Recover*** business-critical activities (this may include interim workarounds in the absence of essential technology);
- ***Resume*** normal working of all business operations from the temporary measures adopted during recovery.

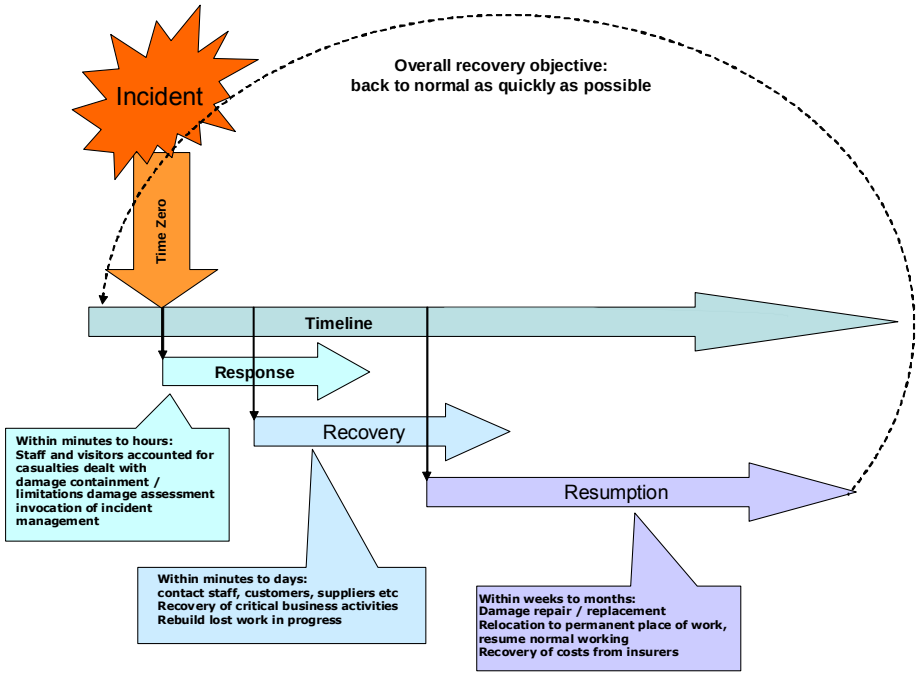


Figure 19 - The Incident timeline (based on [BS 25999-1])

10.3.1 Suite of documents

The suite of documents comprising the BCP will vary from organisation to organisation, but it is recommended that the following plans be considered. In smaller organisations

[9] Adapted from Figure 3.3: Recovery cost balancing [NIST 800-34].

these plans might be combined into one, but in larger organisations they will probably either exist as separate entities or some of the plans may be combined together.

Plan	Incident Timeline	Purpose of Plan	Used by
Incident Response Plan	Response	To manage the immediate aftermath of an incident, including evacuation, liaison with the emergency services and health, safety and welfare of the staff and public	Incident Response Team
Incident Management Plan	Recovery	To centrally manage the incident and ensure that the teams effecting recovery are equipped with their critical resources	Silver Team
Business Recovery Plans	Recovery	To provide the teams who are recovering their critical processes, with the necessary action lists, information, procedures and contact details	Bronze Teams
Recovery Support Plans – HR Plan – Facilities Plan – Health and Safety Plan	Recovery	To provide the teams who have specialist roles in an incident with the necessary information and procedures to be able to support the bronze recovery teams	Bronze Teams
IT Service Continuity Plan	Recovery and Resumption	To detail the actions that ICT and IS should follow in order to restore the critical components to the critical processes within the agreed component RTOs and RPOs	ICT and IS
Communications and Media Plan	Response, Recovery and Resumption	This plan contains all the information necessary to enable the Communication and Media Team to communicate accurately and effectively with the staff, customers, public, suppliers and media	Gold, Silver and Bronze Teams
Business Resumption Plan	Resumption	This plan details the procedures to follow to bring the organisation back to normal. It may be one plan or a series of plans and could include long term project plans	Gold, Silver and Bronze Teams

Table 8 - The use of the constituent parts of the BCP during each phase of an incident

A further illustration of the relationship between the plans comprising the BCP and the phases of recovery are shown in the diagram below.

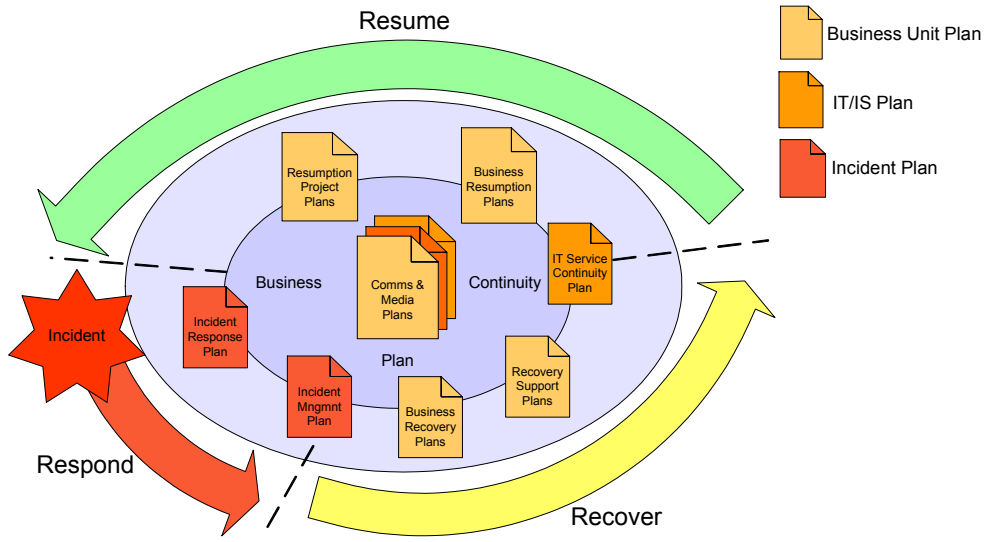


Figure 20 - The inter-relationship between the constituent plans in the BCP and the incident timeline

When BC is introduced into an organisation one of the results is the production of a number of documents, not all of which are necessarily included in the BCP (e.g. a number of policies and procedures such as HR policies). The BCP can be used in isolation to effect recovery in the event of an incident affecting the organisation but in reality it interacts with other documents in the areas of Risk Management, Information Security, HR/Health and Safety policies and ITSC.

The following diagram shows the relationship between the potential plethora of documents and their relative ownership.

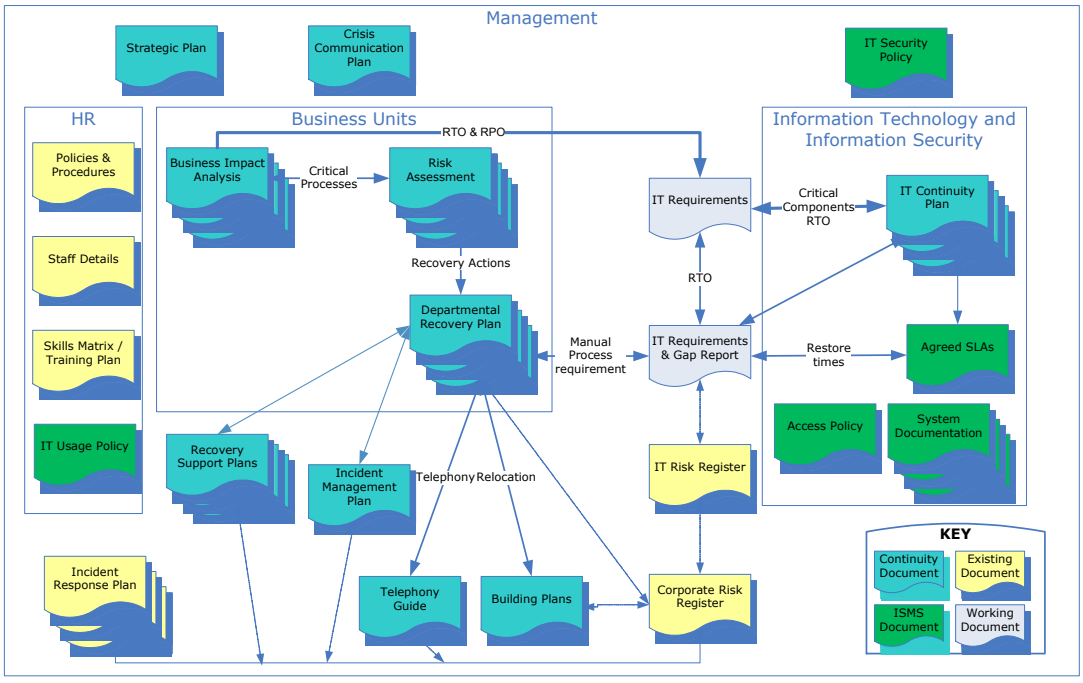


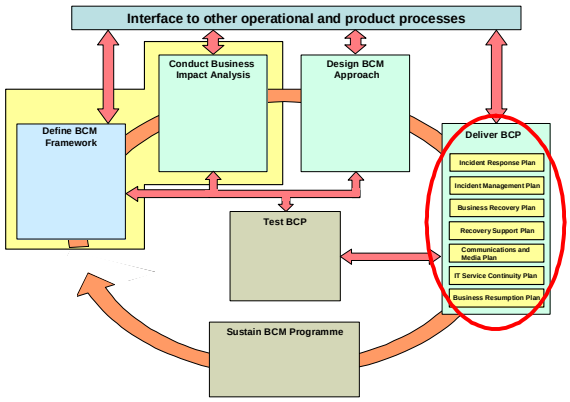
Figure 21 - Relationship of BC/Risk/ITSCM/ISMS documents

Some of the documents and processes already in place will require modification as different information is required e.g. HR will need next of kin information with current

contact details, this system will require change management process to ensure the information is current, an information security policy to ensure that it is not widely accessible and BC to ensure that the information is available during an incident involving the information repository.

The details of the interfaces between these programmes (ISMS, ITSCM, BCM, RM) is dependent on the organisation and method of implementation.

11 Deliver BCP



Once the strategy has been written and the design of the suite of documents comprising the BCP has been determined the Plans can be written.

These documents each serve a different purpose and range from detailing how the incident will be managed by the incident management team, to the tasks which HR, Facilities, Health and Safety and possibly other support functions will carry out to support recovery.

The plans also detail how communications internally and externally will be handled.

It should be noted that the following plans are only suggestions based on a combination of authors' experience and the recommendations of a variety of BC Standards.

11.1 Incident Response Plan

The Incident Response Plan is concerned with the immediate aftermath of an incident and is primarily concerned with keeping people safe. This plan would normally be written by Health and Safety and Security with assistance from the Business Continuity Manager, but ICT and IS should ensure that there is a plan, especially if they are the sole occupants of a building.

The Incident Response Plan should give details of:

- The structure of the Incident Response Team
- Members of the Emergency Response Team
- Roles and responsibilities of the Incident Response Team
- Muster Points
- Decision making process and escalation

In addition the Incident Response Plan should detail procedures to:

- Evacuate the building or shelter in site ("invacuate")
- Move evacuated staff to a safe site
- Liaise with the emergency services
- Stabilise the situation immediately following a incident
- Communicate with people affected by the incident or impending incident – this may include the public and neighbours
- Mobilisation of first aid, safety and evacuation assistance teams
- Account for those who were on site or in the immediate vicinity
- Locate safe site including details for accessing it
- Incident Room location and details for accessing it
- Interact with external agencies and regulatory authorities
- Ensure security or personnel, information and physical premises
- Assess the situation

11.2 Incident Management Plan

This plan details how the incident will be managed from occurrence to back-to-normal operation and provides information about the structure of the Incident Management Team, the criteria for invoking Business Continuity, the management of the incident, resource requirements, any necessary staff movements and critical processes.

PAS 77 suggests that a tiered incident management structure be established that is in line with that used by both public and private sector companies. Figure 11 shows how this three-tiered structure is implemented in the UK.

In outline the IMP should contain:

- Background
- Scope and purpose of document
- Relationship to other plans
- Definition of the Incident Response structure
- Handover from the Emergency Response Team
- Procedure for assessing the situation
- Roles and responsibilities of the Incident Management Team. Only incident roles should be used throughout the document – not names
- Incident Room location and details for accessing it
- Location of an alternate Incident Room
- Invocation criteria
- Invocation procedure including rendezvous points and responsible persons
- Procedure for setting up and managing the Incident Room (this should include a list of the required equipment, procedures and responsibilities for setting up PCs, telephones, teleconferencing or video-conferencing facilities, the layout of the room, location of a quiet room, details about catering arrangements, shift lengths, telephone numbers and so on.) If the room is normally a meeting room it is sometimes beneficial to prepare a notice for the door, stating that in the case of an incident the room must be vacated immediately
- Action plans for implementing the Business Continuity response – it is helpful if these are included as a checklist and have a box for ticking that the action has been completed. Sometimes it is useful if action checklists are written for each member of the team separately so they can be printed and handed to each individual
- Recovery Profiles – these detail the critical activities to be recovered, the number of staff involved and their alternate location. The critical resource requirements for each critical activity will also be detailed and the timescale in which they are required
- Resumption Process – this details how the organisation can resume normal operations following recovery of the critical processes. This may be a separate document or the organisation can decide how to manage this at the time once the critical processes are operational and the organisation has stabilised
- Details of equipment storage
- Maps and directions to all locations mentioned in the Plan
- Site access plans
- Claims management procedure
- Charts, plans (e.g. floor plans), photographs and other information which might be useful

- Contact information. This section can include the names of the staff in each role and should also include at least one deputy.
  - Senior Management Team (gold)
  - Incident Management Team (silver)
  - Bronze Team Leaders (all departments within the organisation)
  - External suppliers
  - Internal contacts
  - Regulatory bodies
  - Useful local information (e.g. hospital, doctors, plumbers, electrician, local council)
  - Neighbours
  - stakeholders
- Communications Matrix
- Incident Log
- Incident Management stand-down procedures
  - Decision to stand down
  - Who to communicate with
  - Filing of paperwork
  - Post incident report

11.3 Business Recovery Plans

Business Recovery Plans are the plans used by the bronze or operational teams following an incident which affects their ability to operate normally. They provide the information for the ICT or IS teams to recover their processes in order for the IT Service Continuity Plan to be put into action. If necessary the critical business units affected by the incident and who are suffering a loss of critical technology or information will also activate their Business Recovery Plans.

The Business Recovery Plans should include:

- Background
- Scope and purpose of document
- Relationship to other plans
- Definition of the Business Unit Team
- Roles and responsibilities of the Business Unit Team. Only incident roles should be used throughout the document – not names
- Procedure for assessing the situation
- Incident Room contact information
- Invocation criteria
- Escalation criteria
- Invocation procedure including rendezvous points and responsible persons
- Action plans for implementing the Business Continuity response – it is helpful if these are included as a checklist and have a box for ticking that the action has been completed. Sometimes it is useful if action checklists are written for each member of the team separately so they can be printed off and handed to each individual. These action lists should cover the loss of each critical resource i.e. equipment, materials, technology and information, staff and buildings
- Recovery Profiles – these detail the critical activities to be recovered, the number of staff involved and their alternate location. The critical resource requirements for

each critical activity will also be detailed and the timescale in which they are required
- Details of equipment storage
- Maps and directions to all locations mentioned in the Plan
- Incident Log
- Communications Matrix
- Contact information – this section can include the names of the staff in each role and should also include at least one deputy
  - Incident Management Team (silver)
  - Other Bronze Team Leaders
  - External suppliers
  - Internal contacts
  - Regulatory bodies
  - Useful local information (e.g. hospital, doctors, plumbers, electrician, local council)
- Recovery stand down procedures
  - Decision to stand down
  - Who to communicate with
  - Filing of paperwork
  - Post incident report

11.4 Recovery Support Plans

Recovery Support Plans are aimed at the teams who have a supporting role to the organisation and who, during an incident, would have very specific roles to play. They include, but are not limited to:

- Human Resources
- Facilities
- Health and Safety
- Security
- Legal
- Alternate Site Co-ordination
- Original Site Salvage
- Damage Assessment

The ICT/IS Incident Management Team should be aware of these plans and enlist the help of these departments if required. Representatives can be co-opted onto the ICT Incident Management Team, but if the incident has a far-reaching affect, it is advisable to invoke the organisation-wide Incident Management Team which automatically includes the managers from these teams.

11.5 Communications and Media Plan

NFPA 1600 suggests that procedures should be developed to disseminate and respond to requests for pre-incident, incident and post-incident information, as well as to provide information to internal and external audiences including the media, and to respond to their enquiries.

Organisations should also establish and maintain the capability to provides accurate and up to date information for the organisation and the public which includes:

- Central contact point for the media
- Systems for gathering, monitoring and disseminating emergency information
- Pre-scripted information bulletins for potential disruption scenarios
- Method to co-ordinate and clear information for release
- Identification of the audience for communications (e.g. stakeholders, key customers, staff, emergency services, suppliers, families, regulators, government ministers etc)
- Policies for communicating with the audience
- Policies for communicating with special needs populations
- Ongoing employee/customer communications and safety briefings
- Protective action guidelines (e.g. shelter at site, evacuation, move to safe site)
- Advice to the public through appropriate agencies concerning threats to the people, property and the environment
- Definition of the means and frequency with which information will be provided

BS 25999-1 also suggests that a suitable venue should be established to support liaison with the media and other stakeholder groups and that appropriate numbers of trained, competent spokespeople should be nominated and authorised to release information to the media.

A communications (or audience) matrix should be written to summarise key information about the audience including who should communicate with each group. The key points of the message could also be noted in this matrix. It is useful to include this tool in all plans, to avoid confusion over who communicates with whom.

11.6 IT Service Continuity Plan

The Information Technology Service Continuity Plan is the collection of policies, standards, procedures and tools through which organisations not only improve their ability to respond when major system failures occur, but also improve their resilience to major incidents, ensuring that critical systems and services do not fail or that failures are recovered within acceptable process RTO limits.

BIA information is used to define the process RTO and determine the recovery prioritisation. This makes the recovery process a user-centric activity matching business requirements.

The recovery plans are organized in a hierarchy. A site loss plan details the systems which would be affected by the loss of a building. A separate plan for each service should provide detailed procedures and step-by-step guidelines for each stage of an incident so that the Recovery Teams are able to restore the services and thereby to meet the agreed process and component RTOs.

The plans should be clear and concise and expect a level of knowledge but not presume explicit local knowledge, in the event that external assistance is required to rebuild systems (the same is true of Disaster Recovery Plans). Each procedure should be self-contained so that it can be utilised to effect recovery of a single system or component (e.g. the server is running successfully but the database management system has crashed). Each document must also contain details of pre-requisites; this means that in the event of multiple component failures the correct sequence can be followed (e.g.

replace failed disk, rebuild operating system, install database, configure security settings and then restore data).

In summary the IT Service Continuity Plan should typically contain the following information:

- Details of the combined component RTOs and RPOs and inclusion of the IT Requirements Gap Analysis
- IT Architecture
- Roles and Responsibilities
- Invocation Procedures
- Damage Assessment
- Escalation and process flow charts
- Detailed procedures specifying how to recover each component of the IT system
- Test Plans specifying how to test that each component has been recovered successfully
- Incident Logs
- Contact Details
- Fail-back procedures
- IT Test Plan

These plans detail the four stages:

- Initial response: damage assessment and invocation of the appropriate incident management teams.
- Service recovery: this maybe staged and offer a degraded service.
- Service delivery in abnormal circumstances: interim measures may include relocation of services to another site or utilisation of spare equipment (often training or test servers). This is a temporary measure to provide a limited service until normal service can be resumed.
- Normal service resumption: returning to the usual service, fail-back from the abnormal service delivery.

PAS 77 also details strategy and infrastructure improvements to improve resilience. Improving the environment is a proactive measure to minimise the risk of IT outages. The strategy is a phased approach to achieving that resilience. It is driven by budgets, risk, experiences and changing user requirements. Experience comes from implementation, testing and failures. The three criteria they use for strategy are component RTO, RPO and cost; introducing measures to reduce component RTO and get to a stable RPO can be very costly in time, resources and finances for new technology.

If an ITSC Plan is successful then its success is difficult to measure. Any incident will be recovered within the process RTO and will not invoke a BC incident. The only measurement is the reduction of downtime and improvement to SLA adherence.

11.7 Business Resumption Plan

Business Resumption Plans (BRP) are defined in NIST 800-34, BS 25999-1, APS 232, NFPA 1600, COBiT, HB 292-2006 and PAS 77. This plan details how the business unit can resume normal operations following recovery of their critical processes. This may be a separate document or the business may decide how to manage this at the time that

critical processes are operational and the organisation has stabilised (PAS 77 refers to this process as 'fail-back').

While Business Continuity may necessarily involve adopting temporary measures (such as office relocation, reduction of working hours, reduction of staffing levels and/or usage of backup IT systems), business resumption is concerned with restoring operations to as near normal levels as possible.

The upheaval of relocating, changing IT systems, etc. can be as traumatic to an organisation as the BC event which invoked plans in the first place. One advantage of the resumption process is that it can be scheduled to cause minimum disruption through correct planning.

Resumption may be to the original site or to a new location (depending on the damage sustained) and will need to be treated as a work programme in its own right, utilising the information from the resource matrices to develop a programme plan for reinstating normal operations in order of priority. The plan details the sequence, parties involved and other considerations (security, various timings, intermediate measures, communication, etc).

The Office of the Chief Information Officer (US Government) states that "Development of the Business Resumption Plan should be coordinated with Disaster Recovery Plan and Business Continuity Plan".

11.8 Supporting Documents

The following documents are not formally part of the BCP in any standard but experience shows that they are necessary in order to support the process:

11.8.1 IT Requirements & Gap Analysis

These two documents are working documents which are the liaison between BC and ITSCM. ITDR does not take this into consideration. Although these documents are not defined in any specifications the Requirements document is implied in ITIL. From a practical perspective they are important as they are the formal specification of requirements and the risk response and as such require a high-level sign-off from senior management.

The IT Requirements are the details taken from the BIAs. This lists the applications and IT components in general, and for each relevant IT component an RTO and RPO dictated by each critical process. This information is used to determine the critical components and their RTOs. This will ultimately drive the Service Catalogue, Service Level Agreements and IT Strategy as well as the ITSC Plans.

ICT are not always able to meet these requirements due to the current infrastructure. This leads to a Gap Analysis report which highlights the gaps (see Figure 17). The BCSC (or senior management) can then decide how to mitigate the risk. This may either be a strategic decision to upgrade the infrastructure (at some cost) or the Business Units may have to provide manual workarounds to meet the actual recovery time. Items from the Gap Analysis are logged in the Risk Register.

11.8.2 Risk Registers

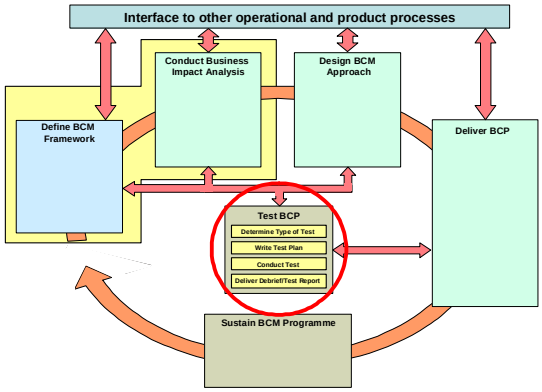
The Corporate Risk Register contains details of all of the risks to the organisation. It is a tool that captures, describes and assesses risks as they are identified, together with risk accountabilities, actions where required, review dates and dates when actions were completed and the risk item closed [BS 31100].

A Business Continuity Risk Register will include the date of the last assessment, a description of the risk, an estimate of the impact and the likelihood, any mitigating controls, and a statement of action required, with target date and owner. A properly maintained risk register provides a useful vehicle for communication [ISO 27000].

The IT Risk Register records the risks identified with Information Technology and Information Systems. While many companies will bundle this into the Corporate Risk Register, larger organisations tend to have one Register per department with the highest severity risks being promoted to the Corporate Risk Register.

These Risk Registers are owned by the senior management team since the acceptance of risks contained therein is not the responsibility of ICT, given that some of the risks will affect business areas.

12 Test BCP



BS 25999-1 states that an organisation's Business Continuity and Incident Management arrangements cannot be considered reliable until tested. Testing is essential to develop teamwork, competence, confidence and knowledge all of which are vital at the time of an incident.

ISO 27002 expands this further by stating that the tests should ensure that all members of the recovery teams and other relevant staff are aware of the plans and of their responsibility for Business Continuity and Information security as well as know their role when a plan is invoked.

12.1 Determine type of test

There are many ways of testing that a BCP is fit for purpose and the table below describes a number of these methods. The method chosen will depend on the maturity of BCM within the organisation and the testing which has been conducted before. It would not be a good idea to opt for a full rehearsal if the BCP has not been tested before.

In some case, it would be a good idea to appoint some of the people involved (employees and also trusted external consultants) in the role of facilitator and observer to help conducting and understanding the test.

The facilitator runs the test or exercise, but does not take an active part. He will brief the participants on the objectives of the test and will set the scene of the scenario. During the test, the facilitator co-ordinates the test activities (e.g. phone calls, playing of mock radio/TV broadcasts) and ensures that the test runs to time. After the test the facilitator will run a debriefing session and be responsible for writing a Test Report.

An observer observes the test and takes no part in the test at all. He records the outcomes of the test, as it progresses, against the critical success criteria for the test. He will assist in the debriefing session by summarising the key points observed and will pass their results to the facilitator to enable the Test Report to be written.

Type of test	Function of test	Participants	Minimum frequency	Complexity
Desk check	Challenge and QA content of the BCP	Author of plan Another manager	On completion of a plan	Low . . . .
Desktop walkthrough	Challenge content of BCP	Author of plan and main participants in plan	Annually or twice yearly	
Desktop scenario	Use a scenario to walk through the plan to validate that the BCP contains both necessary and sufficient information to enable a successful recovery	Participants in plan Observers Facilitators	Annually or twice yearly	
Call out	Test that the contact	Staff on the	Annually or	

Type of test	Function of test	Participants	Minimum frequency	Complexity
communications	numbers for the people on the call out list are up to date and they know how to respond	call out lists	twice yearly	. . . . Medium
Scenario exercise	Use a scenario to role play the management of an incident to test that the IMP and associated plans will work. These exercises can be run to test the bronze, silver or gold teams	Participants in plans Observers Facilitators	Annually or twice yearly	
Technical Testing	Testing that the information and technology systems can be restored effectively at the alternate sites	ICT Recovery Teams WARF teams if appropriate Observers	Annually	. . . .
Activity Testing	Moves business activities to their alternate sites for a fixed time to test that they can access their systems, information, equipment and materials and carry out their critical processes	Business Recovery Teams WARF teams if appropriate Observers	Annually	. . . .
Complete Rehearsal	Shut down an entire building and sends critical staff to their relocation sites	All staff in building Gold, silver and bronze teams Observers Facilitators	Annually	. . . . . High

Table 9 - Business Continuity testing: types, function and frequency (Based on [PAS 77], [BS25999-1] and Elliot, Herbane and Swartz Handbook [EHS BCM])

12.2 Write test plan

To derive the most value from a test a Test Plan should be developed to define the selected elements against explicit test objectives and success criteria. The test plan should contain a schedule detailing the time frames for each test and test participants and should clearly delineate scope, objectives, scenario and logistics.

The scenario should be as realistic as possible to test the plan properly and gain maximum support from the participants. In some tests it is appropriate to seek involvement from outside personnel such as emergency services, security, the Local Authority emergency planning officer, subject experts and suppliers

Questionnaires should be prepared for observers so they can record their observations during the test.

12.3 Conduct test

Prior to the test the participants should be provided with the necessary information and briefed about the ‘situation’.

The participants take part in the test using the relevant plans, which is facilitated by the Facilitator. The Observers will determine which aspects of the test they are observing and record what they see and hear on the questionnaire.

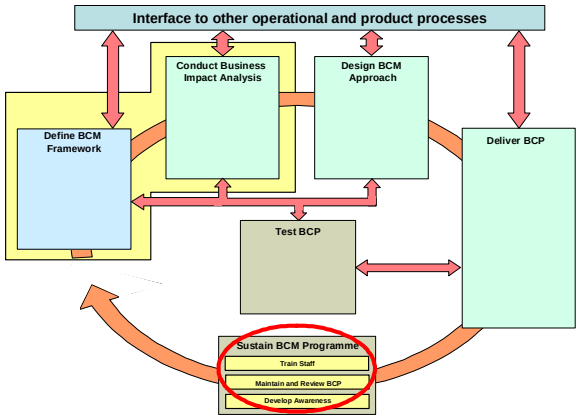
After the test the Facilitator and Observers should get together to document the outputs from the test and identify key learning outcomes and potential improvement actions.

12.4 Deliver debrief and test report

As soon as possible after the test a debriefing should be conducted where the participants say what they felt went well, what went badly and where their response could be improved. The debriefing should include all participants, the observers and those with responsibility for plan maintenance or future activation. At the end of the debriefing responsibilities for plan improvement activities should be assigned.

The final deliverable is a Test Report outlining the scope, approach, method and results of the test with the recommendations for action and the action owners. The audience for this report should be the BC Steering Committee.

13 Sustain BCM Programme



Plans can get out of date very rapidly (particularly contact lists) and even after a few weeks, if not updated, the effectiveness and relevance of plans can begin to deteriorate.

Following implementation of the tested BCP, it is therefore necessary to keep the plan up to date, ensure that all the staff involved with ongoing BCM or incident response and management have been trained in their roles and awareness of BCM is raised at all levels throughout the organisation.

13.1 Train staff

[NIST 800-34] advises that training for personnel with Business Continuity responsibilities should complement testing. Training should be provided at least annually; new staff who will have plan responsibilities should received training shortly after they are hired. Ultimately personnel must be trained to the point that they are able to execute their respective incident response and incident management procedures without the aid of the documents.

Training should encompass:

- Purpose of the plan
- Cross team co-ordination and communication
- Reporting procedures
- Security arrangements
- Team specific processes
- Individual responsibilities

[TR 19:2005] recommends that training be aimed also at specific groups, namely:

Target	Description
All staff	Basic awareness training which gives the staff an insight into basic Business Continuity and informs them about their Business Recovery Plans and what will happen to them during an incident
Management Team	Management training to inform managers about the overall incident response and management, the purpose of their Business Recovery Plans, what they will be expected to do during an incident and how they will implement their plans
Business Continuity and Incident Personnel	Specialised training to train all staff involved in incident response, management and recovery. This will probably involve a number of different training courses. Scenario exercises as mentioned in Section 12.1 are a good way of training staff following a classroom session.

Table 10 - Business Continuity Management training levels

Examples of the types of training courses which could be delivered to the staff in the third group are:

- Evacuation
- Media communications (aimed at spokespeople)
- Establishing an Incident Room
- Managing an incident
- Crisis communications
- Working from alternate sites

Training should also be provided for the staff who will form the Business Continuity Management Team, which should cover:

- Programme management
- Conducting a BIA
- Designing and implementing BCPs
- Risk and threat evaluation
- Designing tests and exercises

The Business Continuity training programme should be embedded within the organisation's training and development programme and form part of staff personal development plans. Details of the specific training and its frequency (taking into account refresher training as well as training new members of the team) should be included in a Training Manual that is part of the organisation's training portfolio.

Ideally, general Business Continuity training is included within the induction programme so that all staff are made aware of Business Continuity from the start of their career.

13.2 Maintain and review BCP

The programme should ensure that any changes (internal or external) which impact the organisation are reviewed in relation to BCM. It should also identify any new products and services and their dependent activities which need to be included in the BCM maintenance programme.

If there are any major business changes, a revision of the BIA ought to be undertaken. The other components of the BCM programme may be amended to take account of these changes.

The organisation's top management should, at intervals that it deems appropriate, review the organisation's BCM capability to ensure its continuing suitability, adequacy and effectiveness. This review should be documented and should ensure that within the BCM programme:

- All key products and services and their supporting critical activities and resources have been identified and included in the BCM strategy;
- The BCM policy, strategies, framework and plans accurately reflect priorities and requirements;
- The BCM competence and capability are effective and fit for purpose and will allow management command, control and co-ordination of an incident;
- The BCM solutions are effective, fit for purpose and appropriate to the level of risk faced by the organisation;

- BCM strategies and plans incorporate improvements identified during incidents and exercises as well as in the maintenance programme;
- The organisation has an ongoing programme for BCM awareness and training;
- BCM procedures have been effectively communicated to relevant staff, who understand their roles and responsibilities;
- The BCM maintenance and exercising programmes have been effectively implemented;
- Change control processes are in place and operate effectively.

Details of the review periods and frequency of testing and training may be included in a separate Maintenance and Review document. This document specifies how and when the BCP will be reviewed and tested and the process for maintaining the plan. The intervals between tests and reviews will depend on the organisation, its complexity and rate of change. A training schedule may also be included.

The organisation should provide for the independent audit of its BCM competence and capability to identify actual and potential shortcomings. Independent audits can be conducted by competent external or internal persons.

The BCP may contain sensitive information (e.g. Executive contact numbers or location of vital records) which should be appropriately protected. Copies of the BCP should be stored in a remote location, at a sufficient distance to escape any damage from an incident at the main site. Management should ensure that copies of the BCP are up to date and protected with the same level of security as applied at the main site [ISO 27002].

Once BCM has been embedded into the organisation as an ongoing management process it enters an iterative cycle; being reviewed at regular intervals and updated when necessary.

13.2.1 Change Management

Changes to the BCP which have been identified as a result of exercising, testing, training or organisational developments cannot be made without passing through the Change Management process. What may seem to be small changes at the business unit level can have significant impacts on the BCP in other areas.

The changes must be approved by the Business Continuity Manager and if necessary go before the BC Steering Committee for final approval. The Business Continuity Manager will be responsible for issuing the changes in accordance with the organisation's procedures for document and version control.

13.2.2 Continuous Improvement

Continuous improvement, in regard to organisational quality and performance, focuses on improving customer satisfaction through continuous and incremental improvements to processes, including the removal of unnecessary activities and variations. Business Continuity Management should therefore be included as part of the continuous improvement process to ensure that it remains effective and workable and is embraced by every member of staff at all levels within the organisation.

13.3 Develop Awareness

It is necessary to communicate the Business Continuity message to all staff so that they are informed about the key principles of Business Continuity. This will embed it into the

business culture so that it becomes second nature and is part of the organisation's core values and effective management.
There are various ways in which the information can be communicated:

- Training courses
- Induction training
- Scenario exercises and tests
- Articles in the organisation's newsletter
- Visits to WARF
- Inclusion on intranet
- Agenda item on team meetings

Throughout the BCM programme and in the subsequent BCM maintenance cycle, staff at all levels should be consulted about Business Continuity and their ideas, if approved, incorporated in the BCP.

14 Bibliography

ANAO	The Australian National Audit Office. Audit Report No. 53 2002-2003. Business Continuity Management Follow-on Audit
APRA	Australian Prudential Regulatory Authority http://www.apra.gov.au
APS 232	Australian Prudential Regulatory Authority - APS 232, 2005, Business Continuity Management.
BASEL II	Basel Committee on Banking Supervision, Risk Management Principles for Electronic Banking, May 2001 www.bis.org
BCI GPG	Business Continuity Institute Good Practice Guidelines 2007 - A Management Guide to Implementing Global Good Practice in Business Continuity Management
BILL 198	3rd Session, 37th Legislature, Ontario 51 Elizabeth II 2002. Bill 198 – Chapter 22, Statutes of Ontario, 2002. An Act to Implement Budget Measures and Other Initiatives of the Government. http://www.ontla.on.ca/bills/bills-files/38_Parliament/Session2/b198.pdf
BS 7799-3	British Standards Institute. BS 7799-3:2006. Information Management Systems - Part 3: Guidelines for Information Security Risk Management
BS 31100	British Standards Institute. BS 31100 – Code of Practice for Risk Management
BS 25999-1	British Standards Institute. BS 25999-1. Business Continuity Management.
CC ACT	Statutory Instruments No. 2042, 2005. The Civil Contingencies Act 2004 Regulations 2005. http://www.co-ordination.gov.uk/upload/assets/www.ukresilience.info/finalregs.pdf UK Act of Parliament. The Civil Contingencies Act 2004 – Chapter 36. http://www.opsi.gov.uk/acts/acts2004/ukpga_20040036_en_1
COBIT	CobiT, Control Objectives for Information and related Technology, IT Governance Institute www.isaca.org
DH BCM	The Definitive Handbook of Business Continuity Management Andrew Hiles (Editor), Peter Barnes (Editor)

John Wiley & Sons Ltd, London - 2001
ISBN: 978-0-471-48559-9

ENISA Regulation — Regulation EC no 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency
www.enisa.europa.eu

ENISA RM — ENISA Report - Risk Management: Implementation Principles and Inventories for Risk Management/Risk Assessment Methods and Tools, 2006
http://www.enisa.europa.eu/rmra/files/D1_Inventory_of_Methods_Risk_Management_Final.pdf

FEMA — Federal Emergency Management Agency (FEMA) - U.S. Department of Homeland Security
Emergency Management Guide for Business & Industry

http://www.fema.gov/business/guide/index.shtm

FSA — Financial Services Agency (UK). Business Continuity Management Practice Guide, 2006.
www.fsa.gov.uk

HB 221-2004 — Standards Australia/Standards New Zealand. HB 221-2004, Business Continuity Management.

HB 254-2005 — Standards Australia/Standards New Zealand. HB 254-2005. Handbook. Governance, Risk Management and Control Assurance

HB 292-2006 — Standards Australia/Standards New Zealand. HB 292-2006. Handbook. A Practitioners Guide to Business Continuity Management.

HB 293-2006 — Standards Australia/Standards New Zealand. HB 293-2006. Handbook. Executive Guide to Business Continuity Management.

EHS BCM — Dominic Elliott, Brahim Herbane, Ethne Swartz
Business Continuity Management: A Crisis Management Approach
Routledge Editions - 2006
ISBN-13: 978-0415371087

ISO 27000 — ISO/IEC 27000 family - Information technology - Security techniques - Information security management systems - Overview and vocabulary

ISO 27001 — ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems – Requirements

ISO 27002 — ISO/IEC 27001:2005 - Information technology - Security techniques - Code of practice for information security management.

IT Grundschutz	BSI Standard 100-2: 2005 - BSI-Empfehlungen des zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit www.bsi.de
ITIL	Information Technology Infrastructure Library. ITIL v3; OGC – UK Office of Government Commerce www.ogc.gov.uk Also referred in: ISO/IEC 20000:2005, Information technology - Service management www.iso.ch
NFPA	National Fire Protection Association. NFPA 1600. Standard on Disaster/Emergency Management and Business Continuity Programs. 2007 Edition
NIST	National Institute of Science and Technology. NIST SP 800-34. Contingency Planning Guide for Information Technology Systems
PAS 77	British Standards Institute. Publicly Available Specification PAS 77: 2006. IT Service Continuity Management Code of Practice
PDD 67	Presidential Decision Directives. PDD-NSC-67 – Enduring Constitutional Government and Continuity of Government Operations (U). 21 October 1998. http://www.fas.org/irp/offdocs/pdd/pdd-67.htm
SOX	107th Congress of USA - Sarbanes-Oxley Act of 2002, H.R. 3763. An Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes, 23 January 2002 http://www.sarbanes-oxley.com/search.php?q=sarbanes+oxley+act
TR 19:2005	Spring Singapore Technical Reference. TR 19:2005. Technical Reference for Business Continuity Management

14.1 Standards under development

- International Standards Organisation. ISO/PAS 22399 – Societal Security - Guideline for Incident Preparedness and Operational Continuity Management

- Bundesamt für Sicherheit in der Informationsverarbeitung (Federal Office for Security in Information Technology). BSI Standard 100-4.

- British Standards Institute. BS 25777. IT Service Continuity.

- International Standards Organisation. ISO/IEC FDIS 24762:2007(E) - Information Technology - Security Techniques - Guidelines for Information and Communications Technology Disaster Recovery Services.

15 Websites

Website	Background
www.thebci.org	Business Continuity Institute – information on BC standards, good practice, training courses, Forums and certification
www.itil.org.uk	IT Infrastructure Library – information on the various parts of the handbook
www.drj.com	Disaster Recovery Journal
www.continuitycentral.com	Current BC news, topics, white papers and recruitment
www.contingencyplanning.com	Contingency Planning and Management
www.drii.org	Disaster Recovery Institute International
www.docleaf.com	Crisis management concentrating on the human aspect
www.bsi.de	German Federal Office for Security in Information Technology (Bundesamt fur Sicherheit in der Informationstechnik)
www.ukresilience.info	UK Government website for civil protection practitioners
www.preparingforemergencies.gov.uk	UK website on preparing for emergencies, aimed at businesses, the voluntary sector and the public
www.globalcontinuity.com	Global portal for Business Continuity, Disaster Recovery and Risk Management specialists.
www.continuityforum.org	The Continuity Forum provides independent advice, information and support to the private and public sectors covering all aspects of BCM, Disaster Recovery, Crisis Management, Emergency Planning and Security. It is an independent NGO that specialises in providing practical information, assistance and guidance to organisations of all types that need to create effective Business Continuity Management programmes
www.nasp.org.uk	National Association of Security Professionals. Providing information on worldwide security, private guarding, company guarding and close quarter protection
www.the-sia.org.uk	The Security Industry Association administers the licensing of the private security industry as set out in the Private Security Industry Act 2001. It also aims to raise standards of professionalism and skills within the

Website	Background
	private security industry and to promote widespread use of best practice
www.fsc.gov.uk	A website resource established by the UK's Tripartite Authorities (HM Treasury, the Bank of England and the Financial Services Authority) to provide a central point of information about work on continuity planning relevant to the UK's financial sector
www.epcollege.gov.uk	The Emergency Planning College is part of the UK government, established within the Civil Contingencies Secretariat (CCS) of the Cabinet Office
www.bs25999.com	Online resource for help and information regarding the standard for BC planning
www.itgovernance.co.uk	Specialist services and solutions for IT governance, Risk Management, compliance and information security
www.securityforum.org	The Information Security Forum (ISF) is the world's leading independent authority on information security
www.isfsecuritystandard.com	The Standard of Good Practice for Information Security (the Standard) is the foremost authority on information security
www.mi5.gov.uk	Current information on UK security threat level and portal to Preparing for the Unexpected
www.the-eps.org	The Emergency Planning Society
www.fema.gov	Agency of the US government tasked with Disaster Mitigation, Preparedness, Response & Recovery planning.

APPENDICES

Appendix A: Business Continuity for SME essentials

A.1 Introduction

For small businesses the potential impact of the risks they face is likely to be more destructive since the majority operate in specialised markets where even a short interruption to normal business can have a disproportionate effect – totally halting output and letting customers down. In addition it is more difficult fro small firms to absorb the financial impact of business interruption, making recovery more difficult even after a return to normal operations.

A.2 Implementing Business Continuity

A.2.1 Project Management

Writing a Business Continuity Plan should be treated just like any other project and a project manager should be appointed. This ensures that the plan is written to specification, within budget and on time, all critical targets for a small business.

A.2.2 Basic Emergency procedures

The first part of an effective Business Continuity Plan is the Emergency Procedures, and small businesses should ensure that:

- Employees understand the evacuation procedures;
- Employees know what to do if a fire breaks out;
- Employees know what to do if a colleague is injured;
- Roles and responsibilities have been assigned for evacuation and first aid;
- All staff have been trained in their roles;
- Alternate muster sites have been determined if it is not considered safe to remain close to the building;
- An indoor emergency muster site has been identified, so staff can remain together safe, warm and dry while the next steps are decided.

A.2.3 Identify threats, assess risks and quantify impacts of loss

Business Continuity is one method of risk treatment and before it can be decided what should be included in the Business Continuity Plan, it is necessary to understand the threats that the small business faces, the risks that these threats pose and the impact of loss should the risk occur. Although these risks may be similar to those faced by larger firms, the impact can be much worse.

Some of the threats which a business faces include (but are not limited to):

- Fire/flood
- Computer/telecoms failure
- Key equipment failure
- Personnel issues
- Denial of access
- Employee theft
- Email viruses
- Computer hacking
- Loss of data
- Product defects
- Bomb/terrorism threat
- Legal/regulatory action
- Utilities failure

Once the threats are understood, the risks can be identified and a risk score assigned, based upon the likelihood of their occurring and their potential impact. The risks should be recorded in a Risk Register in order of priority.

It is much more effective to manage risks proactively and to prevent them from occurring than to try to recover reactively from an unforeseen event. A prioritised list of risks allows a small business to see where their greatest risks lie and to determine where their efforts should be expended for active prevention.

A.2.4 Perform an impact assessment

The last part of this stage of the work is to identify the critical processes and to calculate how long the organisation could survive if they were not to be carried out. In this stage the following questions about the resources upon which critical processes depend are considered:

- Which buildings does the organisation work from?
- Can anyone in the organisation work from another location?
- Who are the critical staff?
- Can anyone else do their job (internal or external)?
- What is the reliance on internal and external information and data?
- What are the critical systems?
- What telephony system is used? What are the option if it fails?
- What servers do the critical systems run from?
- Where is the data stored?
- How often is the data backed up?
- What media is used to back up the critical information?
- Where is the data backed up?
- Who are the external suppliers?
- What are the suppliers' continuity arrangements?

The impact of the unavailability of any of the critical resources is to be calculated. For example, if the building were inaccessible, a system failed, critical data were lost or the telephones were to go down. The impact could be a loss of reputation, failure to provide goods or services on time thus incurring penalty charges, poor customer service, a health and safety issue or a beach of regulatory requirements.

A.2.5 Develop the recovery strategy

Once the organisation understands their key risks, knows what their critical processes are, for how long they could remain non-operational, and what would be the impact of a critical resource failing, a strategy can then be developed for dealing with continuity problems should they arise. Strategies should cover:

- Alternate working locations (this could be as simple as relocating to a Director's house);
- Access to the systems from the alternate location;
- Arranging for data back ups to be carried out automatically and stored off site;
- Enabling data back ups to be accessed from alternate locations;
- Enabling remote working;
- Cross training;
- Storage of installation disks so they can be accessed if the building is unavailable;
- Storing license keys, insurance details and employee information securely off site;
- Identification of an Emergency Operations centre;
- Priority of recovery of business processes;
- Priority of recovery of essential technology;
- Identification of alternate suppliers and establishing a supply contract with them;

- Maintain an up to date maintenance schedule for all equipment (technology, electrical, fire extinguishers, smoke alarms, emergency lighting etc...);
- Ensure that the building meets all local fire regulations;
- Document all critical processes;
- Archive information;
- Ensure that insurance details are up-to-date and decide whether to subscribe to business-interruption insurance.

A.2.6 Create a Business Continuity Plan

Despite risk prevention measures being implemented, problems will still occur and in order to ensure that these problems can be dealt with effectively while minimising the impact to the organisation, a Business Continuity Plan (BCP) should be written.

The Business Continuity Plan should cover:

- Emergency Response procedures (life, health, safety, exit routes, evacuation, emergency notifications, muster points etc…);
- Disaster Recovery (recovery and resumption of information systems hardware, software, data and network);
- Business Recovery (recovery and resumption of critical business processes).

It should be written to cover the worst-case scenario of business-operations interruption. This is often loss of premises.

A checklist of items to include in the BCP is given below:

- BC Project Manager's name and contact details
- Management team who will make key decisions
- Contact details to enable the team to be brought together
- Nominated control centre as a meeting point
- Identification of business critical processes
- Skills matrix
- Details of how a recovery would be phased (emergency response, recovery of critical processes, resumption of normal operations)
- Telephone divert arrangements
- Emergency contact number employees to obtain the latest information
- Resource requirements (people, work area, technology (IT and telecoms)
- Details of recovery resources
- Contacts for internal and external agencies committed to supporting the recovery efforts
- Address of the recovery site (this may be a reciprocal arrangement with a neighbour, a room in one of the Directors' houses, a meeting room in a management facility)
- Location of an internal shelter in case an evacuation is not possible
- Contents and storage location of a disaster pack
- List of key customers, suppliers, third parties and their contact details
- Comprehensive team cascade list
- Network diagrams and other technical information
- Precautions to be taken in the event of an incident (e.g. water shut off, how to power down the servers, gas supply shut off)
- Communications Plan (who will communicate with staff, customers, shareholders, the emergency services etc. and what they will say)

The organisation should work out whether the business is large enough to require recovery teams. For a business of approximately 20 employees or less, one plan should be sufficient with one team responsible for effecting recovery.

An organisation of 20 to 40 staff members may use four recovery teams, which cover:

- Emergency response and damage assessment
- Crisis management and administration
- Information systems and voice and data
- Core business and support function

A small business which has from 40 to 80 employees may use up to eight recovery teams:

- Emergency response
- Damage assessment and reconstruction
- Crisis management
- Administration
- Corporate support
- Information systems
- Voice and data
- Core business

Taking the recovery one stage further, an organisation of up to 140 employees may use the previously mentioned eight recovery teams, but split the core business team into three additional teams or they may wish to split the Information Systems team into two teams.

Therefore the bigger the business the more recovery teams will be required and each team will have a Team Leader and a deputy. The Team Leader is responsible for developing their own team's plan. Once the team plans are completely developed, the administrator needs to review each plan for accuracy and detail. The information gathered in the business impact assessment can be used as a reference point.

To support the emergency and recovery phases a supply kit should be created, which includes essential items in case of an emergency. This could include:

- Water
- Food
- First aid kit
- Torches
- Radio and batteries
- Pay-as-you go mobile phone and charger
- Tarpaulins
- Cleaning supplies
- Gloves (rubber and leather)
- Plastic bags
- Camera
- Tool kit
- Duct tape
- Blankets
- Business Continuity Plan
- Critical information (on a memory stick or CD)
- Paper copies of critical pro-formas and procedures

A.2.7 Test the Plan

Once the plan has been agreed it should be communicated to work teams. This will expose any flaws in the plan and will also ensure all the roles and responsibilities are understood. It is worth completing a test simulation of the plan to ensure that it will run smoothly if and when it is needed.

A.2.8 Regularly update the Plan

The plan should be reviewed at least every six months. It should be checked to make sure that it includes correct contact details for the recovery site, vital records, suppliers and the team.

The plan should be distributed to everyone with assigned responsibility and these individuals should be advised to keep copies off-site. Team meetings are opportune moments to remind all employees of the process to follow.

A.3 Bibliography

- AXA Insurance UK plc. Business Continuity Guide for Small Businesses
- DRJ Business Continuity Resource Centre for the Small/Medium Sized Business. The Small and Medium Size Businesses Guide to a Successful Continuity Programme
- US Small Business Administration. Expect the Unexpected – Prepare Your Business for Disaster
- Hester, Robert F. Business Continuity for Small Businesses. www.continuitycentral.com/feature0216.htm
- Wilson, Belinda. The Myths of Business Continuity and Disaster Recovery. www.continuitycentral.com/feature0139.htm

Appendix B: Example of Business Continuity Management Policy

B.1 Introduction

All entities of the River Bank must have detailed Business Continuity Plans in place to ensure that critical business processes can be continued in the event that a serious unplanned event occurs, which may disrupt the normal execution of those processes.

B.2 Scope

This Business Continuity Management (BCM) Policy covers the functions contained within the Bank's Head Office campuses in Perth and forms the basis for all Business Continuity Planning activities.

B.3 BCP Drivers

- Regulation
  - The FSA recommend that wholesale payments, trade clearing and settlement should be recovered to 60%-80% of normal values and volumes within 4 hours, rising to 80%-100% by the next working day
  - Data Protection Act
  - Health and Safety
- Customer Service
  - River Bank has been voted the "No. 1 Bank for Customer Service", for the third year running
- Current and emerging risks
  - The River Tay floods on average every 5 years and Riverside House was flooded 4 years ago
  - The rise in demand for mortgages has been a significant challenge both in terms of staffing, ICT and IS

B.4 BCP Objectives

In the event of a disaster, it is River Bank's aim to meet the following objectives:

- Maintain a healthy and safe working environment to ensure staff and customers' safety, welfare and confidence
- Fulfil regulatory requirements
- Maintain integrity of customer information
- Continue to operate critical business processes at a level of operation that meets regulatory requirements or for non-regulated critical process at a level of operation which is acceptable to management
- Provide timely availability of all key resources necessary to operate critical business processes
- Maintain customer/staff/River Bank stakeholders contact and confidence and to continue to be considered the "No. 1 Bank for Customer Service"

- Control of expenditure/lower extraordinary costs caused by event
- Management of risk – apply a Risk Management framework to priority areas

B.5 Stakeholders

The following groups of people can be defined as the stakeholders within River Bank:

- Staff
- Directors
- Customers
- Regulators
- Shareholders

B.6 Activities

The Business Continuity Management Policy covers the following activities:

Project Phase	Description
Define BCM Framework	***Coordination and Management of Business Continuity Planning Activities*** This is the ongoing process of ensuring that the Business Continuity measures are coordinated and controlled. There will be a regular review and agreement made to ensure that Business Continuity Planning measures implemented in the various River Bank locations are uniform, covering the interfaces and inter-dependencies between each location.
Business Impact Analysis	***Business Impact and Risk Analysis*** This is the process for managing overall River Bank risks through the Risk Management process and identifying which of these have a Business Continuity aspect, requiring preparation, active review and management attention. The impact of each risk will be assessed, their priority assigned and the requirements determined for each of the critical processes.
BCM Approach	***Business Continuity Strategy Development*** This is the process of identifying critical business functions and the personnel, IT and infrastructure required to support these functions in an incident. It also includes identifying suitable alternative locations, from which work can continue in a incident and the identification of 'workaround' procedures in the absence of IT functionality.
Deliver BCP	***Business Continuity Plan Development*** This is the process of documenting the Business Continuity Strategy in such a way that it is of practical use in an incident and that it fulfils business, regulatory, training and audit requirements. The plan should contain sufficient detail to allow the recovery and resumption of critical business processes and the supporting infrastructure and resources identified in the Business Continuity Planning Strategy.
Test BCP	***Business Continuity Plan Tests*** This is the verification process, to ensure that the BCP actually works and that the technology can be recovered to meet business requirements

Project Phase	Description
Sustain BCM	***Training of Staff and Maintenance and Review of BCP*** All staff with an involvement in BCM should be trained so that they are familiar with the BCP and are confident in their roles. The BCP must be continuously monitored to ensure that changes in the way business functions are undertaken and changes in the supporting infrastructure are reflected in the Business Continuity Strategy and Plan Improvements identified as a result of testing and training will also be made to the BCP. All changes must be assessed as part of change management.

B.7 BCM Operational Framework

The Business Continuity Steering Committee (BCSC) is responsible for defining and maintaining the framework for Business Continuity Management (including policy, strategy, overall implementation, plan documentation structure – including provision of business and support unit templates – tests and training concept, review and change management concept) and for initiating tests and reviews.

The Business Continuity Manager will be responsible for day to day management of the BCM programme and delivery and implementation of the BCP.

It is the responsibility of the business units to ensure that they have enough information in their specific section of the Business Continuity Plan to enable them to recover from an incident and continue to provide a service to clients within acceptable timeframes. Each Business Unit should nominate a member of staff to be their Business Continuity Co-ordinator.

It is the responsibility of the support units to ensure that they have enough information in their specific section of the Business Continuity Plan, to enable them to recover the infrastructure and services required to support business recovery activities within Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

An Incident Management Team will be established to manage Level 3 and 4 Incidents.

B.7.1 Review and Audit

The Bank's Internal Auditor shall consider coverage and review of this policy during the course of the annual audit programme or for any ad hoc investigations.

B.8 Invocation

Incidents are defined to be one of four levels of significance. The level of an incident is initially set by the Incident Management Team (IMT). However, the Senior Management Team has full discretion over the assigned level. Typically full invocation of the BCP only occurs given a level 3 or 4 incident and is based on the RTO.

The four levels of escalation for an incident are defined in the following table.

Level	Description	One or more of the following apply:
1	Minor incident (Normal Operating Procedures Apply)	• The incident is unlikely to affect critical business operations • The incident can be dealt with and closed at an operational level by the functional unit • Senior Management Team involvement not required
2	Minor disruption to critical business process (Normal Operating Procedures Apply)	• Critical business process interrupted (expected to be dealt with inside the critical process RTO) • Senior Management Team notified
3	Significant disruption	• Access is denied to the work environment, or key facility, key supporting technology component or data and is expected to go beyond 24 hours • Critical business process is interrupted (may go beyond the process MAO) • Senior Management Team involvement is mandatory
4	Major disruption	• Access is denied to the work environment, or key facility, key supporting technology component or data and is expected to go beyond the key resource MAO • Critical business process interrupted (expected to go beyond the process RTO) • Senior Management Team involvement is mandatory

B.9 Glossary

Definition of terms used in the Policy.

B.10 Bibliography

List of any reference material which has been referred to e.g. FSA, HM Treasury and the Bank of England Resilience Benchmarking Project.

Appendix C: Application Form for methods

C.1 Product Identity Card

1. General information

Method or tool name	Vendor / Publisher name	Country of origin

2. Level of reference of the product

National Standardisation body	International Standardisation body	Private sector organisation /association	Public / government organisation	White Paper/ Recommendation	Handbook	Guidelines

3. Identification

Define BCM Framework	Business Impact Analysis	Design BCM Approach	Deliver BCP	Test BCP	Sustain BCM Programme

If Define BCM Framework method:

BCM Framework activities	Included? (-, ●..●●●)	Comments
Initiate BCM Programme		
Assign BCM Responsibilities		
Define BCM Policy		
Assign Incident Teams		

If Business Impact Analysis method

Business Impact Analysis processes	Included? (-, ●..●●●)	Comments
Identify the organisation		
Assess Risks & Impacts		
Analyse Results		
Prioritise Recovery & define critical resource requirements		

If Design BCM Approach method

Design BCM Approach processes	Included? (-, ●..●●●)	Comments
Design Recovery Strategy		
Design Recovery Profile		
Design BCP		

If Deliver BCP method

Deliver BCP Method processes	Included? (-, ●..●●●)	Comments
Incident Response Plan		
Business Recovery Plan		
Incident Management Plan		
Business Resumption Plan		
Communications & Media Plan		
IT Service Continuity Plan		
Recovery Support Plans: • Facilities • HR • Health & Safety • Telephony		

If Test BCP method

Test BCP Method processes	Included? (-, ●..●●●)	Comments
Determine type of test		
Write test plan		
Conduct Test		
Deliver Debrief & Test Report		

If Sustain BCM Programme method

Sustain BCM Programme processes	Included? (-, ●..●●●)	Comments
Train Staff		
Maintain & Review BCP		
Develop Awareness		

Brief description of the product:

4. Lifecycle

Date of the first release	Date and identification of the last version

5. Useful links

Official web site	
User group web site	
Relevant web site	

6. Languages

Availability in European languages	

7. Price

Free	Not free	Updating fee

C.2 Scope

1. Target organisations

Government, agencies	Large companies	SME	Commercial companies	Non commercial companies
Specific sector				

2. Geographical spread

Used in EU member states	
Used in non-EU countries	

3. Level of detail

Management		Operational		Technical	

4. License and certification scheme

Recognised licensing scheme	
Existing certification scheme	

C.3 Users Viewpoint

1. Skills needed

To introduce	To use	To maintain

2. Consultancy support

Open market	Company specific

3. Regulatory compliance

4. Compliance to IT standards

5. Trial before purchase

CD or download available	Identification required	Trial period

6. Maturity level of the Information System

It is possible to measure the I.S.S. maturity level	

7. Tools supporting the method

Non commercial tools	Commercial tools

8. Technical integration of available tools

Tools can be integrated with other tools	

9. Organisation processes integration

Method provides interfaces to other organisational processes	

10. Flexible knowledge databases

Method allows use of sector adapted databases	

Appendix D: Application Form for Tools

D.1 Identity Card

1. General information

Tool name	Vendor name	Country of origin

2. Level of reference of the tool

World-wide (state oriented)	World-wide (sector oriented)	Regional (e.g. European directive)	Local
Supported by organisation, club,…(e.g. as sponsor)			

3. Brief description of the product

4. Supported functionality

BCM Framework activities	Supported or not	Comments
Initiate BCM Programme		
Assign BCM Responsibilities		
Define BCM Policy		
Assign Incident Teams		

If Business Impact Analysis Method

Business Impact Analysis processes	Supported or not	Comments
Identify the organisation		
Assess Risks & Impacts		
Analyse Results		
Prioritise Recovery & define critical resource requirements		

If Design BCM Approach Method

Design BCM Approach processes	Supported or not	Comments
Design Recovery Strategy		
Design Recovery Profile		
Design BCP		

If Deliver BCP Method

Deliver BCP Method	Supported or not	Comments

processes		
Incident Response Plan		
Business Recovery Plan		
Incident Management Plan		
Business Resumption Plan		
Communications & Media Plan		
IT Requirements & Gap Analysis		
IT Service Continuity Plan		
Recovery Support Plans: • Facilities • HR • Health & Safety • Telephony		

If Test BCP Method

Test BCP Method processes	Supported or not	Comments
Determine type of test		
Write test plan		
Conduct Test		
Deliver Debrief & Test Report		

If Sustain BCM Programme Method

Sustain BCM Programme processes	Supported or not	Comments
Train Staff		
Maintain & Review BCP		
Develop Awareness		

Other functionality:

Name	Description

Information processed

Name	Description

5. Lifecycle

Date of first release	Date and identification of the last version

6. Useful links

Official web site	
User group web site (optional)	
Relevant web site:	

7. Languages

Languages available									

8. Pricing and licensing models

Free	Not free		Maintenance fees	
Sectors with free availability or discounted price				

9. Trial before purchase

CD or download available	Identification required	Trial period(days)

10. Tool architecture

Technical component	Purpose	Comment
Database		
Web server		
Application Server		
Client		

D.2 Scope

1. Target organisations

Government, agencies	Large scale companies	SME	Commercial CIEs	Non commercial CIEs
Specific sector :				

2. Spread

General information	World-wide in many different organisations								
Used inside EU countries									
Used outside EU countries									

3. Level of detail

Level	Tool functions	Comment
Management		
Operational		
Technical		

4. Compliance to IT Standards

Standard	Compliance notice	Comment

5. Tool helps towards a certification

Certification according to standard	Comments

6. Training

Course	Duration	Skills	Expenses

D.3 Users Viewpoint

1. Skills needed (Global IT)

Skills	Comments
To install	
To use	
To maintain	

2. Tool support

Support method	Comment

3. Organisation processes integration

Role	Functions

4. Interoperability with other tools

Integration Method	Tools

5. Sector adapted knowledge databases supported

Database Name	Contents

6. Flexibility of tool's database

Database Name	Comments

D.4 Guidance for Business Continuity Planning tools

What should a Business Continuity Planning tool do?
A BCP solution should provide the capability to constantly update all aspects of the Business Continuity Plan of the enterprise and allow individual parts of the organisation to update and maintain their own part of the plan. From a plan governance perspective it should support monitoring of each BCP in accordance with predefined review frequencies, reporting on out-of-date and incomplete information.

Critical records
Vital records cover a spectrum of hardcopy documents and electronic files, many of which are subject to laws and legislation dictating how they must be processed, stored and protected.

A BCP solution should provide the capability to maintain a vital records inventory mapped to the processes and technologies create and maintain it.

Recovery and Continuity Plans
The ultimate purpose of any Business Continuity initiative is to create a viable plan to ensure availability of key services, together with a collection of procedures which clearly communicate the activities that should be performed in order to re-establish services to the required level. Historically this has involved generating paper or static documents.

With the increased reliance on both technology and inter-dependence inside and outside an organisation, BCPs need to be responsive to change and a BCP solution needs to support plan standardisation, maintenance and evidence of review.

Managing Recovery processes and components
Regardless of the methodology employed to create it, a BCP should consist of a number of key pieces of information:

- where to go
- systems to recover
- data to recover
- network and infrastructure to be restored
- restoration processes for systems and business activities
- people to carry it out

Any planning tool should provide the capability to capture this information as well as a framework to monitor it going forward, in order to provide reasonable assurance that the plan reflects the organisation's risk profile and that, if invoked, the plan is likely to work.

Testing
Creating plans that are subsequently forgotten is not sufficient, they must be tested regularly to confirm their effectiveness and to identify and correct problems before an actual interruption occurs. A BCP solution should provide an organisation with the capability to schedule tests, record the results and monitor remediation efforts.

Regulators and auditors need more than verbal assurance that tests have been conducted. They require proof that tests have been conducted, that test results have been evaluated, and that remedial action if required is under way and its progress monitored.

Governance
With so much attention directed towards a firm's Risk Management controls and internal governance program, a key attribute for any BCP solution is to provide the necessary capabilities to facilitate the standard and processes that collectively comprise a 'Business Continuity Management (BCM) Framework'. This implies that all of the required features of a robust BCP framework such as risk and impact analysis, planning, plan review and plan testing are supported by the tool. Just as important, however, are features that ensure these processes are being performed and, when they are not, that the appropriate individuals are notified. These features provide transparency, auditability of the BCP together with the assurance that the organisation is in a reasonable state of readiness.

What makes a Business Continuity tool effective?
An overriding requirement of a BCP solution is that it provides an enterprise-wide framework managing a wide array of structured and unstructured information, collectively forming the organisation's BCP. The Supplier Directory section provides detailed responses from suppliers in terms of the capabilities of their solutions. Notwithstanding these features, our experience has shown that there are five key attributes that should be present in any solution for it to be an effective tool:

Pervasive – the production of plans is subsumed within an enterprise-wide process that enforces the plan governance process

Consistent – all information related to the plan is produced and managed in the same way

Persistent – exceptions, out-of-date plans, incomplete plans are identified and clearance is monitored and reported

Unavoidable – documents and records related to the plan can only be produced via the prescribed methods and are subject to pre-defined approval cycles

Transparent – the status of any document or record and the overall governance process is visible to all members of the enterprise who have an interest or responsibility for it. The collective status of documents or records can be assessed - providing a barometer of the firm's state of readiness.

In order to deliver these key attributes, any solution must leverage a number of key technologies within its design. The basic requirements are search, workflow, version management, categorisation and mail enablement.

Search
Search tools help to gather all types of information relating to a particular subject. They help users to locate what they need on an ad hoc basis without having to rely on pre-defined queries.

Workflow
Workflow is generally the means by which approval and review cycles are enforced upon different types of information. By using workflow techniques, firms can ensure that changes to plans are properly authorised and are 'fit for purpose'.

Version Management
Versioning provides an all important audit trail from the current form of a document to its original state. Keeping prior versions of plans provides not only an audit trail of changes but can assist in the review of changes.

Categorisation

Categorisation is the means by which unstructured information becomes usable in a structured way. There are basically two ways to achieve categorisation:

- create a relational database model and migrate existing information from various sources into the database

- create a managed document repository whereby all documents pertaining to the plan are created and maintained in the repository. Meta Data is then created to provide multiple levels of categorisation for documents which can subsequently be 'navigated', rather like a website.

Categorisation of unstructured content provides the basis for ensuring the content is appropriately managed against various regulations and legal requirements throughout its life. For many organisations which have invested in comprehensive, document-based plans, categorisation capabilities provide the means by which documents can be collected and 'viewed' along differing lines, i.e. organisationally or by business process, without undergoing complex data conversion exercises.

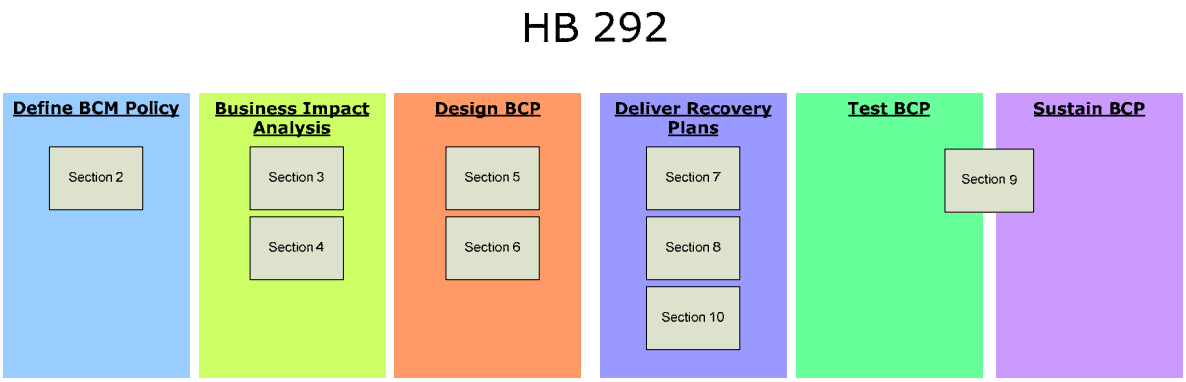
Mail enablement

By linking to individuals with specific plan responsibilities via their e-mail address, an application becomes truly enterprise-enabled. Individuals can be alerted and reminded to address issues arising from their plans, with each e-mail containing a URL link to the records or documents they are responsible for. Although e-mail is an application often taken for granted, tools which leverage corporate e-mail systems can lower solution deployment costs and provide a pervasive 'nervous system' capable of addressing the whole firm, regardless of physical location.

Appendix E: Process Maps of Methods and Good Practices from around the World

E.1 HB 292

E.1.1 Process Map



E.1.2 Description

Section 2 – Commencement of Business Continuity Management
The commencement step establishes the infrastructure and much of the capability required for each of the other steps of the process. Commencement is concerned with creating awareness and understanding of BCM and the skills required, gaining the commitment and support of management and staff and establishing the organisational infrastructure programme management required for successful implementation. The sections below discuss the following themes in more detail:

- Awareness and Understanding
- Gaining Management Commitment
- The Need for Communication and Engagement
- Gaining the Commitment of Others
- Establishing the Infrastructure for BCM
- Development of the BC Policy
- Confirmation of Processes
- Resource Allocation
- BCM Programme Governance

Section 3 – Assessing Risks and Developing Disruption Scenarios
Risk Assessment is a critical step in the BCM process. It provides a means of identifying and prioritising the type of events that could cause disruption to the organisation and give a broad indication of the consequences of such events and their likelihood. This provides the key inputs upon which subsequent Business Impact Analysis can be developed. If the Risk Assessment process is approached from a broader risk perspective than just BCM, it can generate additional business value.

If the BCM practitioner liaises with the risk managers much effort may be saved since a considerable amount of the Risk Assessment may already have been undertaken by others.

The topics covered in this section include:

- What is Risk?
- Using Risk Assessment in BCM
- Communicate and Consult
- Establishing the Context

- Identifying Risk
- Analysing Risk
- Evaluating Risk
- Treating Risk

Section 4 – Conducting the Business Impact Analysis
The BIA provides an analysis of how key disruption risks could affect an organisation's operations and what capabilities will be required to manage them. The BIA comprises eight steps:

- Developing communications for the BIA
- Confirming critical business functions
- Identifying resource requirements
- Establishing interdependencies
- Determining the disruption impacts
- Identifying the Maximum Tolerable Outage Times and Recovery Objectives
- Identifying alternate workarounds and processes
- Confirming current preparedness

Section 5 – Developing BCM Strategies
The development of BCM strategies is concerned with determining how an organisation will react to an incident and the manner in which the different elements of this overall response will interact. Typically there are three phases to an event and each phase will have a degree of overlap with the next. HB 292 defines the three phases as:

- The emergency response phase
- The continuity phase
- The recovery and restoration phase

A strategy is required for each of these phases which focuses on:

- Meeting regulatory, industry and organisational requirements
- Providing adequate cost benefit returns
- Matching strategic objectives with the practical realities of access to capabilities and resources

Section 6 – Assessing and Collating Resource Requirements
Once the strategies have been developed, resource requirements need to be confirmed as appropriate to achieving these strategies. This step involves collating the information from across all the functions which were analysed during the previous phase. It is important to ensure that the synergies and conflicts in resource availability, access and use are identified and managed.

Section 7 – Writing the Plan
One of the most important issues in writing a plan for managing a disruption is to ensure that it is written so that it can be understood and applied by those expected to use it. A plan should be written in such a way that it can be understood by someone who has not previously seen it. This section describes:

- The framework of plans
- Content of plans – generic
- Content of plans – specific
- Continuity plan checklist

Section 8 – Developing the Communications Strategy

It is vital that communications are considered to be one of the highest priorities throughout all BCM activities, both pre and post-event. The three broad areas for which development of a communication strategy are internal and external stakeholders, incident related communications, ongoing maintenance of developed plans. This section is divided into the following sub-sections:

- Communicating during and after an incident
- Developing the written communications plan
- Identifying stakeholders and their needs
- Using IRACI
- Communications strategy checklist

Section 9 – Maintenance of BCM
Plans can get out of date very rapidly, and even after a few weeks the effectiveness and relevance of plans begins to deteriorate. Also, in order for plans to be effective the relevant people need to know how to use them for them. A regular maintenance programme is therefore needed if plans are to remain fit for purpose. This section describes the following activities to ensure that a robust maintenance programme is established:

- Understanding – training and awareness
- Performance
- Assurance

Section 10 – Activation and Deployment
Following a disruptive event there will be a number of plans activated which will require overall central control and co-ordination. This section of the handbook describes:

- The co-ordination and control framework
- Building disaster kits
- Record keeping
- Activation and deployment checklist

E.1.3 Detail

Section 2 – Commencement of Business Continuity Management

Responsible:
Accountable:
Consulted:
Inputs:
Output: BCM Policy; critical business objectives; disruption potential; communication framework; management commitment; resource plan; BCM programme governance

Section 3 - Assessing Risks and Developing Disruption Scenarios

Responsible: BCM Practitioner
Accountable:
Consulted: Risk Managers
Inputs: Organisational Risk Assessments
Output: BCM Risk Assessment; Risk Treatment Strategy

Section 4 – Conducting the Business Impact Analysis

Responsible: BCM Manager
Accountable:
Consulted: BC Planner; Business Function Owners
Inputs: Risk Assessment

Output: Business Impact Assessment; critical organisational objectives and performance levels; key personnel; normal operational resource requirements and minimum resource requirements; interdependencies; areas requiring workarounds; contact details for key stakeholders

Section 5 – Develop BCM Strategies

Responsible:
Accountable:
Consulted:
Inputs: Business Impact Assessment
Output: Emergency Response Strategy; Continuity Strategy; Recovery and Restoration Strategy

Section 6 – Assessing and Collating Resources Requirements

Responsible:
Accountable:
Consulted:
Inputs: Business Impact Assessment
Output: Resource Matrix

Section 7 – Writing the Plan

Responsible:
Accountable:
Consulted:
Inputs: Regulatory requirements; industry standards; critical objectives; critical functions; Resource Matrix
Output: Tier 1 Plans; Tier 2 Plans; Tier 3 Plans

Section 8 – Develop the Communications Strategy

Responsible:
Accountable:
Consulted:
Inputs: IRACI Tool; Identified Stakeholders; emergency strategies; continuity and restoration strategies
Output: Communications Plans

Section 9 – Maintenance of BCM

Responsible:
Accountable:
Consulted: Staff and internal and external individuals involved in all phases of BCM
Inputs: Completed plans
Output: Schedule of internal and external reviews, exercises and training

Section 10 – Activation and Deployment

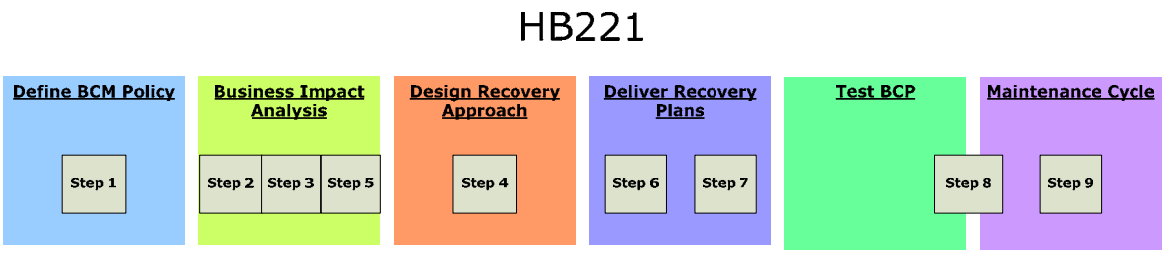
Responsible: Management
Accountable: Incident Controller
Consulted:
Inputs: Emergency Response Plans; BC Plans; Recovery and Restoration Plans
Output: Incident Control System; disaster kits; Incident Log

E.1.4 Links

The Bibliography references a number of other BC publications.

E.2 HB 221

E.2.1 Process Map



E.2.2 Description

Step 1 – Commencement
The scope, objectives and outcomes for the Business Continuity program or planning project are determined.

Step 2 – Risk and Vulnerability Analysis
A comprehensive understanding of the external and internal business drivers and constraints is obtained. Risks requiring mitigation through Business Continuity Planning are identified and prioritised.

Step 3 – Conduct a Business Impact Analysis
The potential operational and financial impacts of a disruption over time are determined. Critical business functions and processes that support achievement of key business objectives are identified. The resource requirements of critical business functions and processes that will allow a minimum acceptable level of operation are defined.

Step 4 – Define Response Strategies
Emergency Response: The criteria for activation, duration and stand-down of the immediate (emergency) response are defined.

NOTE: The principle purpose of the emergency response is the preservation of life and property.

Continuity Response: The criteria for activation, duration and stand-down of the continuity response are defined.

NOTE: The principle purpose of the continuity response is the continued delivery of a minimum acceptable level of performance.

Recovery Response: The criteria for activation, duration and stand-down of the recovery response are defined.

NOTE: The principle purpose of the recovery response is the staged return to a level of normal (pre-disruption) or improved capability and performance.

Step 5 – Developing Resource and Interdependency Requirements
Resource requirements are finalised and the approach to meet requirements is determined. The range and nature of external interdependencies are defined.

Step 6 – Develop Continuity Plans for the Chosen Strategy
Specialist and Organisation Plans: Plans are developed to cover specialist and organisation requirements for continuity and recovery.

Continuity Plans: Continuity plans are developed and documented in a comprehensive and simple manner which allows the organisation to respond flexibly to a wide variety of potential disruption scenarios.

An organisation may determine that each business unit has specialised BCM plans that will be enacted and that the organisation will have an overarching BCM plan to manage the activities of each business unit and to coordinate assets required for restoration and recovery activities.

Step 7 – Develop a Communication Strategy
The purposes of different types of messages are defined in advance of any disruption.

Step 8 – Training, Maintenance and Testing Plans
Training: In the event of a disruption, plans can be implemented efficiently and effectively.
Those with tasks that are part of the plans are fully aware of their responsibilities.
Employee and management awareness of emergency procedures and the significance of Business Continuity is enhanced.
Confidence in the ability to manage a disruption is improved.
Through a robust regime of plan testing, effective awareness and training can be delivered.

Maintenance: Plans are revised on a regular basis to ensure that content reflects current risks, priorities, functions, personnel responsibilities and resource requirements.

Plan Testing: Plan inadequacies are identified and corrected.
The feasibility of plan components is assessed and confirmed.
Resourced requirements are clarified.
Confidence in the ability to manage a disruption is improved.
Auditors and insurers can be provided with documented proof of plan adequacy.

Step 9 – Activation and Development of Plans
Plans are activated according to the nature of the disruption and in an appropriate authorised manner. Post activation governance requirements are identified as part of the response plan and are managed during after the response is activated and stood down.

E.2.3 Detail

Step 1 - Commencement

Responsible:	Senior Management/Board – for scope, budget and resources
Accountable:	Project Manager – for policy and strategy
Consulted:	Senior Management/Board
Inputs:	Budgets, risks, costs
Output:	Scope, objectives and outcomes

Step 2 – Risk and Vulnerability Analysis

Responsible:	
Accountable:	
Consulted:	Management
Inputs:	Annual Reports, Corporate and business unit plans, management and board minutes, internal audit reviews, existing BC Plans, media reports
Output:	Environmental Analysis, management interviews, internal audit reviews, analysis of key infrastructure and processes

Step 3 – Conduct a Business Impact Analysis

Responsible:
Accountable:
Consulted: Management and teams
Inputs: Critical business objectives and success factors (from Steps 1 and 2), key risk exposures (from Step 2)
Output: High level process map, minimum resource requirements; Maximum Acceptable Outage time (MAO); backlog impacts; alternative workarounds

Step 4 – Define Response Strategies

Responsible:
Accountable:
Consulted:
Inputs: Existing Emergency Response plans, Emergency Command and co-ordination plans, etc…
Output: Creation of Crisis Management Team (CMT). Criteria for activation, scale back and deactivation of an integrated suite of plans:

- Emergency Response
- Continuity Response
- Recovery Response

Step 5 – Developing Resource and Interdependency Requirements

Responsible:
Accountable:
Consulted:
Inputs: Minimum resourcing requirements (from Step 3); vital records, staff contact lists, operating and procedure manuals, IT technical recovery plan and procedures, alternative office locations, emergency expense payment authority/delegation, IT infrastructure, telecommunications support, office and specialist equipment locations, external interdependency contact details, stakeholder expectations, alternative relationships and sources for contract requirements
Output: Confirm requirements from Step 3

Step 6 - Develop Continuity Plans for the Chosen Strategy

Responsible:
Accountable:
Consulted: Business units
Inputs: Response strategy; interdependency requirements
Output: Determine requirements for specialist plans; documented continuity plans

Step 7 - Develop a Communication Strategy

Responsible:
Accountable:
Consulted: Stakeholders, Board, Regulators
Inputs: Regulatory requirements; communication channels; content pro forma
Output: Who requires what information, how it is delivered and by whom

Step 8 – Training, Maintenance and Testing Plans

Responsible:
Accountable:
Consulted:
Inputs: BIAs; tests; changes in personnel, risks, priorities and functions
Output: Documented results of tests for plan improvements; basic awareness for all staff; basic training for staff with roles/responsibilities; regular maintenance cycle and audits for the BCM process, plans, testing, training and BIAs

Step 9 – Activation and Development of Plans

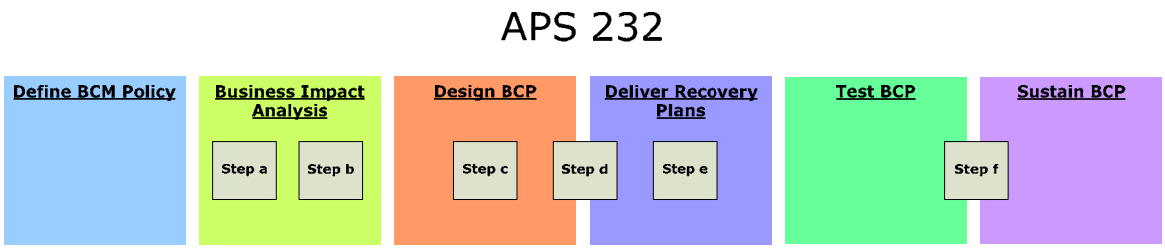
Responsible:
Accountable:
Consulted: Insurance agents, regulators, etc…
Inputs: Regulations, standards, policies and procedures, document control
Output: Updates to current plans

E.2.4 Links

This standard contains no links to other standards.

E.3 Australian Prudential Standard APS 232

E.3.1 Process Map



E.3.2 Description

Business Continuity is a requirement for Australian financial institutions, as decided by the Australian Prudential Regulatory Authority that released this standard.

As the document is 8 pages in length, it does not go into depth on any part of the process.

E.3.3 Detail

Step a – Risk Assessment

Responsible: Board of Directors
Accountable:
Consulted:
Inputs:
Output: Plausible disruption scenarios and likelihood of them occurring

Step b – Business Impact Analysis

Responsible: Senior Management
Accountable:
Consulted:
Inputs: Legal and regulatory requirements; revenue by product; RTO
Output: Identification of all critical business functions, resources and infrastructure; impact of disruption; priorities for recovery (validated by Senior Management)

Step c – Consideration of Recovery Strategies

Responsible: Senior Management
Accountable:
Consulted:
Inputs: BIA data
Output: Approved resources for implementation

Step d – Business Continuity Planning

Responsible: Board of Directors
Accountable:
Consulted:
Inputs:
Output: Includes:
Documented procedures for recovery of critical business functions

Resumption plans
Resources required
Communication plan

Step e – Establishing Business Continuity/Crisis Management Teams

Responsible:
Accountable:
Consulted:
Inputs:
Output: Composition of Teams; invocation procedures

Step f – Review and Testing

Responsible:
Accountable:
Consulted:
Inputs:
Output: Annual review (minimum if there is no change management process in place); testing program; test results

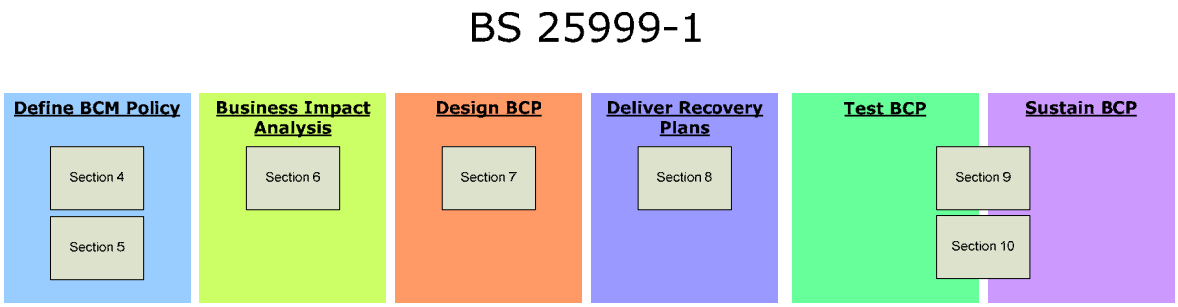
E.3.4 Links

Risk Assessments and testing are conducted in accordance with:

- AGN 232.1 Risk Assessment and Business Continuity Management
- APS 310 Auditing and Related Arrangements for Prudential Reporting

E.4 BS 25999-1

E.4.1 Process Map



E.4.2 Description

British Standard 25999-1 establishes the process, principles and terminology of Business Continuity Management (BCM) and provides a basis for understanding, developing and implementing Business continuity within an organisation.

It is intended for use by anyone with responsibility for business operations or the provision of services, from top management through all levels of the organisation.

The seven steps in the Business Continuity lifecycle as defined in BS 25999-1 are as follows:

Step1: The Business Continuity Management Policy (Section 4)
It is important to develop a Business Continuity Policy to ensure:

- All BCM activities are performed in an agreed manner
- BCM capability meets changing business needs
- A framework for ongoing BCM is established

This is achieved by taking the following measures:

- Put the BCM programme into context
- Develop the policy
- Determine the scope of the BCM programme
- Review audited evidence of outsourced supplier Business Continuity Plans

Step 2: BCM Programme Management (Section 5)
Programme management is at the heart of the BCM process and this section describes what should be put in place to establish and manage BCM in the organisation

- Assign responsibilities
- Implement BCM in the organisation
- Manage the programme on an ongoing basis

Step 3: Understanding the Organisation (Section 6)
The BCM programme must be aligned to the organisation's objectives, obligations and statutory duties and this is achieved by understanding the critical activities and resources which support them. The steps to reach this understanding are:

- Conduct Business Impact Analysis
- Identify Critical Activities
- Determine continuity requirements

- Evaluate threats to critical activities
- Determine choices (i.e. accept, transfer, change, suspend or terminate the risk or develop a Business Continuity Plan to improve the organisation's resilience to a disruption)

Step 4: Determining Business Continuity Strategy (Section 7)
As a result of the analysis in the previous stage of the BCM programme, the organisation can choose the appropriate continuity strategies to enable it to meet its objectives. Strategies should be considered for:

- People
- Premises
- Technology
- Information
- Supplies
- Stakeholders

Development of these strategies should include familiarisation with local emergency responder bodies, so that the organisation's recovery activities take into account the civil emergency capacity of their community.

Step 5: Developing and Implementing a BCM Response (Section 8)
In this section of the standard, BS 25999-1 describes the areas to be covered in the BCM response document(s):

- Incident response structure
- Roles and responsibilities
- Plan invocation
- Document Owner and maintainer
- Task and action lists
- Emergency contacts
- People activities
- Media response
- Stakeholder management
- Incident management location
- Resource requirements

Step 6: Exercising, Maintaining and Reviewing BCM Arrangements (Section 9)
This stage of the lifecycle ensures that all the plans which have been written and arrangements which are in place are kept fit for purpose and up-to-date.

- Exercising
  - Desk check
  - Walkthrough
  - Simulation
  - Alternate Site
  - Full BCP
- Maintaining BCM Arrangements
- Reviewing BCM Arrangements

Step 7: Embedding BCM in the Organisation's Culture (Section 10)
Raising and maintaining awareness of BCM on the part of the organisation's staff is important to ensure that they are aware of BCM's importance to the organisation. This is achieved through awareness-raising activities such as articles in the organisation's newsletter, or on the intranet, inclusion of BCM in induction training and visits to designated alternate sites.

Skills training is essential for any staff member with a BCM or incident role, and different training sessions should be identified for different skill areas.

E.4.3 Detail

Section 4 – The Business Continuity Management Policy

Responsible: Top Management
Accountable: Board Director or Elected Representative
Consulted:
Inputs: Relevant standards; regulations or policies; identification of key activities
Output: BCM Policy

Section 5 – BCM Programme Management

Responsible: Top Management
Accountable: Board Director or elected representative
Consulted: Management
Inputs: BCM Policy
Output: Establishment of BCM Programme

Section 6 – Understanding the Organisation

Responsible:
Accountable: Top Management
Consulted:
Inputs: Risk Registers
Output: Critical Activities; Impacts of Loss; Recovery Time Objectives; Risk Assessment

Section 7 – Determining Business Continuity Strategy

Responsible:
Accountable: Top Management
Consulted:
Inputs: Maximum Tolerable Period of Disruption; BCM Risk Register; Critical Activities; Impacts of Loss
Output: Strategies (people, premises, technology, information, supplies, stakeholders)

Section 8 - Developing and Implementing a BCM Response

Responsible: Nominated person
Accountable: Board Sponsor
Consulted: Top Management
Inputs: BCM Strategies
Output: Incident Management Plan; Business Continuity Plan

Section 9 - Exercising, Maintaining and Reviewing BCM Arrangements

Responsible: Top Management
Accountable:
Consulted:
Inputs:
Output: Exercise programme; post exercise report; BCM Maintenance programme; reviewed BCM arrangements; documented review results

Section 10 - Embedding BCM in the Organisation's Culture

Responsible:

Accountable:
Consulted:
Inputs:
Output: Identified and delivered BCM awareness requirements; training programme for incident and BCM personnel

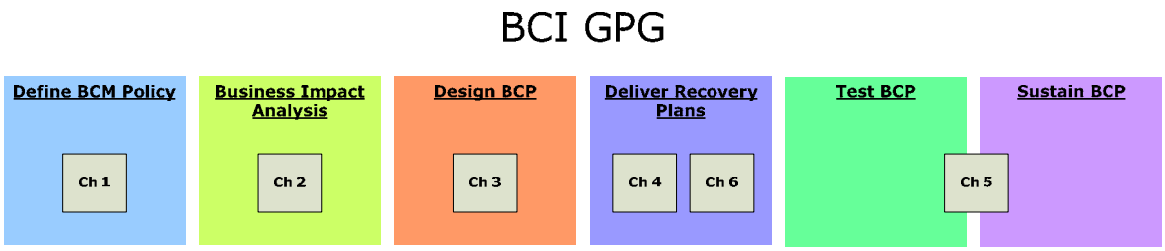
E.4.4 Links

BS 25999-1 references the following publications:

- BS EN ISO 9000, quality Management Systems – Fundamentals and Vocabulary
- BS ISO/IEC 20000 (both parts), Information Technology – Service Management
- BS ISO/IEC 27001, Information Technology – Security Techniques – Information Security Management Systems – Requirements
- Civil Contingencies Act 2004, London, TSO

E.5 BCI Good Practice Guidelines

E.5.1 Process Map



E.5.2 Description

The Good Practice Guidelines define the BCM process, requirements, outcomes and methods. This will provide a step-by-step guide to an organisation for undertaking a Business Continuity Programme but does not detail the roles and responsibilities.

Methodologies for BIAs and Risk Assessments are detailed.

E.5.3 Detail

Chapter 1 – BCM Programme Management

Responsible:
Accountable:
Consulted: External BCM practitioners (to review current situation/gap analysis
Inputs: Statutory and Regulatory responsibilities; Good Practice Guidelines; Gap analysis; identification of clearly defined roles; responsibilities and authorities to manage the BCM programme; budget
Output: BCM Policy (Scope and Governance); a scope and terms of reference document for the Business Impact Analysis and Risk Assessment; organisational definition of BC; implementation and maintenance plan for the Policy; roles, responsibilities and job specifications; project plan with clear deliverables, work estimates and budgetary requirements

Chapter 2 – Understanding the Organisation

Responsible:
Accountable:
Consulted:
Inputs: BCM Policy
Output: MTPD and justification thereof; RTO; Resource Requirements Analysis (RRA); Risk Analysis

Chapter 3 – Determining BCM Strategy

Responsible:
Accountable:
Consulted:
Inputs: BCM Policy; RTOs and RRA
Output: Formation of a Business Continuity Management Strategy Team; an agreed BCM strategy for each of the organisation's products and services; BC options for each

strategy; consolidated view of Resource requirements

Chapter 4 – Developing and Implementing BCM Response

Responsible:
Accountable:
Consulted:
Inputs:
Output: Incident Management Plan; Incident Communications Plan; a Business Continuity Plan which should be 'signed-off' by the Executive; a documented Operational Response Plan for each business activity or department; escalation procedure to Business Continuity Team; clearly defined BCM roles within the department

Chapter 5 – Exercising, Maintaining and Reviewing Plans

Responsible:
Accountable:
Consulted: Training timetable
Inputs: BCM Policy (outlines timetable and responsibilities for the exercise programme and audit requirements); change management
Output: Timetable for an exercise programme; exercises (testing staff, plans and the recovery infrastructure); post-exercise reports; a documented BC monitoring and maintenance programme; a clearly defined and documented BCM Maintenance Report Action Plan agreed and 'signed off' by an appropriate senior manager; an independent BCM audit opinion report that is agreed and 'signed-off' by senior Management; Remedial Action Plan

Chapter 6 – Embedding BCM in the Organisation's Culture

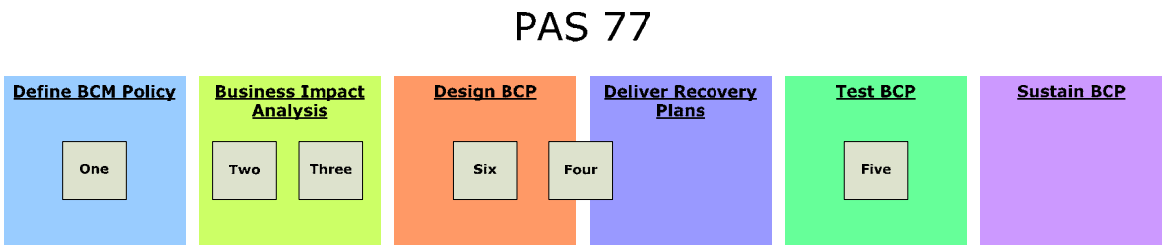
Responsible:
Accountable:
Consulted:
Inputs: The BCM Policy provides the framework for supporting the need and requirement for cultural change
Output: A statement of the current level of awareness and effectiveness of staff to support BCM; Training Needs Analysis

E.5.4 Links

There are no formal links but BS 25999, ISO 17799 and the FSA are referred to throughout. ISO 27001 is mentioned under the heading of BCM Awareness.

E.6 PAS 77

E.6.1 Process Map



E.6.2 Description

The ITSC strategy should enable the organisation to plan for and rehearse the whole life-cycle of a major incident from the point of initial disruption, through the recovery, to abnormal service and finally to the point where normal service levels are once again guaranteed. This is agreed at the Board level and the CEO is responsible.

The ITSC strategy should be a by-product of a Business Continuity Management Plan (BCMP) but can be defined without such a plan. Where a BCMP exists, those responsible for IT service levels are likely to have contributed to the plan and already be aware of the implications of that plan on the IT strategy and direction.

It must be noted that this is a developing standard and is subject to change as it develops and is accepted as BS 25777.

E.6.3 Detail

IT Service Continuity Strategy

Responsible: CEO
Accountable: Board member
Consulted: Board level
Inputs:

- priority for key business units at given moments in time
- peak loads on business
- strategically important business periods e.g. reporting
- periods, manufacturing deadlines etc
- compliance with Business Continuity Management
- Plans and objectives
- investment vs. risk
- impact of failure or loss
- recovery time objectives
- acceptable levels of downtime and performance
- system changes and upgrades
- new projects
- interdependencies
- compliance with legislation
- deadline management
- rehearsing and rehearsing recovery plans
- data protection
- data availability
- plan maintenance
- education and awareness programmes for all IT staff

Output: High-level methods

Understanding Risks and Impacts within Your Organisation

Responsible:
Accountable: Board member
Consulted:
Inputs: System resilience and availability; key suppliers and agreements; documentation; hardware and software assets; storage; back-up regimes; staff exposure; staff training; location of buildings and facilities; IT security; systems monitoring; power; data communications; archiving; IT environment and monitoring; telephony; any other relevant exposure
Output: Vulnerability Assessment; RTOs for critical activities

Conducting Business Criticality and Risk Assessments

Responsible:
Accountable: Board member
Consulted:
Inputs: Physical and organisational risks
Output: Risk Assessments

IT Service Continuity Plan

Responsible:
Accountable: Board member
Consulted:
Inputs: RTO; RPO; cost of RTO/RPO
Output: Incident Management Teams; detailed recovery procedures for all IT System Components; Roles and Responsibilities; failback procedures

Rehearsing an IT Service Continuity Plan

Responsible: Service Continuity Manager
Accountable: Board member
Consulted: Business Continuity Coordinator; Business Continuity Steering Group; Compliance/Audit Team; Business Continuity Rehearsal Group.
Inputs: Staff resources; costs; implications; knowledge of the rehearsal subject; testing strategy (method)
Output: Rehearsal result; updated continuity plans

Solutions Architecture and Design Considerations

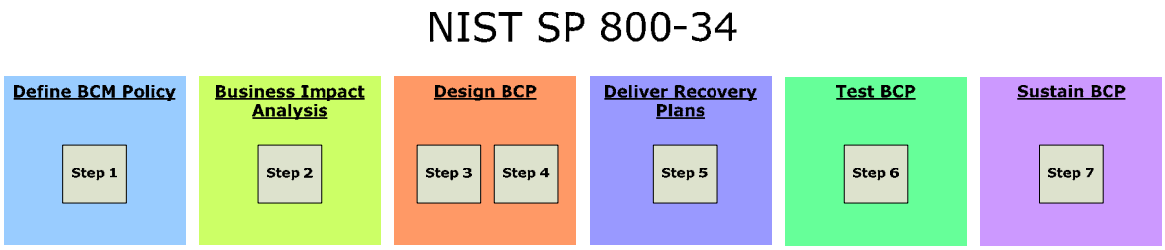
Responsible:
Accountable: Board member
Consulted:
Inputs: Critical systems; critical applications; network; data and backups
Output: Resilient architecture

E.6.4 Links

- ITIL (For guidance on Service Level Agreements)
- BS ISO/IEC 17799:2005 (For guidance on creating Risk Assessments relating to information security)
- Prince 2 (Project Management)
- Project Management Institute – 'Project Management Body of Knowledge'

E.7 NIST SP 800-34

E.7.1 Process Map



E.7.2 Description

The processes to develop and maintain an effective IT contingency plan are common to all IT systems. The seven steps in the process are as follows:

Step 1 - Develop the Contingency Planning Policy Statement
Identify statutory or regulatory requirements for contingency plans
Develop IT contingency planning policy statement
Obtain approval of policy
Publish policy

Step 2 - Conduct the Business Impact Analysis (BIA)
Identify critical IT resources
Identify outage impacts and allowable outage times
Develop recovery priorities

Step 3 - Identify Preventive Controls
Implement controls
Maintain controls

Step 4 - Develop Recovery Strategies
Identify methods
Integrate information system architecture

Step 5 - Develop an IT Contingency Plan
Document recovery strategy

Step 6 - Plan Testing, Training and Exercises
Develop test objectives
Develop success criteria
Document lessons learned
Incorporate into the plan
Train personnel

Step 7 - Plan Maintenance
Review and update plan
Coordinate with internal/external organisations
Control distribution
Document changes

E.7.3 Detail

Step 1 - Develop the Contingency Planning Policy Statement

Responsible: Senior Management
Accountable: CIO
Consulted:
Inputs: System security plans, facility-level plans (OEP and COOP); agency-level plans (business resumption and CIP)
Output: Contingency planning policy statement

Step 2 - Conduct the Business Impact Analysis (BIA)

Responsible:
Accountable:
Consulted: Contingency Planning Coordinator
Inputs:
Output: Identification of Critical IT resources; Identification of Impacts and allowable Outage times; Recovery Priorities; BIAs

Step 3 - Identify Preventive Controls

Responsible:
Accountable:
Consulted:
Inputs:
Output: Outage preventative measures

Step 4 - Develop Recovery Strategies

Responsible:
Accountable:
Consulted:
Inputs: Options (recovery sites, SLAs, technology, backup strategies, etc)
Output: Recovery strategy; an MOU, memorandum of agreement (MOA), or an SLA for an alternate site (if applicable); agreements for equipment replacement; roles and responsibilities of the various teams

Step 5 - Develop an IT Contingency Plan

Responsible:
Accountable:
Consulted:
Inputs: BIAs, recovery strategy
Output: IT Contingency Plan

Step 6 - Plan Testing, Training and Exercises

Responsible:
Accountable:
Consulted:
Inputs:
Output: Test plan of dates and test types

Step 7 - Plan Maintenance

Responsible: Contingency Planning Coordinator
Accountable:
Consulted:
Inputs: Changing business requirements; technology updates, information updates; BIAs; contracts; options; hardware and software requirements; MOUs or SLAs; security requirements; contingency policies; training materials;

	testing scope
Output:	Updated plans

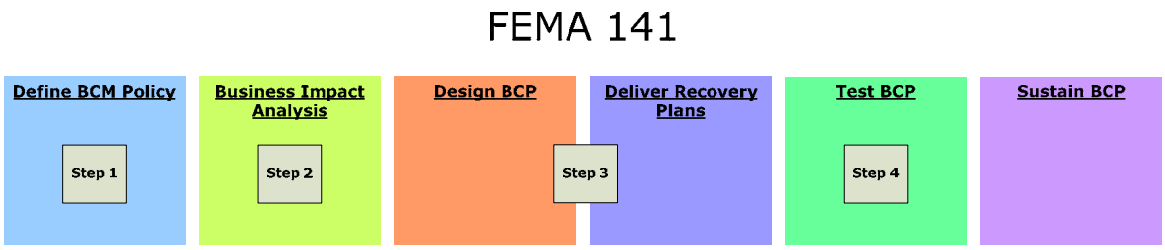
E.7.4 Links

Reference is made to the following:

- **Continuity of Support Plan** required by Office of Management and Budget (OMB) Circular A-130, Appendix III
- **COOP** is required by Presidential Decision Directive 67 (PDD-67)

E.8 FEMA 141

E.8.1 Process Map



E.8.2 Description

The document is aimed at Emergency Planners. The specific scenarios are:

- Fire, hazardous materials
- Floods
- Hurricanes
- Tornadoes
- Severe winter storms
- Earthquakes
- Technical emergencies

Obviously the document centres around analysis of risk, creating plans and the various aspects of responding to a large scale emergency such as:

- Incident control
- Emergency Operations Centre
- Communications
- Life and limb
- Property
- Restoration
- Logistics

Testing is treated as part of staff training! Plans are subject to a tabletop test exercise before final release. More tabletop exercises are part of the training as well as Walk-through Drills, Functional Drills, Evacuation Drills and Full-scale Exercises.

An annual audit asks the question: "does the plan reflect the reality of the situation or has that changed?" There is no formal maintenance cycle, re-evaluation of Capabilities and Hazards of change control for plans.

E.8.3 Detail

Step 1 - Establish a Planning Team

Responsible: Chief Executive
Accountable:
Consulted: Management
Inputs:
Output: Establish authority; mission statement; budget and schedule

Step 2 – Analyse Capabilities and Hazards

Responsible:
Accountable:
Consulted: External agencies
Inputs: Existing plans and policies; regulatory requirements; resource requirements for company products/services; suppliers; single points of failure in the supply chain; facilities and backup systems; risks; potential hazards; impact; recovery costs
Output: Risk Assessment; Business Impact Analysis

Step 3 – Develop the Plan

Responsible:
Accountable:
Consulted: Government (local and state) agencies
Inputs: Contact lists; maps; risk and hazardous material data sheets; 3rd party contracts
Output: Executive summary; roles and responsibilities; emergency response procedures; supporting documents; emergency call lists; training schedule; (tabletop-tested) plans.

Step 4 – Implement the Plan

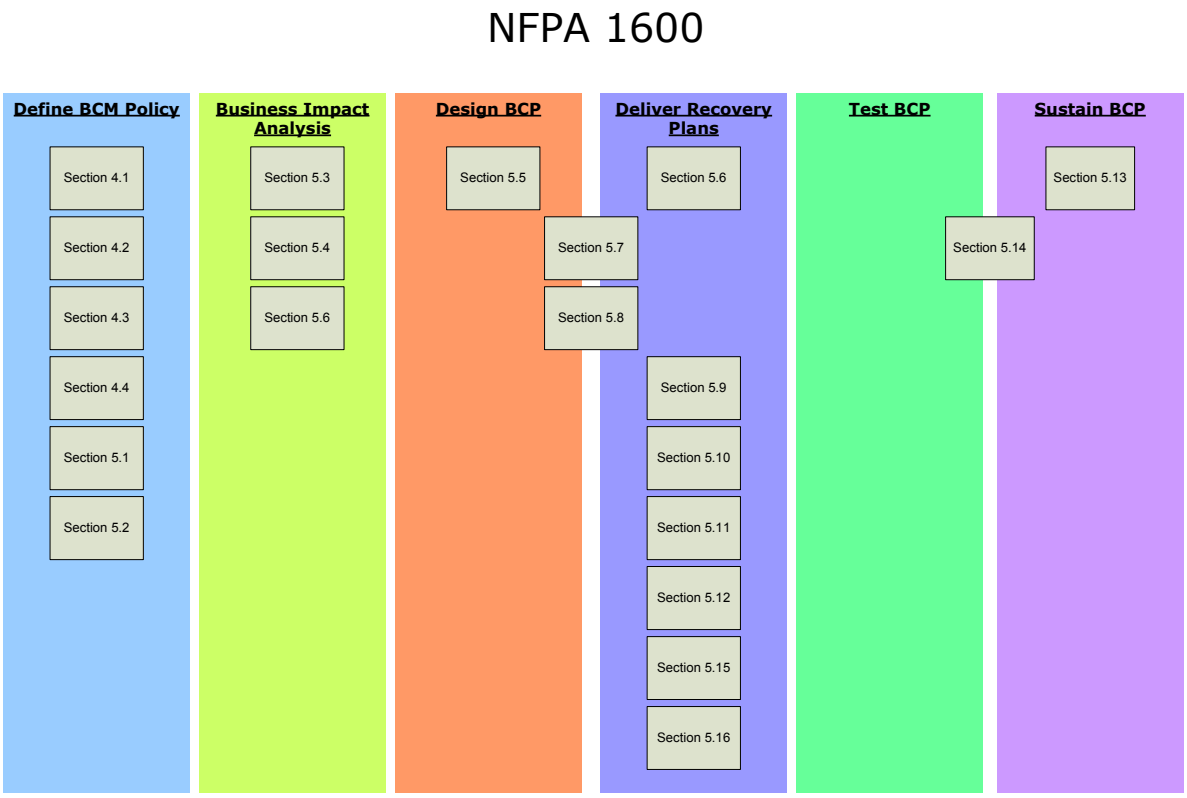
Responsible:
Accountable:
Consulted:
Inputs:
Output: Change of corporate culture; awareness of staff; 12-month Training Plan; annual audit.

E.8.4 Links

There are no links from this standard.

E.9 NFPA 1600

E.9.1 Process Map



E.9.2 Description

NFPA 1600 constitutes a standard for disaster and emergency management and Business Continuity programmes. It is aimed at public, not for profit and private entities. It covers the whole Business Continuity lifecycle, although Testing and Sustaining BCP are not covered in much depth. The main part of the standard is quite high level, although more detail can be found in the appendices.

Chapter 4. Programme Management

Section 4.1: Programme Administration: The programme should include Policy, goals, objectives, programme evaluation, programme plans, statutory and regulatory obligations, budget and records management

Section 4.2: Programme Co-ordinator: The need for a Programme Co-ordinator is highlighted.

Section 4.3: Advisory Committee: The role and responsibilities of the Advisory Committee are given.

Section 4.4: Programme Evaluation: Performance measurements should be established and the programme periodically reviewed.

Chapter 5. Programme Elements

Section 5.1: General: The programme should cover prevention, mitigation, preparedness, response and recovery to identified hazards.

Section 5.2: **Laws and Authorities:** Compliance with applicable regulatory and statutory obligations is required and changes should be reflected within the programme.

Section 5.3: **Risk Assessment:** A Risk Assessment should be conducted which covers natural hazards, human caused events and technological events. The impact of the hazards should be evaluated.

Section 5.4: **Incident Prevention:** A strategy should be developed which prevents incidents which threaten people, property and the environment. The strategy should be kept up to date and the hazards monitored on an ongoing basis.

Section 5.5: **Mitigation:** Based on the identified hazards, interim and long term actions should be developed as part of a mitigation strategy, for incidents which cannot be prevented.

Section 5.6: **Resource Management and Logistics:** The resource requirements to support the programme should be identified and the process of making the resources available during an incident should be documented. Resource shortfall should be detailed and plans put in place to cope with the shortfall.

Section 5.7: **Mutual Aid and Assistance:** The requirements for mutual aid should be determined and planned for if necessary.

Section 5.8: **Planning:** A process should be followed for writing Plans, which should include the following elements, objectives; internal and external roles and responsibilities; lines of authority; logistics and resource requirements; incident management; internal and external communication; strategic, emergency, prevention mitigation, recovery and continuity plans.

Section 5.9: **Incident Management:** An incident management system should be established, which must comply with applicable statutes or regulation.

Section 5.10: **Communications and Warning:** Communications systems should be established and periodically tested, to alert people impacted by the incident.

Section 5.11: **Operational Procedures:** Procedures should developed to respond to and recover from the consequences of the identified hazards.

Section 5.12: **Facilities:** A primary and secondary emergency operations centre should be established, which can support response, continuity and recovery operations.

Section 5.13: **Training:** A full training and education curriculum should be implemented to train personnel in management of the programme and incident management.

Section 5.14: **Exercises, Evaluations and Corrective Actions:** Periodic reviews should be held to evaluate the programme plans, procedures and capabilities. Exercises should be held to test elements of the plan and any deficiencies addressed.

Section 5.15: Crisis Communication and Public Information: Procedures should be written to detail how information should be communicated to internal and external audiences, including the public.

Section 5.16: Finance and Administration: Financial and administrative procedures should be in place to support the programme before, during and after an incident.

E.9.3 Detail

Section 4.1: Programme Administration

Responsible:
Accountable:
Consulted: Executive
Inputs: Applicable authorities; regulators; legislation; codes of practice
Output: BC Policy, Project Plan

Section 4.2: Programme Co-ordinator:

Responsible:
Accountable:
Consulted:
Inputs:
Output: Appointed Programme Co-ordinator

Section 4.3: Advisory Committee

Responsible:
Accountable:
Consulted:
Inputs: Policy
Output: Appointed Advisory Committee.

Section 4.4: Programme Evaluation

Responsible:
Accountable:
Consulted:
Inputs:
Output: Programme Performance Objectives

Section 5.1: General

Responsible:
Accountable:
Consulted:
Inputs:
Output:

Section 5.2: Laws and Authorities

Responsible:
Accountable:
Consulted:
Inputs: Applicable legislation; regulations; directives; policies and industry codes of practice
Output: Strategy for updates to programme to reflect changes in legislation, regulations, directives, policies and industry codes of practice

Section 5.3: Risk Assessment

Responsible:
Accountable:
Consulted:
Inputs:
Output: Hazard Evaluation and Impact Analysis

Section 5.4: Incident Prevention

Responsible:
Accountable:
Consulted:
Inputs: Hazard Evaluation and Impact Analysis
Output: Incident Prevention Strategy

Section 5.5: Mitigation

Responsible:
Accountable:
Consulted:
Inputs: Hazard Evaluation; Risk Assessment; Impact Analysis; Cost Benefit Analysis
Output: Mitigation Strategy

Section 5.6: Resource Management and Logistics

Responsible:
Accountable:
Consulted:
Inputs: BC Policy, Project Plan, Hazard Evaluation, Impact Analysis
Output: Resource Management Objectives

Section 5.7: Mutual Aid/Assistance

Responsible:
Accountable:
Consulted:
Inputs:
Output: Mutual Aid Agreements

Section 5.8: Planning

Responsible:
Accountable:
Consulted:
Inputs: BC Policy
Output: Strategic Plan; Emergency Operations/Response Plan; Prevention Plan; Mitigation Plan; Recovery Plan; Continuity Plan

Section 5.9: Incident Management

Responsible:
Accountable:
Consulted:
Inputs:
Output: Incident Management System; policies and procedures

Section 5.10: Communications and Warning

Responsible:
Accountable:
Consulted:

Inputs:
Output: Emergency Communications Systems; Processes and Procedures

Section 5.11: Operational Procedures
Responsible:
Accountable:
Consulted:
Inputs:
Output: Operational Procedures

Section 5.12: Facilities
Responsible:
Accountable:
Consulted:
Inputs:
Output: Established Primary and Secondary Emergency Operations Centre

Section 5.13: Facilities
Responsible:
Accountable:
Consulted:
Inputs:
Output: Training curriculum

Section 5.14: Exercises, Evaluations and Corrective Actions
Responsible:
Accountable:
Consulted:
Inputs: Programme plans and procedures
Output: Reviewed, tested, exercised and updated programme plans, procedures and capabilities

Section 5.15: Crisis Communications and Public Information
Responsible:
Accountable:
Consulted:
Inputs: Hazard Evaluation; Impact Analysis
Output: Procedures for pre-incident, incident and post incident communications

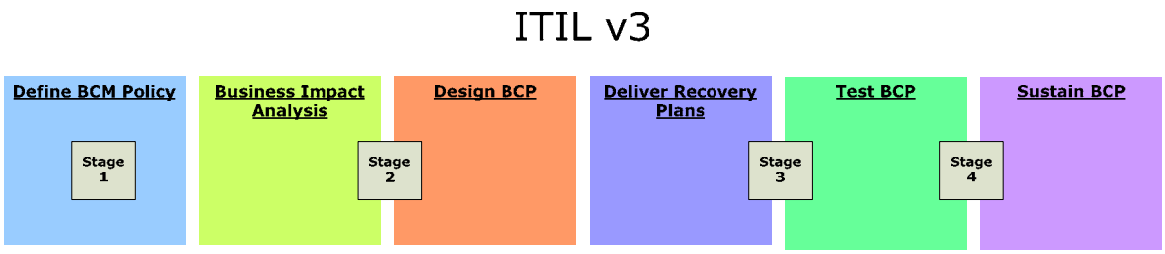
E.9.4 Links

Reference is made to the following:

NFPA 1561, Standard on Emergency Services Incident Management System, 2005 edition
FEMA CAR

E.10 ITIL v3

E.10.1 Process Map



E.10.2 Description

Information Technology Infrastructure Library (ITIL) is the documentation and management of consistent and comprehensive best practice for IT Service Management. Used by many hundreds of organisations around the world, a whole ITIL philosophy has grown up around the guidance contained within the ITIL books and is supported by a professional qualification scheme.

The ITIL framework has a number of modules, one of which is IT Service Continuity Management. The framework allows modules to be implemented in isolation although there are obvious links between them.

The ITSCM component does not rely on BCM being in place but is enhanced if implemented in conjunction with it.

E.10.3 Detail

Stage 1 - Initiation

Responsible:
Accountable:
Consulted:
Inputs:
Output: Scope; Terms of Reference; roles and responsibilities; resource allocation; project organisation and control structure; agreed quality and project plan

Stage 2 - Requirements and Strategy

Responsible:
Accountable:
Consulted:
Inputs:
Output: BIAs; Risk Analysis; Risk Response Measures; ITSCM recovery options

Stage 3 - Implementation

Responsible:
Accountable:
Consulted:
Inputs: Business Continuity Plans; Change Management and Configuration Management
Output: IT Service Continuity Plan; initial testing

Stage 4 - Requirements and Strategy

Responsible:
Accountable:
Consulted:
Inputs:
Output: Education, awareness and training; regular review; test programme; Change Management

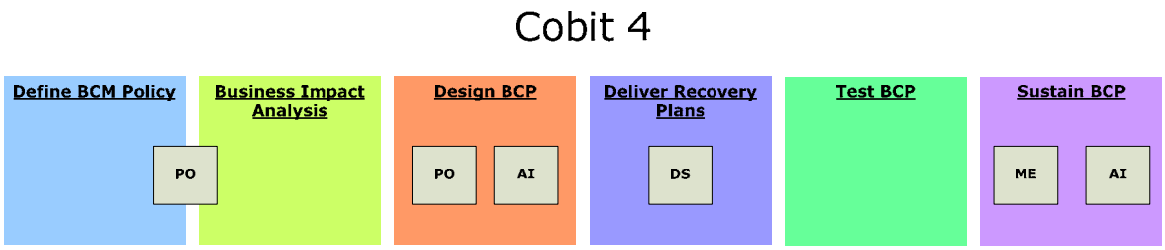
E.10.4 Links

The framework references are:

- ISO 27001
- Prince 2 (Project Management)
- Project Management Institute – 'Project Management Body of Knowledge'
- ITIL - Change Management and Configuration Management
- ITIL – Service Operation

E.11 Cobit v4

E.11.1 Process Map



E.11.2 Description

The four programmes run in parallel and overlap greatly, the four disciplines are:

Plan and Organise
PO1 Define a Strategic IT Plan
PO2 Define the Information Architecture
PO3 Determine Technological Direction
PO4 Define the IT Processes, Organisation and Relationships
PO5 Manage the IT Investment
PO6 Communicate Management Aims and Direction
PO7 Manage IT Human Resources
PO8 Manage Quality
PO9 Assess and Manage IT Risks
PO10 Manage Projects

Acquire and Implement
AI1 Identify Automated Solutions
AI2 Acquire and Maintain Application Software
AI3 Acquire and Maintain Technology Infrastructure
AI4 Enable Operation and Use
AI5 Procure IT Resources
AI6 Manage Changes
AI7 Install and Accredit Solutions and Changes

Deliver and Support
DS1 Define and Manage Service Levels
DS2 Manage Third-party Services
DS3 Manage Performance and Capacity
DS4 Ensure Continuous Service
DS5 Ensure Systems Security
DS6 Identify and Allocate Costs
DS7 Educate and Train Users
DS8 Manage Service Desk and Incidents
DS9 Manage the Configuration
DS10 Manage Problems
DS11 Manage Data
DS12 Manage the Physical Environment
DS13 Manage Operations

Monitor and Evaluate
ME1 Monitor and Evaluate IT Performance
ME2 Monitor and Evaluate Internal Control
ME3 Ensure Regulatory Compliance

ME4 Provide IT Governance

E.11.3 Detail

Plan and Organise

Responsible: ICT and business stakeholders
Accountable: CEO, CIO
Consulted: Senior management (CEO, CFO, CIO) and IT stakeholders.
Inputs: Business requirements; business goals and ICT goals; IT skills matrix, HR policies; IT financials, infrastructure requirements; IT Risk Management guidelines; Post-implementation Review; process framework improvements; known errors; supplier risks; IT risk remedial action plans; report on effectiveness of IT controls; enterprise appetite for IT risks
Output: Strategic IT Plan; Tactical Plans; technological standards; IT process framework documentation/framework roles and responsibilities; cost benefits IT budgets IT service portfolio IT project portfolio; IT control framework IT policies Risk Assessment IT sourcing strategy IT acquisition strategy HR policies IT training requirements; project management guidelines

Acquire and Implement

Responsible: CIO
Accountable: CIO
Consulted: IT management
Inputs: Strategic IT Plan Tactical Plans IT service portfolio IT acquisition strategy; Business Requirements; Documentation/framework roles and responsibilities; IT control framework IT policies; IT acquisition strategy; IT risk remedial action plans; Project Management guidelines; cost benefits; required Documentation updates; Supplier catalogue; required security changes; RFCs; Problem records; SLAs
Output: Business Requirements; Post-implementation Review; procurement decisions; Planned SLAs Planned OLAs; Change process description change process status reports change authorisation; physical environment requirements; User, ops, support, technical and admin. manuals; training material; 3rd party relationship management; contracts; release configuration known errors promotion to production Software release and Distribution Plan

Deliver and Support

Responsible: CIO Head of Operations
Accountable: Head of Operations
Consulted: Business users IT stakeholders
Inputs: Strategic IT Plan Tactical Plans IT sourcing Strategy; Documentation/framework roles and responsibilities; IT budgets; IT control framework IT policies IT training requirements; IT acquisition strategy; Risk Assessment; Planned SLAs Planned OLAs SLAs OLAs; physical environment requirements; User, ops, support, technical and admin manuals; training material; 3rd party relationship management Contracts; change authorisation;

	Release configuration known errors promotion to production Software release and Distribution Plan
Output:	Updated service requirements updated service portfolio; IT financials; required Documentation updates; Supplier catalogue; required security changes; RFCs; Problem records; SLAs OLAs; Supplier risks; Process performance reports; Incident tickets; Backup storage and Protection Plan

Monitor and Evaluate

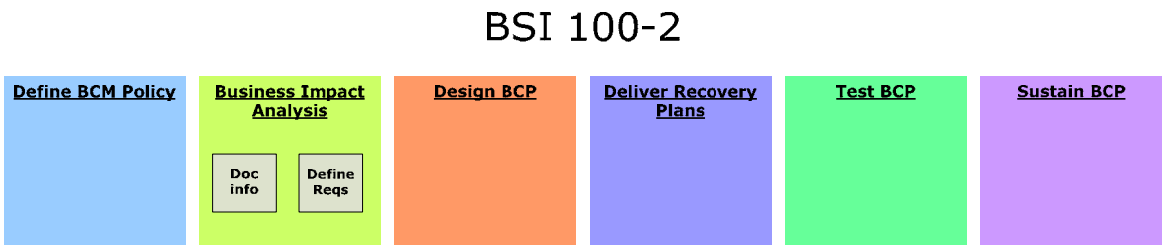
Responsible:	CEA
Accountable:	Board
Consulted:	CFO CIO IT stakeholders
Inputs:	IT governance status report Strategic direction for IT; IT process framework; Documentation/framework roles and responsibilities; IT control framework IT policies; Risk Assessments; change process status reports; known errors; Process performance reports; legal and regulatory compliance requirements
Output:	IT risk remedial action plans; process framework improvements; report on effectiveness of IT Controls; catalogue of IT; enterprise appetite for IT risks

E.11.4 Links

This framework contains no links to other standards.

E.12 BSI 100-2

E.12.1 Process Map



E.12.2 Description

The IT-Grundschutz methodology is a BSI methodology for effective IT Security Management. It defines a requirement for data protection to ensure confidentiality, integrity and availability.

It helps to develop the IT Security Concept but falls short of a full and tested Continuity Plan. The section at the end covers the full process of IT security from determining requirements, assigning responsibilities to writing and implementing plans. This is a very high-level process with no detail, training or testing.

E.12.3 Detail

Documenting Information about the IT Applications and Related Information

Responsible:
Accountable:
Consulted:
Inputs: Network Plan; IT Asset Register
Output: IT Systems documentation; IT Applications and data documentation; room usage and security documentation.

Defining Protection Requirements (for IT Applications, Systems, Communications and Rooms)

Responsible:
Accountable:
Consulted:
Inputs: Potential damage of data loss; legal and regulatory requirements; financial consequences
Output: Assignment table (Risk Assessment); network link criticality.

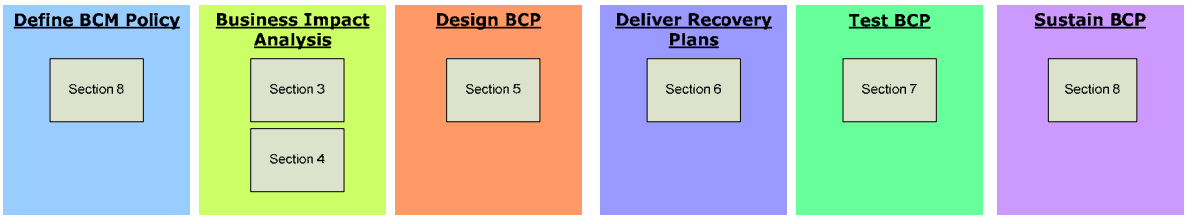
E.12.4 Links

- There are no links from this standard.

E.13 TR 19

E.13.1 Process

TR 19



E.13.2 Description

Section 3 – Risk Analysis and Review
This section describes a Risk Management process and provides some examples of potential areas of risk. Risks should be considered in the following categories:

- Processes
- People
- Infrastructure

Each risk should then be assessed and the relevant risk treatment applied. This will be:

- Risk avoidance
- Risk reduction
- Risk transfer
- Risk acceptance

Risks that cannot be avoided, reduced, transferred or accepted should be passed to the BCM Steering Committee, who will review the outstanding risks together with the probable disaster which could ensue if the risk is not dealt with. This work will lead to a list of critical functions and the selected probable disaster shall also serve as the focus for the development of the BC Plan.

Section 4 – Business Impact Analysis
Section 4 describes how an organisation should conduct a Business Impact Analysis to assess the potential loss from a risk occurrence. It states that the following activities should be undertaken:

- Establish policies to govern the assessment of losses due to interruptions to business operations or processes and document the Minimum Business Continuity Objective of the organisation
- Draw up a preliminary list of potential risks and threats for further deliberation by the BCM Steering Committee
- Establish the priority of analysing the impact of risk on critical business functions
- Identify the probable disasters that could disrupt the organisation's operations and functions
- Identify and analyse critical business functions
- Assign knowledgeable functional area representatives to take part in the BIA
- Identify and assess the probable impacts on infrastructure

Section 5 – Strategy
This section of TR 19 examines the possible strategies for maintaining the operations of the organisation's Critical Business Functions (CBFs). It suggests that the organisation may wish to adopt a composite strategy based on its CBFs interdependencies and their recovery time requirements in conjunction with the probable disasters.

The strategy should cover:

- Processes
- People
- Infrastructure

The strategy shall be formulated to cover:

- Revert to alternate processing capability
- Arrange reciprocal arrangements, eg. With another organisation in the same industry
- Establish alternate site or business facility
- Arrange for alternate source of supply eg. of raw materials
- Outsource to external vendor
- Transfer of operation to subsidiary business units
- Rebuild from scratch after disaster
- Do nothing
- Others

Section 6 - Business Continuity Plan
The BC Plan should cater to a minimum of three sets of activities:

- Response to an incident, emergency or disaster
- Recover and resume critical business functions
- Restore and return all business operations from temporary measures adopted during recovery to support business requirements after disaster

TR 19 states that the BC Plan should cover:

- Criteria for disaster declaration
- Business units
- Priorities for action
- Emergency response
- Documentation
- Pre-incident preparation
- Initial damage assessment
- Emergency response procedures
- Crisis communications
- Co-ordination with external agencies
- Critical items list
- Hazardous materials handling
- Inventory lists
- IT Disaster Recovery Plan
- Security and control (physical, logical and information)
- Information processing, information security and information system requirements
- Restoration and return after disaster
- BC Plan distribution and control
- Roles and responsibilities
- Infrastructure

- Emergency operations centre
- Alternate site requirements
- Contact lists

Section 7 – Tests and Exercises
This section of the Standard describes why testing and exercising should be carried out and how to implement this stage of BCM.

A schedule of tests and exercises should be established which should achieve the following objectives:

- Verify that the BCP is viable and practical
- Verify that the recovery time scale and priorities can be met eg. the RTO
- Verify that vendors identified in the BCP can support the recovery in a timely, efficient and effective manner
- Verify that the resources identified in the BCP can be activated an accessed in a timely efficient, effective and adequate manner
- Rehearse and train personnel involved in the actual recovery
- Identify areas to be improved or fine tuned

Section 8 – Programme Management
This area of BCM as described in TR 19 examines the ongoing efforts and activities of the organisation to maintain the vibrancy of BCM in the organisation. Reviews should be conducted on a systematic and periodic basis or when there are significant changes to the business operations and or environment. These reviews shall cover:

- Risks and recovery strategies
- Minimum Business Continuity objective
- Roles and responsibilities
- BCP
- Vendor contracts
- Training and awareness
- BCM trends
- Infrastructure
- Facilities
- Alternate site readiness

A programme structure should be established which defines:

- Roles and responsibilities
- BCM Meetings
- Participation in industry BCM activities

All staff should undergo BCM training and awareness programmes and receive training in the following activities:

- Evacuation and assembly
- Activation of alarm
- Emergency response
- Reporting to the appropriate authority to handle the emergency

E.13.3 Details

Section 3 – Risk Analysis and Review
Responsible: Personnel with appropriate expertise

Accountable: BCM Steering Committee
Consulted:
Inputs: Threats to the organisation
Output: Risk Assessment, probable disasters

Section 4 – Business Impact Analysis
Responsible: Personnel with appropriate expertise
Accountable: BCM Steering Committee
Consulted:
Inputs: Risk Assessment
Output: Business Impact Analysis, Critical Business Functions (CBF), Minimum Business Continuity Objective (MBCO)

Section 5 – Strategy
Responsible: Staff with relevant skills
Accountable: BCM Steering Committee
Consulted:
Inputs: CBFs, BIA
Output: BCM Strategies

Section 6 – Business Continuity Plan
Responsible:
Accountable: BCM Steering Committee
Consulted:
Inputs: Strategies
Output: BCP to cover incident response, recover and resumption, restore and return to normal operations, establishment of Emergency Operations Centre

Section 7 – Tests and Exercises
Responsible:
Accountable: BCM Steering Committee
Consulted:
Inputs: BCP, CBFs
Output: Verified BCP, trained personnel

Section 8 – Programme Management
Responsible:
Accountable: BCM Steering Committee
Consulted: Staff
Inputs: BCP, MBCO
Output: Reviewed BCP Programme Management Plan

E.13.4 Links

The Bibliography references a number of other BC publications.

Appendix F: GLOSSARY

Foreword

This Glossary of Terms has been produced to accompany the ENISA Report on Business and IT Continuity. It comprises Business Continuity, IT Continuity, Information Security, Security Emergency and Risk terminology.

Terminology	Explanation	Source
ACCEPTABLE RISK	The level of residual risk that has been determined to be a reasonable level of potential loss/disruption	CIAO – Critical Infrastructure Assurance Office - USA
ACCESS OVERLOAD CONTROL (ACCOLC)	The Access Overload Control scheme gives call preference to registered essential users on the four main mobile networks in the UK if the scheme is invoked during an emergency.	NASP – National Association of Security Professionals
ACCOUNTABILITY	The property that ensures that the actions of an entity may be traced uniquely to the entity	ENISA
ACTION LISTS	A specific Business Continuity Management term referring to defined actions, allocated to recovery teams and individuals, within a phase of a plan. These are supported by reference data.	ENISA
ACTIVATION	The implementation of Business Continuity procedures, activities and plans in response to a Business Continuity Emergency, Event, Incident and/or Crisis	The BCI
ACTIVITY	Processes carried out by an organisation, for example, Accounts. See: Business Activity	Emergency Planning College
AGREED SERVICE TIME	The time during which a particular Business Continuity is agreed to be fully available, ideally as defined in the Service Level Agreement. Different levels of service might apply within the agreed service time, for instance the Service Desk might not be available for all the hours that users can access their services.	ENISA
ALERT	A formal notification that an incident has occurred which may develop into a Business Continuity Management or Crisis Management invocation	ENISA
ALERT PHASE	The first phase of a Business Continuity Plan in which the initial emergency procedures and damage	ENISA

Terminology	Explanation	Source
	assessments are activated	
ALTERNATE ROUTING	The routing of information via another medium should the primary means become unavailable	The BCI
ALTERNATE SITE	A site held in readiness for use during a Business Continuity incident to maintain the Business Continuity of an organisation's Mission Critical Activities. The term applies equally to office or technology requirements. Alternate sites may be 'cold', 'warm' or 'hot'. This type of site is also known as a Recovery Site.	The BCI
ALTERNATE WORK AREA	Recovery environment complete with necessary infrastructure (desk, telephone, workstation, and associated hardware and equipment, communications, etc.)	ENISA
ALTERNATIVE	The routing of information via an alternative cable routing medium (i.e. using different networks should the normal network be rendered unavailable)	Emergency Planning College and The BCI
ANNUAL LOSS EXPOSURE/EXPECTANCY (ALE)	A Risk Management method of calculating loss based on a value and level of frequency	Emergency Planning College
APPLICATION RECOVERY	The component of Disaster Recovery that deals specifically with the restoration of business system software and data after the processing platform has been restored or replaced	IT Recovery Site
ASSEMBLY AREA	The designated area at which employees, visitors, and contractors assemble if evacuated from their building/site	The BCI
ASSET	An item of property and/or component of a business activity/process owned by an organisation	The BCI
ASSURANCE	The activity and method whereby an organisation can verify and validate its BCM capability	ENISA
AUDIT	The method by which procedures and/or documentation are measured against pre-agreed standards	The BCI
AUTOMATIC FAILOVER	The ability to automatically re-route end users and applications to a replica server, where they can continue to work with minimal interruption and productivity loss	ENISA

Terminology	Explanation	Source
AVAILABILITY	An umbrella term that includes reliability (including resilience), maintainability, serviceability and security. A common definition of availability is 'the ability of a component or Business Continuity (under combined aspects of its reliability, maintainability and security) to perform its required function at a stated instant or over a stated period of time'. Service availability is sometimes expressed as an availability percentage, i.e. the proportion of time that the service is actually available for use by the customers within the agreed service time.	ENISA
BACKLOG	The effect on the business of a build-up of work that occurs as the result of a system or method being unavailable for an unacceptable period. A situation whereby a backlog of work requires more time to action than is available through normal working patterns. In extreme circumstances, the backlog may become so marked that the backlog cannot be cleared.	The BCI
BACKLOG TRAP	The effect on the business of a backlog of work that develops when a system or process is unavailable for a long period, and which may take a considerable length of time to reduce	ENISA
BACK-OUT PLAN	A plan that documents all actions to be taken to restore the service if the associated Change or Release fails or partially fails. Back-out plans may provide for a full or partial reversal. In extreme circumstances they may simply call for the Business Continuity Plan to be invoked.	Emergency Planning College and the UK Financial Sector Continuity
BACKUP	A method by which data, electronic or paper based, is copied in some form so as to be available and used if the original data from which it originated is lost, destroyed or corrupted	The BCI
BACKUP GENERATOR	An independent source of power, usually fuelled by diesel or natural gas	ENISA
BATTLE BOX	A container in which data, information and other essentials is stored so as to become readily available to those responding to an incident	The BCI
BENCHMARKING	A form of comparison usually between the activities of one organisation and	UK Financial Sector Continuity

Terminology	Explanation	Source
	those of one or more comparable external organisations. Also used to describe a form of simulation modelling where the entire operational environment is replicated or simulated	
BODY HOLDING AREA	An area close to the scene of an emergency where the dead can be held temporarily before transfer to the emergency mortuary or mortuary	NASP – National Association of Security Professionals
BRAINSTORMING	A Problem Management technique used to quickly generate, clarify and evaluate a sizeable list of ideas, Problems, issues , themes, etc. by documenting 'what we know' as a team, tapping the creative thinking of the team and getting everyone involved. The technique is particularly useful in identifying possible causes when constructing a Cause / Effect Diagram.	UK Financial Sector Continuity
BRONZE TEAM	Bronze or Operational (Incident) Team is the level at which the management of hands-on work is undertaken at the incident site or impacted areas.	ENISA
BS 25999	The British Standards Institution 'Specification for Business Continuity Management'	ENISA
BS 7799	The British Standards Institution standard for information security management. Section 9 deals with Business Continuity Management. The corresponding international standard is known as ISO 17799.	The BCI
BS 7799-1:2000	The British Standards Institution 'Code of practice for information security management'. Also referred to as ISO/IEC 17799-2000	ENISA
BS 15000	The British Standards Institution 'Specification for IS service management'	ENISA
BSA	Bomb Shelter Area; internal area that offers protection from blast, flying glass and other fragments.	The British Army
BSI	The British Standards Institution	The BSI
BUILDING DENIAL	Any damage, failure or other condition which causes denial of access to the building or the working area within the building, e.g. fire, flood, contamination, loss of services, air conditioning failure, and forensics	ENISA
BUSINESS ACTIVITY	A group of activities/processes undertaken by an organisation to	The BCI

Terminology	Explanation	Source
	produce a product and/or service and/or in pursuit of a common goal	
BUSINESS ACTIVITY LEVELS	The predicted or historic levels of business method activity that are to be or have been supported by the IS infrastructure. Measured in business terms (e.g. number of account holders).	ENISA
BUSINESS AS USUAL (BAU)	The normal state of operations	The BCI
BUSINESS CONTINUITY (BC)	A proactive process which identifies the key functions of an organisation and the likely threats to those functions	The BCI
BUSINESS CONTINUITY MANAGEMENT (BCM)	A holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities. Also the management of the overall programme through training, rehearsals, and reviews, to ensure the plan stays current and up to date.	The BCI, modified by ENISA
BUSINESS CONTINUITY MANAGEMENT ACTIVITY	An action or series of actions that forms part of the BCM process	The BCI
BUSINESS CONTINUITY (MANAGEMENT) CO-ORDINATOR	A member of the Business Continuity Management team who is assigned the overall responsibility for co-coordination of the recovery planning programme including team member training, testing and maintenance of recovery plans (associated terms: business recovery planner, disaster recovery planner, business recovery co-coordinator, disaster recovery administrator)	The BCI modified by ENISA
BUSINESS CONTINUITY MANAGEMENT LIFECYCLE	The activities and processes divided into various stages that are necessary to manage Business Continuity	The BCI
BUSINESS CONTINUITY MANAGEMENT MATURITY	The level and degree to which Business Continuity activities have become standard and assured practices within the organisation	The BCI
BUSINESS CONTINUITY MANAGEMENT PLAN	A collection of procedures and information which is developed, compiled and maintained in readiness for use in the event of an emergency or disaster	BS 25999-1
BUSINESS CONTINUITY MANAGEMENT PLANNING	The advance planning and preparations which are necessary to	The BCI

Terminology	Explanation	Source
	identify the impact of potential losses; to formulate and implement viable recovery strategies; to develop recovery plan(s) which ensure continuity of organisational services in the event of an emergency or disaster; and to administer a comprehensive training, testing and maintenance programme	
BUSINESS CONTINUITY MANAGEMENT POLICY	A BCM policy sets out an organisation's aims, principles and approach to BCM, what and how it will be delivered, key roles and responsibilities and how BCM will be governed and reported upon	The BCI
BUSINESS CONTINUITY MANAGEMENT PROCESS	A set of activities/processes with defined outcomes, deliverables and evaluation criteria that form a distinct part of the BCM lifecycle	The BCI, modified by ENISA
BUSINESS CONTINUITY MANAGEMENT PROGRAMME	An ongoing management and governance method supported by senior management and 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/services through exercising, rehearsal, testing, training, maintenance and assurance	The BCI
BUSINESS CONTINUITY MANAGEMENT TEAM	A group of individuals functionally responsible for directing the development and execution of the Business Continuity Plan, as well as responsible for declaring a disaster and providing direction during the recovery process, both pre-disaster and post-disaster	ENISA
BUSINESS CONTINUITY OBJECTIVE	The desired time within which business method should be recovered, and the minimum staff, assets and services required within this time	ENISA
BUSINESS CONTINUITY PLAN (BCP)	Documents describing the roles, responsibilities and actions necessary to resume business processes following a disruption. The Business Continuity Plan will provide a defining structure for and exert a major influence upon the development of IS continuity plans. Its scope both encompasses and exceeds Business Continuity Management and is normally a business responsibility.	ENISA
BUSINESS CONTINUITY TEAM	One of a number of groups of people with defined, agreed and documented	ENISA

Terminology	Explanation	Source
	roles within the business recovery process	
BUSINESS CRITICAL FUNCTIONS	Critical operational or support activities	The BCI
BUSINESS CRITICAL POINT	The latest moment at which the business can afford to be without a critical function or process	The BCI
BUSINESS FUNCTION	A business unit within an organisation e.g. a department, division, branch	The BCI
BUSINESS IMPACT ANALYSIS (BIA)	An assessment of the minimum level of resources e.g. personnel, workstations, technology, telephony required, overtime, after a Business Continuity Incident to maintain the continuity of the organisation's Mission Critical Activities at a minimum level of service/production. The BIA measures the effect of resource loss and escalating losses over time in order to provide senior management with reliable data upon which to base decisions on risk mitigation and continuity planning. Generally considered to be part of a BIA it is an integral part of any subsequent resource Gap Analysis.	The BCI, UK Financial Sector Continuity, modified by ENISA
BUSINESS INTERRUPTION	Any event, whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout) which disrupts the normal course of business operations at an organisation’s location	ENISA
BUSINESS INTERRUPTION COSTS	The impact to the business caused by different types of outages, normally measured by revenue lost	ENISA
BUSINESS INTERRUPTION INSURANCE	Insurance coverage for disaster related expenses that may be incurred until operations are fully recovered after a disaster	ENISA
BUSINESS OBJECTIVES	The measurable targets designed to help an organisation achieve its overall business strategy	ENISA
BUSINESS OPERATIONS	Activities and procedures carried out by the User community in performing the business role of an organisation. A Service Desk is concerned with supporting and dealing with the comments and requests arising from those business operations.	ENISA
BUSINESS PROCESS	A series of related business activities aimed at achieving one or more business objectives in a measurable manner. Typical business processes include receiving orders, marketing services, selling products, delivering	ENISA

Terminology	Explanation	Source
	services, distributing products, invoicing for services, accounting for money received. A business method will usually depend upon several business functions for support e.g. IT, personnel, accommodation. A business method will rarely operate in isolation, i.e. other business processes will depend on it and it will depend on other processes. See Process	
BUSINESS RECOVERY CO-ORDINATOR	An individual or group designated to coordinate or control designated recovery processes or testing	ENISA
BUSINESS RECOVERY TEAM	A group of individuals responsible for maintaining the business recovery procedures and coordinating the recovery of business functions and processes See Disaster Recovery Teams	The BCI, modified by ENISA
BUSINESS RECOVERY TIMELINE	The chronological sequence of recovery activities, or critical path, that must be followed to resume an acceptable level of operations following a business interruption. This timeline may range from minutes to weeks, depending upon the recovery requirements and methodology.	ENISA
BUSINESS RISK	The risk that external factors, such as a fall in demand for an organisations products or services, will result in unexpected loss. Business risk, if managed well, can also result in a competitive advantage being gained.	ENISA
BUSINESS UNIT RECOVERY (PLAN)	A component of Business Continuity which deals specifically with the recovery of a key function or department in the event of a disaster	UK Financial Sector Continuity
CALL TREE	A structured cascade method (system) that enables a list of persons, roles and/or organisations to be contacted as a part of a plan invocation procedure or in order to disseminate information. Graphically depicts the calling responsibilities and the calling order used to contact management, employees, customers, vendors, and other key contacts in the event of an emergency, disaster, or severe outage situation.	The BCI, modified by ENISA
CALL TREE CASCADE TEST	A test designed to validate the currency of contact lists and the processes by which they are maintained	The BCI

Terminology	Explanation	Source
CAPABILITY	Originally a military term which includes the aspects of personnel, equipment, training, planning and operational doctrine, now used to mean a demonstrable capacity or ability to respond to and recover from a particular threat or hazard	The British Army
CASCADE SYSTEM	A system whereby one person or organisation calls out/contacts others who in turn initiate further call-outs/contacts as necessary. Similar Terms: Contact List, Call Tree	The BCI
CASUALTY BUREAU	The purpose of the Casualty Bureau is to provide the initial point of contact for the receiving and assessing of information relating to persons believed to be involved in the emergency. The primary objectives of a Casualty Bureau are to: inform the investigation process relating to the incident; trace and identify people involved in the incident; and reconcile missing persons and collate accurate information in relation to the above for dissemination to appropriate parties.	NASP – National Association of Security Professionals
CATEGORY 1 RESPONDER	A person or body listed in Part 1 of Schedule 1 to the UK Civil Contingencies Act. These bodies are likely to be at the core of the response to most emergencies. As such, they are subject to the full range of civil protection duties in the Act. Examples of Category 1 responders include the emergency services and local authorities.	UK Civil Contingencies Act, modifed by ENISA
CATEGORY 2 RESPONDER	A person or body listed in Part 3 of Schedule 1 to the UK Civil Contingencies Act. These are co-operating responders who are less likely to be involved in the heart of multi-agency planning work, but will be heavily involved in preparing for incidents affecting their sectors. The Act requires them to co-operate and share information with other Category 1 and 2 responders. Examples of Category 2 responders include utilities and transport companies.	UK Civil Contingencies Act, modified by ENISA

Terminology	Explanation	Source
CBRN	Chemical, Biological, Radiological and Nuclear. Chemical, biological and radiological incidents involve both the release of the corresponding material and threats, hoaxes and false alarms. A nuclear incident would involve the detonation of a nuclear weapon or an improvised nuclear device.	NASP – National Association of Security Professionals and The British Army, modified by ENISA
CENTRAL COMPUTER AND TELECOMMUNICATIONS AGENCY	The CCTA was the UK Government Centre for Information Systems responsible for producing and maintaining ITIL. Now subsumed within the OGC	UK Government Site
CERTIFICATION	The formal evaluation of an organisation's processes by an independent and accredited body against a defined standard and the issuing of a certificate indicating conformance	ENISA
CHANGE	Any deliberate action that alters the form, fit or function of key business activities - typically, an addition, modification, movement or deletion that impacts on the IS infrastructure	ENISA
CHANGE CONTROL	The procedures to ensure that all changes are controlled, including the submission, recording, analysis, decision making, approval, implementation and post-implementation review of the change	ENISA
CHECKLIST	A tool to remind and /or validate that tasks have been completed and resources are available, to report on the status of recovery	ENISA
CHECKLIST EXERCISE	A method used to exercise a completed disaster recovery plan. This type of exercise is used to determine whether the information such as phone numbers, manuals, equipment, etc. in the plan is accurate and current.	ENISA
CIVIL CONTINGENCIES ACT (CCA)	The Civil Contingencies Act 2004 establishes a single framework for civil protection in the United Kingdom. Part 1 of the Act establishes a clear set of roles and responsibilities for local responders. Part 2 modernises the emergency powers framework in the United Kingdom.	UK Financial Sector Continuity, modified by ENISA
CIVIL EMERGENCY	Event or situation which threatens serious damage to human welfare in a place in the UK, the environment or security of the UK as defined in the Civil Contingencies Act 2004	NASP – National Association of Security Professionals and The British Army,

Terminology	Explanation	Source
		modified by ENISA
CIVIL PROTECTION	Preparedness to deal with a wide range of emergencies from localised flooding to terrorist attack	NASP – National Association of Security Professionals and The British Army, modified by ENISA
CLERICAL BACKUP	In case of contingency, delivering some part of the required services without the IS infrastructure. Nowadays, as well as some manual processes, this is likely to be via standalone PCs and commercial office systems software.	ENISA
COLD SITE	One or more data centres or office space facilities equipped with sufficient pre-qualified environmental conditioning, electrical connectivity, communications access, configurable space and access to accommodate the installation and operation of equipment by critical staff required to resume business operations	The BCI, modified by ENISA
COLD STANDBY/START/SITE (portable or fixed)	An empty computer room, either in portable accommodation or on a fixed site, with power, environmental control and telecommunications, but no IS equipment or software for use in an emergency. See Gradual Recovery	Disaster Recovery Journal, modified by ENISA
COMAH	UK Control of Major Accident Hazards regulations. They apply mainly to the chemical industry, but also to some storage, explosives and nuclear sites, and other facilities which use or keep dangerous substances.	NASP – National Association of Security Professionals
COMMAND AND CONTROL	Principles adopted by an agency acting with full authority to direct its own resources (both personnel and equipment). During an incident operations will be directed at strategic, tactical or operational levels to achieve the recovery objectives of the organisation and to bring the incident to a successful conclusion.	The BCI, modified by ENISA
COMMAND CENTRE (CC)	The facility used by a Crisis/Incident Management Team after the first phase of a Business Continuity incident (often referred to as the incident response or emergency response phase). An organisation must have a primary and secondary location for a command centre in the event of one being unavailable. It	The BCI, modified by ENISA

Terminology	Explanation	Source
	may also serve as a reporting point for deliveries, services, press and all external contacts. See also Emergency Operations Centre	
COMMAND, CONTROL, AND COORDINATION	A Crisis Management process. Command means the authority for an organisation or part of an organisation to direct the actions of its own resources (both personnel and equipment). Control means the authority to direct strategic, tactical and operational operations in order to complete an assigned function. This includes the ability to direct the activities of others engaged in the completion of that function, i.e. the crisis as a whole or a function within the crisis management process. The control of an assigned function also carries with it the responsibility for the health and safety of those involved. Coordination means the integration of the expertise of all the agencies/roles involved with the objective of effectively and efficiently bringing the crisis to a successful conclusion.	The BCI
COMMUNICATIONS RECOVERY	The component of Disaster Recovery which deals with the restoration or rerouting of an organisations telecommunication network, or its components, in the event of loss	The Disaster Recovery Journal
COMPUTER RECOVERY TEAM	A group of individuals responsible for assessing damage to the original system, processing data in the interim, and setting up the new system.	ENISA
CONSEQUENCE	The end result following a Business Continuity incident that can be defined as loss, injury, disadvantage or gain	The BCI
CONSORTIUM AGREEMENT	An agreement made by a group of organisations to share processing facilities and/or office facilities if one member of the group suffers a disaster	The Disaster Recovery Journal
CONTACT LIST	A list of team members and/or key personnel to be contacted including their backups	ENISA
CONTINGENCY FUND	An operating expense that exists as a result of an interruption or disaster which seriously affects the financial position of the organisation	ENISA
CONTINGENCY PLAN	Actions to be followed in the event of	ENISA

Terminology	Explanation	Source
	a disaster or emergency occurring which threatens to disrupt or destroy the continuity of normal business activities and which seeks to restore operational capabilities. Now largely incorporated within Business Continuity Plan.	
CONTINGENCY PLANNING	Process of developing advanced arrangements and procedures that enable an organisation to respond to an undesired event that negatively impacts the organisation	ENISA
CONTINUITY OF GOVERNMENT (COG)	The basis of PDD-NSC-67 (Presidential Decision Directives) - Enduring Constitutional Government and Continuity of Government Operations	PDD-NSC-67
CONTINUITY OF OPERATIONS PLAN (COOP)	A COOP provides guidance on the system restoration for emergencies, disasters, mobilization, and for maintaining a state of readiness to provide the necessary level of information processing support commensurate with the mission requirements/priorities identified by the respective functional proponent. The US Federal Government and its supporting agencies traditionally use this term to describe activities otherwise known as Disaster Recovery, Business Continuity, Business Resumption, or Contingency Planning.	PDD-NSC-67
CONTINUOUS AVAILABILITY	A characteristic of an Business Continuity that masks from the users the effects of losses of service, planned or unplanned. See Continuous Operation	The Disaster Recovery Journal, modified by ENISA
CONTINUOUS OPERATIONS	The ability of an organisation to perform its processes without interruption	The Disaster Recovery Journal, Modified by ENISA
CONTROL	Any action which reduces the probability of a risk occurring or reduces its impact if it does occur	The BCI

Terminology	Explanation	Source
CONTROL CULTURE	Sets the tone for an organisation, influencing the control consciousness of its people. Control culture factors include the integrity, ethical values and competence of the entity's people: management's philosophy and operating style; the way management assigns authority and responsibility, and organises and develops its people; and the attention and direction provided by a Board.	The BCI
CONTROL ENVIRONMENT	The entire system of controls, financial and otherwise, established by a Board and management in order to carry on an organisation's business in an effective and efficient manner, in line with the organisation's established objectives and goals. Also exists to ensure compliance with laws and regulations, to safeguard an organisation's assets and to ensure the reliability of management and financial information. Also referred to as Internal Control.	The BCI
CONTROL FRAMEWORK	A model or recognised system of control categories that covers all internal controls expected within an organisation	The BCI
CONTROL REVIEW / MONITORING	Involves selecting a control and establishing whether it has been working effectively and as described and expected during the period under review	The BCI
CONTROL SELF ASSESSMENT (CSA)	A class of techniques used in an audit or in place of an audit to assess risk and control strength and weaknesses against a control framework. The 'self' assessment refers to the involvement of management and staff in the assessment process, often facilitated by internal auditors. CSA techniques can include workshop/seminars, focus groups, structured interviews and survey questionnaires.	The BCI
CONTROLLED AREA	The area contained, if practicable, by the inner cordon	ENISA
CORDON	The boundary line of a zone that is determines, reinforced by legislative power and exclusively controlled by the emergency services from which all unauthorised persons are excluded for a period of time	The BCI
CORPORATE GOVERNANCE	The system/process by which the directors and officers of an	The BCI

Terminology	Explanation	Source
	organisation are required to carry out and discharge their legal, moral and regulatory accountabilities and responsibilities	
CORPORATE RISK	A category of Risk Management that looks at ensuring that an organisation meets its corporate governance responsibilities, takes appropriate actions and identifies and manages emerging risks	The BCI
COST BENEFIT ANALYSIS	A process (after a BIA and Risk Assessment) that facilitates the financial assessment of different strategic BCM options and balances the cost of each option against the perceived savings	The BCI
COUNTERMEASURE	An action taken to reduce risk. It may reduce the 'value' of the asset, the threats facing the asset or the vulnerability of that asset to those threats.	ENISA
CRISIS	A critical event, which, if not handled in an appropriate manner, may dramatically impact an organisation's profitability, reputation, or ability to operate. Or, an occurrence and/or perception that threatens the operations, staff, shareholder value, stakeholders, brand, reputation, trust and/or strategic/business goals of an organisation. See Event and Incident	The BCI and UK Financial Sector Continuity
CRISIS MANAGEMENT	The method concerned with managing the entire range of impacts following a disaster, including elements such as adverse media coverage and loss of customer confidence	ENISA
CRISIS MANAGEMENT PLAN	A clearly defined and documented plan of action for use at the time of a crisis. Typically a plan will cover all the key personnel, resources, services and actions required to implement and manage the Crisis Management process.	ENISA
CRISIS MANAGEMENT TEAM (CMT)	A management team who direct the recovery operations whilst taking responsibility for the survival and the image of the enterprise	ENISA
CRISIS MANAGEMENT PLAN OR CRISIS PLAN	A plan of action designed to support the crisis management team when dealing with a specific emergency situation which might threaten the operations, staff, customers or reputation of an enterprise	ENISA
CRISIS MANAGER (CM)	The leader of the Crisis Management	ENISA

Terminology	Explanation	Source
	Team	
CRISIS SIMULATION	The process of testing an organisation's ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis	ENISA
CRISIS ROOM	See Command Centre	The BCI
CRITICAL DATA POINT	The point in time to which data must be restored in order to achieve recovery objectives	The BCI
CRITICAL INFRASTRUCTURE (CI)	Physical assets whose incapacity or destruction would have a debilitating impact on the economic or physical security of an organisation, community, nation, etc.	The Disaster Recovery Journal, modified by ENISA
CRITICAL RECORDS	Records or documents that, if damaged or destroyed, would cause considerable inconvenience and/or require replacement or recreation at considerable expense	ENISA
CRITICAL SERVICE	Any service which is essential to support the survival of the enterprise	ENISA
CRITICAL SUCCESS FACTORS (CSFs)	The certain factors that will be critical to the success of the organisation, in the sense that if the objectives associated with those factors are not achieved, the organisation will fail - perhaps catastrophically so. Identification of CSFs should help determine the strategic objectives of the organisation.	ENISA
CUSTOMER RELATIONSHIP MANAGEMENT CRM	All of the activities necessary to ensure that Business Continuity Managers have a true understanding of their customers' needs and that the customers also understand their responsibilities. Use of the term in an Business Continuity Management sense should not be confused with the specific CRM term which is generally focused on helping a business 'sell' more to its customers rather than deliver better services.	ENISA
DAMAGE ASSESSMENT	The method of assessing the financial/non-financial damage following a Business Continuity incident. It usually refers to the assessment of damage to physical assets e.g. vital records, buildings, sites, technology to determine what can be salvaged or restored and what must be replaced.	The BCI

Terminology	Explanation	Source
DATA AVAILABILITY	Data is accessible and services are operational.	ENISA
DATA BACKUP STRATEGIES	Data backup strategies will determine the technologies, media and offsite storage of the backups necessary to meet an organisations data recovery and restoration objectives.	The Disaster Recovery Journal, modified by ENISA
DATA BACKUPS	The copying of production files to media that can be stored both on and/or off-site and can be used to restore corrupted or lost data or to recover entire systems and databases in the event of a disaster	The Disaster Recovery Journal, modified by ENISA
DATA CENTRE RECOVERY	The component of Disaster Recovery which deals with the restoration of data centre services and computer processing capabilities at an alternate location and the migration back to the production site	The Disaster Recovery Journal, modified by ENISA
DATA CONFIDENTIALITY	The protection of communications or stored data against interception and reading by unauthorised persons	ENISA
DATA INTEGRITY	The confirmation that data which has been sent, received or stored is complete and unchanged	ENISA
DATA MIRRORING	A method whereby critical data is copied instantaneously to another location so that it is not lost in the event of a Business Continuity incident	The BCI
DATA PROTECTION	Statutory requirements to manage personal data in a manner that does not threaten or disadvantage the person to whom it refers	The BCI
DATA RECOVERY	The restoration of computer files from backup media to restore programs and production data to the state that existed at the time of the last safe backup	The Disaster Recovery Journal, modified by ENISA
DATABASE REPLICATION	The partial or full duplication of data from a source database to one or more destination databases	
DECISION POINT	The latest moment at which the decision to invoke emergency procedures has to be taken in order to ensure the continued viability of the enterprise	The BCI
DECLARATION (OF DISASTER)	A formal statement that a state of disaster exists	The Emergency Planning Society
DECLARATION FEE	A fee charged by a Commercial Hot Site Vendor for a customer invoked disaster declaration	ENISA
DELEGATION	A formal agreement whereby one organisation's functions will be carried	ENISA

Terminology	Explanation	Source
	out by another.	
DENIAL OF ACCESS	The inability of a organisation to access and/or occupy its normal working environment. Usually imposed and controlled by the Emergency and/or Statutory Services.	The BCI
DEPENDENCY	The reliance or interaction of one activity or process upon another	The BCI
DESKTOP EXERCISE	See: Table Top Exercise	ENISA
DISASTER	A sudden, unplanned catastrophic event causing unacceptable damage or loss	The Disaster Recovery Journal
DISASTER RECOVERY (DR)	Disaster Recovery refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency. The scope may overlap that of an IT Service Continuity Plan; however, the DR Plan is narrower in scope and does not address Business Impact Analysis. Also referred to as IT Disaster Recovery.	NIST SP 800-34, with some modification by ENISA
DISASTER RECOVERY COORDINATOR	A role of the Disaster Recovery programme that coordinates planning and implementation for overall technical recovery of a component	The Disaster Recovery Journal
DISASTER RECOVERY PLAN (DRP) OR RECOVERY PLAN	A plan to resume, or recover, a specific essential technical operation	ENISA
DISASTER RECOVERY PLANNING	The process of writing a Disaster Recovery Plan	ENISA
DISASTER RECOVERY SOFTWARE	An application program developed to assist an organisation in writing a comprehensive disaster recovery plan	ENISA
DISASTER RECOVERY TEAMS	A structured group of teams ready to take control of the recovery operations if a disaster should occur	The Disaster Recovery Journal
DISK MIRRORING	Disk mirroring is the duplication of data on separate disks in real time to ensure its continuous availability, currency and accuracy. Disk mirroring can function as a disaster recovery solution by performing the mirroring remotely. True mirroring will enable a zero recovery point objective. Depending on the technologies used, mirroring can be performed synchronously, asynchronously, semi-synchronously, or point-in-time.	The Disaster Recovery Journal, modified by ENISA
DISRUPTION	An event which interrupts the ability of an organisation to deliver its outputs	ENISA
DIVERSE ROUTING	The routing of information through	The Disaster

Terminology	Explanation	Source
	split or duplicated cable facilities	Recovery Journal, modified by ENISA
DOWNTIME	The total period that a service or component is not operational within an agreed service time. Measured from when a service or component fails to when normal operations recommence.	The Disaster Recovery Journal, modified by ENISA
DROP SHIP	A strategy for providing replacement hardware within a specified time period via prearranged contractual arrangements with an equipment supplier at the time of a Business Continuity event	The Disaster Recovery Journal, modified by ENISA
ELECTRONIC VAULTING	Electronic transmission of data to a server or storage facility.	ENISA
EMERGENCY	An actual or impending situation that may cause injury, loss of life, destruction of property or cause the interference, loss or disruption of an organisation's normal business operations to such an extent that it poses a threat	The BCI
EMERGENCY CHANGE	A change that is planned, scheduled and implemented at very short notice in order to protect a service from an unacceptable risk of failure or degradation, lack or loss of functionality	ENISA
EMERGENCY CONTROL/COMMAND CENTRE (ECC)	The location from which an incident is directed and tracked. It may also serve as a reporting point for deliveries, services, press and all external contacts. See Command Centre	ENISA
EMERGENCY CO-ORDINATOR	The person designated to plan, exercise, and implement the activities of sheltering in place or the evacuation of occupants of a site with the first responders and emergency services agencies	ENISA
EMERGENCY DATA SERVICES	Remote capture and storage of electronic data, such as journalling, electronic vaulting and database shadowing	The BCI
EMERGENCY MANAGEMENT PLAN	A plan which supports the emergency management team by providing them with information and guidelines	The Emergency Planning Society modified by ENISA
EMERGENCY MANAGEMENT TEAM	The group of staff who command the resources needed to recover the enterprises operations	The Emergency Planning Society, modified by ENISA
EMERGENCY OPERATIONS CENTER (EOC)	A site from which response teams/officials (municipal, county, state and federal) provide direction	The Emergency Planning Society, modified by ENISA

Terminology	Explanation	Source
	and exercise control in an emergency or disaster. See Emergency Control Centre, Crisis Centre, Crisis Room, Incident Room	
EMERGENCY PLANNING (EP)	Development and maintenance of agreed procedures to prevent, reduce, control, mitigate and take other actions in the event of an emergency	The Emergency Planning Society, modified by ENISA
EMERGENCY PREPAREDNESS	The capability that enables an organisation or community to respond to an emergency in a coordinated, timely, and effective manner to prevent the loss of life and minimize injury and property damage	The Emergency Planning Society, modified by ENISA
EMERGENCY PROCEDURES	A documented list of activities to commence immediately to prevent the loss of life and minimize injury and property damage	The Emergency Planning Society, modified by ENISA
EMERGENCY RESPONSE	The immediate reaction and response to an emergency situation commonly focusing on ensuring life safety and reducing the severity of the incident	The Emergency Planning Society, modified by ENISA
EMERGENCY RESPONSE PLAN	A documented plan usually addressing the immediate reaction and response to an emergency situation	The Emergency Planning Society, modified by ENISA
EMERGENCY RESPONSE PROCEDURES	The initial response to any event,focused upon protecting human life and the organisation's assets	The BCI
EMERGENCY RESPONSE TEAM (ERT)	Qualified and authorized personnel who have been trained to provide immediate assistance	The Emergency Planning Society modified by ENISA
EMERGENCY SERVICES	Usually refers to the civil services of Police, Fire and Ambulance	The BCI
ENTERPRISE	An organisation, a corporate entity; a firm, an establishment, a public or government body, department or agency; a business or a charity	The BCI
ENTERPRISE WIDE PLANNING	The overarching master plan covering all aspects of Business Continuity within the entire organisation	ENISA

Terminology	Explanation	Source
ESCALATION	Passing information and/or requesting action on an Incident, Problem or Change to more senior staff (hierarchical escalation) or other specialists (functional escalation) The circumstances in which either vertical escalation for information/authority to apply further resources or horizontal escalation for greater functional involvement need to be precisely described, so that the purpose of the escalation and the nature of the required response is absolutely clear to all parties as the escalation occurs. Escalation rules will be geared to priority targets. Functional Escalation is sometimes called Referral.	The BCI modified by ENISA
ESSENTIAL SERVICE	A service without which a building would be 'disabled'. Often applied to the utilities (water, gas, electricity, etc.) it may also include standby power systems, environmental control systems or communication networks.	The BCI
EVACUATION	The movement of employees, visitors and contractors from a site and/or building to a safe place (assembly area) in a controlled and monitored manner at time of an event	The BCI
EVENT	Any occurrence that may lead to a Business Continuity incident	ENISA
EXCLUSION ZONE	See Cordon	ENISA
EXCEPTION REPORTING	Reducing the Management Information produced to that which most demands or deserves attention. The Top Ten style of list is an example.	ENISA
EXECUTIVE / MANAGEMENT SUCCESSION PLAN	A predetermined plan for ensuring the continuity of authority, decision-making, and communication in the event that key members of executive management unexpectedly become incapacitated	ENISA
EXERCISE	A people-focused activity designed to execute Business Continuity Plans and evaluate the individual and/or organisation performance against approved standards or objectives. Exercises can be announced or unannounced, and are performed for the purpose of training and conditioning team members, and validating the Business Continuity Plan. Exercise results identify plan gaps and limitations and are used to	ENISA

Terminology	Explanation	Source
	improve and revise the Business Continuity Plans.	
EXERCISE AUDITOR	An appointed role that is assigned to assess whether the exercise aims/objectives are being met and to measure whether activities are occurring at the right time and involve the correct people to facilitate their achievement	The UK Financial Sector Continuity
EXERCISE CONTROLLER/FACILITATOR	The person who runs the exercise on the day in accordance with the Exercise Script	ENISA
EXERCISE CO-ORDINATOR	They are responsible for the mechanics of running the exercise.	ENISA
EXERCISE OBSERVER	An exercise observer has no active role within the exercise but is present for awareness and training purposes. An exercise observer might make recommendations for procedural improvements.	The BCI
EXERCISE OWNER	An appointed role that has total management oversight and control of the exercise and has the authority to alter the Exercise Plan.	ENISA
EXERCISE PLAN	A plan designed to evaluate tasks, teams, and procedures that are documented in Business Continuity Plans to ensure the plan's viability. This can include all or part of the BC plan, but should include mission critical components. See Test Plan	ENISA
EXERCISE SCRIPT	A time-line for running the exercise. It states what activities should be happening, when they should happen and who is carrying out the activity. See Test Script	ENISA
EXERCISE REPORT	A report which is written following an exercise to discuss the outcomes of the exercise and recommendations for amendments and further work. See Test Report	ENISA
EXPOSURE	The potential susceptibility to loss; the vulnerability to a particular risk	The BCI
EXTRA EXPENSE	The extra cost necessary to implement a recovery strategy and/or mitigate a loss. An example is the cost to transfer inventory to an alternate location to protect it from further damage, cost of reconfiguring lines, overtime costs, etc. Typically reviewed during BIA and is a consideration during insurance evaluation.	ENISA

Terminology	Explanation	Source
EXTREME OR CATASTROPHIC EMERGENCY, EVENT, INCIDENT AND/OR CRISIS	A Business Continuity incident of immense proportions that has severe consequences, often damaging a large proportion of the organisation's assets that results in a loss greater than an expected loss.	The BCI
FACILITIES MANAGEMENT (FM)	The function that manages all aspects of an organisation's real estate assets and infrastructure.	The BCI
FAILURE	A failure occurs when a functional unit is no longer fit for purpose.	The Disaster Recovery Journal modified by ENISA
FAILOVER	Failover is the capability to switch over automatically to a redundant or standby computer server, system, or network upon the failure or abnormal termination of the previously active server, system, or network. Failover happens without human intervention and generally without warning, unlike switchover.	The Disaster Recovery Journal modified by ENISA
FALLBACK	Another term for alternative e.g. a fallback facility is another site/building that can be use when the original site/building is unusable or unavailable.	The BCI
FAMILY ASSISTANCE CENTRES	A one-stop-shop for survivors, families, friends and all those affected by the emergency, through which they can access support, care and advice.	ENISA
FAULT	A condition that causes a functional unit to fail to perform the required function.	The Disaster Recovery Journal modified by ENISA
FAULT TOLERANCE	The ability of a service to continue when a failure occurs. See Resilience	The Disaster Recovery Journal modified by ENISA
FILE SHADOWING	The asynchronous duplication of the production database on separate media to ensure data availability, currency and accuracy	The Disaster Recovery Journal modified by ENISA
FINANCIAL IMPACT	An operating expense that continues following an interruption or disaster, which as a result of the event cannot be offset by income and directly affects the financial position of the organisation	The UK Financial Sector Continuity
FIRE MARSHALL	A person responsible for ensuring that all employees, visitors and contractors evacuate a site/building	The BCI
FIRST LEVEL SUPPORT	The technical and managerial resources within the Service Desk available at the initial point of contact	ENISA

Terminology	Explanation	Source
	with the Customer/User	
FLOOR WARDEN	Person responsible for ensuring that all employees, visitors and contractors evacuate a floor within a specific site	ENISA
FORTRESS APPROACH	An approach to Business Continuity where the entire site is made as disaster-proof as possible	ENISA
FORWARD RECOVERY	The process of recovering a database to the point of failure by applying active journal or log data to the current backup files of the database	The Disaster Recovery Journal modified by ENISA
FULL REHEARSAL	An exercise that simulates a Business Continuity event where the organisation or some of its component parts are suspended until the exercise is completed	The BCI
FULL RELEASE	A release that tests, distributes and implements all components of a release unit, regardless of whether or not they have changed since the last release of the software	The Disaster Recovery Journal modified by ENISA
FUNCTION	The actions or intended purpose of a person, team or thing in a specific role. Service Management functions may be considered as key business activities, often with a broad scope and associated with a particular job, consisting of a collection of lower level activities. The characteristics of a function are that it is continuous and represents a defining aspect of the business enterprise. It is usually associated with more than one method and contributes to the execution of those processes. Rarely do (or should) functions mirror the organisational structure.	ENISA
GAP ANALYSIS	A survey whose aim is to identify the differences between BCM/Crisis Management requirements (what the business says it needs at time of an incident) and what is in place and/or available	The BCI
GOLD TEAM	Strategic decision makers and groups at the local level. They establish the framework within which operational and tactical managers work in responding to and recovering from emergencies.	ENISA
HAND-CARRIED BOMB	Any type of portable bomb, usually contained in a form that would blend easily with the target surroundings, for example, suitcases, handbags, briefcases, video cassette boxes	NASP; National Association Of Security Professionals

Terminology	Explanation	Source
HARDENING	The process of making something more secure, resistant to attack, or less vulnerable	NASP; National Association Of Security Professionals
HAZARD	An accidental or naturally-occurring event or situation with the potential to cause physical (or psychological) harm to members of the community (including loss of life), damage or losses to property, and/or disruption to the environment or to structures (economic, social, political) upon which a community's way of life depends	ENISA
HAZARD OR THREAT IDENTIFICATION	The process of identifying situations or conditions that have the potential to cause injury to people, damage to property, or damage to the environment	ENISA
HEALTH AND SAFETY	The process by which the well-being of all employees, contractors, visitors and the public is safeguarded. All Business Continuity Plans and planning must be cognisant of Health and Safety statutory and regulatory requirements and legislation. Health and Safety considerations should be reviewed during the Risk assessment.	The BCI, modified by ENISA
HIGH AVAILABILITY	Systems or applications requiring a very high level of reliability and availability. High availability systems typically operate 24x7 and usually require built-in redundancy to minimize the risk of downtime due to hardware and/or telecommunication failures.	The Disaster Recovery Journal modified by ENISA
HIGH-RISK AREAS	Areas identified during the Risk Assessment that are highly susceptible to a disaster situation or might be the cause of a significant disaster.	ENISA
HOT SITE	An alternate facility that already has in place the computer, telecommunications, and environmental infrastructure required to recover critical business functions or information systems	The BCI modified by ENISA
HOT STANDBY	A term that is normally reserved for Technology Recovery. An alternate means of processing that minimises downtime so that no loss of processing occurs. Usually involves the use of a standby system or site that is permanently connected to	The BCI

Terminology	Explanation	Source
	business users and is often used to record transactions in tandem with the primary system.	
HOT STANDBY/START/SITE (internal, external or mobile)	An IT Service Continuity option - either provided from within the organisation or by a 3rd party, possibly in a fixed place or mobile, consisting of a computer room with full environmental and telecommunications facilities plus the necessary hardware and software to enable the site to take over processing from the normal infrastructure with minimal disruption to services. See Immediate Recovery and Intermediate Recovery	The BCI, modified by ENISA
HOUSEKEEPING	The method of maintaining procedures, systems, people and plans in a state of readiness	The BCI
HUMAN RESOURCES	The department of an organisation responsible for the recruitment, employment and welfare of staff. Can also be known as Personnel	ENISA
HUMAN THREATS	Possible disruptions in operations resulting from human actions (i.e. disgruntled employee, terrorism, blackmail, job actions, riots, etc.).	ENISA
ICT	The department responsible for managing IT components within an organisation	ENISA
IED	Improvised Explosive Device	NASP; National Association of Security Professionals
IMMEDIATE RECOVERY	Broadly speaking, this Business Continuity option provides for the immediate recovery of services in a contingency situation. The instant availability of services distinguishes this option from what may be referred to as 'Hot Stand-by/Start', which typically will permit services to be recovered within 2 to 24 hours depending on the criticality of the business method they support. Depending on that business criticality, 'immediate' recovery may then vary from zero to 24 hours. See: Gradual Recovery and Intermediate Recovery	ENISA
IMMEDIATE RECOVERY TEAM	The team with responsibility for implementing the Business Continuity Plan and formulating the organisations initial recovery strategy	ENISA
IMPACT	A measure of the effect that an	The Disaster

Terminology	Explanation	Source
	Incident, Problem or Change is having or might have on the business being provided with Business Continuity. Often equal to the extent to which agreed or expected levels of service may be distorted. Together with urgency, and perhaps technical security, it is the major means of assigning priority for dealing with Incidents, Problems or Changes.	Recovery Journal modified by ENISA
IMPACT ANALYSIS	The identification of critical business processes and the potential damage or loss that may be caused to the organisation resulting from a disruption to those processes, or perhaps from a proposed change. Business impact analysis identifies the form the loss or damage will take; how that degree of damage or loss is likely to escalate with time following an Incident; the minimum staffing, facilities and services needed to enable business processes to continue to operate at a minimum acceptable level; and the time within which they should be recovered. The time within which full recovery of the business processes is to be achieved is also identified.	ENISA
INCIDENT	Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service	ITIL
INCIDENT CATEGORISATION	A sub-division of Classification, which provides a means of identifying -- using a series of structured codes: firstly, what appears to have gone wrong with the IS Service (the symptoms); secondly why the failure occurred (cause); and thirdly the component likely to be at fault. The category codes are elements within the classification data string and are essential for fault analysis purposes.	ENISA
INCIDENT COMMAND SYSTEM (ICS)	Combination of facilities, equipment, personnel, procedures, and communications operating within a common organisational structure with responsibility for the command, control, and coordination of assigned resources to effectively direct and control the response and recovery to an incident	ENISA

Terminology	Explanation	Source
INCIDENT MANAGEMENT	The process by which an organisation responds to and controls an incident using emergency response procedures or plans	The BCI
INCIDENT MANAGEMENT PLAN	A clearly defined and documented plan of action for use during an incident	ENISA
INCIDENT MANAGER	Commands the local emergency operations centre (EOC) reporting up to senior management on the recovery progress. Has the authority to invoke the recovery plan. See Crisis Manager	ENISA
INCIDENT RESPONSE	The response of an organisation to an incident that may significantly impact the organisation, its people, or its ability to function productively. Concentrates on the safety of personnel	ENISA
INCIDENT ROOM	See: Command Centre	ENISA
INFORMATION SECURITY	Preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can be involved.	BS ISO/IEC 17799: 2005
INFORMATION TECHNOLOGY (IT)	Technology components (computer systems, networks, applications, telecommunications, technical support and service desk)	Pas 77
INFRASTRUCTURE	The underlying foundation, basic framework, or interconnecting structural elements that support an organisation	ENISA
INHERENT RISK	The possibility that some human activity or natural event will have an adverse affect on the asset(s) of an organisation and which cannot be managed or transferred away	The BCI modified by ENISA
INNER CORDON	Surrounds and protects the immediate scene of an incident	ENISA
INTEGRATED EXERCISE	An exercise conducted on multiple interrelated components of a Business Continuity Plan, typically under simulated operating conditions. Examples of interrelated components may include interdependent departments or interfaced systems.	UK Financial Sector Continuity

Terminology	Explanation	Source
INTERIM SITE	A temporary location used to continue performing business functions after vacating a recovery site and before the original or new home site can be occupied. Moving to an interim site may be necessary if ongoing stay at the recovery site is not feasible for the period of time needed or if the recovery site is located far from the normal business site that was impacted by the disaster. An interim site move is planned and scheduled in advance to minimize disruption of business processes; equal care must be given to transferring critical functions from the interim site back to the normal business site.	ENISA
INTERNAL HOTSITE	A fully equipped alternate processing site owned and operated by the organisation	ENISA
ISO 9000	Guidelines and assurances of method and procedure standards for quality assurance systems	ISO
IT Service Continuity Management (ITSCM)	The discipline which takes ITDR and aligns it with BC requirements to provide a resilient IT service which inherently supports BC by maintaining the RTO and reducing downtime. BS 25777.	The Disaster Recovery Journal modified by ENISA
ITDR	See Disaster Recovery	ENISA
ITIL	Information Technology Infrastructure Library	ITIL
INVOCATION	The act of declaring that an organisation's Business Continuity plan needs to be put into effect in order to continue delivery of key products or services	BS 25999-1
JOURNALLING	The process of logging changes or updates to a database since the last full backup	ENISA

Terminology	Explanation	Source
KEY PERFORMANCE INDICATOR	A measure (quantitative or qualitative) that enables the overall delivery of a service to be assessed by both business and IS representatives. KPIs should be few in number and focus on the service's potential contribution to business success. To be effective in improving business performance, they must be linked to a strategic plan which details how the business intends to accomplish its vision and mission. The metrics selected must address all aspects of performance results, describe the targeted performance in measurable terms and be deployed to the organisational level that has the authority, resources and knowledge to take the necessary action.	UK Financial Sector Continuity modified by ENISA
KEY BUSINESS ACTIVITY	The critical operational and/or business support functions that could not be interrupted or made unavailable for less than a mandated or predetermined time-frame without significantly jeopardizing the organisation. These tasks identified within a Business Continuity Plan as a priority action typically to be carried out within the first few minutes/hours of the plan invocation.	ENISA
KNOWLEDGE BASE	Data repository holding information on Incidents, Problems and Known Errors, enabling an organisation to match new Incidents against previous ones and thus to reuse established solutions and approaches	ENISA
LEAD TIME	The time it takes for a supplier - either equipment or service - to make that equipment or service available. Business continuity plans should try to minimise this by agreeing Service Levels (Service Level Agreement) with the supplier in advance of a Business Continuity incident rather than relying on the supplier's best efforts.	The BCI
LIKELIHOOD	The chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies or mathematical probabilities	BS 25999-1
LINE RE-ROUTING	A short-term change in the routing of telephone traffic, which can be	The BCI

Terminology	Explanation	Source
	planned and recurring, or a reaction to an outage situation	
LOGISTICS/ TRANSPORTATION TEAM	A team comprised of various members representing departments associated with supply acquisition and material transportation, responsible for ensuring the most effective acquisition and mobilization of hardware, supplies, and support materials. This team is also responsible for transporting and supporting staff.	The BCI
LOSS	Negative consequence	BS 25999-1
LOSS ADJUSTER	Designated position activated at the time of a Business Continuity event to assist in managing the financial implications of the event and should be involved as part of the management team where possible.	The BCI, modified by ENISA
LOSS REDUCTION	The technique of instituting mechanisms to lessen the exposure to a particular risk	ENISA
LOST TRANSACTION RECOVERY	Recovery of data (paper within the work area and/or system entries) destroyed or lost at the time of the disaster or interruption. Paper documents may need to be requested or re-acquired from original sources. Data for system entries may need to be recreated or re-entered	ENISA
LVBIED	Large Vehicle-Borne Improvised Explosive Device	NASP; National Association of Security Professionals
MAJOR INCIDENT	A UK Emergency Services definition. Any emergency that requires the implementation of special arrangements by one or more of the Emergency Services, National Health Service or a Local Authority. Many organisations will use this terminology internally for an incident which causes widespread operational disruption and is likely to involve the Emergency Services.	The BCI, modified by ENISA
MANAGEMENT SYSTEM	The framework of processes and procedures used to ensure that the organisation can fulfil all tasks required to achieve its objectives	ENISA
MANUAL PROCEDURES	An alternative process of working following a loss of IS systems. As working practices rely more and more on computerised activities, the ability of an organisation to fall back to	The BCI

Terminology	Explanation	Source
	manual alternatives lessens. However, temporary measures and methods of working can help mitigate the impact of a Business Continuity incident and give staff a feeling of doing something.	
MARSHALLING AREA	Area to which resources and personnel not immediately required at the scene or being held for further use can be directed to stand by	The BCI
MAXIMUM ACCEPTABLE OUTAGE (MAO)	The maximum period of time that critical business processes can operated before the loss of critical resources affects their operations. See MTPD, MBCO	HB 292-2006
MAXIMUM TOLERABLE PERIOD OF DISRUPTION (MTPD)	The time after which disruption will become critical to the organisation or cause irrevocable damage. See MAO, MTPD	The BCI
METRIC	Measurable element of a service, method or function. The real value of metrics is seen in their change over time. Reliance on a single metric is not advised, especially if it has the potential to affect User behaviour in an undesirable way.	ENISA
MINIMUM BUSINESS CONTINUITY OBJECTIVE (MBCO)	Minimum level of services and/or products which is acceptable to the organisation to achieve its business objectives during an incident, emergency or disaster. MBCO is set by the executive management of the organisation and can be influenced, dictated and/or changed by current regulatory requirements or industry practice. See MTPD, MAO	TR19: 2005
MIRRORED STANDBY SITE	A fully redundant facility with full, real-time information mirroring. Mirrored sites are identical to the primary site in all technical aspects.	The Disaster Recovery Journal modified by ENISA
MISSION-CRITICAL ACTIVITIES	The critical operational and/or business support activities (either provided internally or outsourced) required by the organisation to achieve its objective(s) i.e. services and/or products	The BCI
MISSION-CRITICAL APPLICATION	Applications that support business activities or processes that could not be interrupted or unavailable for 24 hours or less without significantly jeopardizing the organisation	The Disaster Recovery Journal modified by ENISA
MITIGATION	Limitation of any negative consequence of a particular event	ENISA
MOBILE RECOVERY	A mobilized resource purchased or	ENISA

Terminology	Explanation	Source
	contracted for the purpose of business recovery. The mobile recovery centre might include: computers, workstations, telephone, electrical power, etc.	
MOBILE STANDBY	A transportable operating environment, usually complete with accommodation and equipment, which can be transported and set up at a suitable site at short notice	The BCI
MOBILE STANDBY SITE	Self contained, transportable units which are custom fitted with specific telecommunications and IT equipment necessary to meet system requirements	ENISA
MOBILE STANDBY TRAILER	A transportable operating environment, often a large trailer, that can be configured to specific recovery needs such as office facilities, call centres, data centres, etc. This can be contracted to be delivered and set up at a suitable site at short notice.	ENISA
MOBILISATION	The activation of the recovery organisation in response to an emergency or disaster declaration.	The BCI, modified by ENISA
MOCK DISASTER	One method of exercising teams in which participants are challenged to determine the actions they would take in the event of a specific disaster scenario. Mock disasters usually involve all, or most, of the applicable teams. Under the guidance of exercise coordinators, the teams walk through the actions they would take per their plans, or simulate performance of these actions. Teams may be at a single exercise location, or at multiple locations, with communication between teams simulating actual disaster mode communications. A mock disaster will typically operate on a compressed time-frame representing many hours, or even days.	ENISA
N + 1	A fault tolerant strategy that includes multiple systems or components protected by one backup system or component	ENISA
NATURAL THREATS	Events caused by nature that have the potential to impact an organisation	ENISA
NETWORK OUTAGE	An interruption of voice, data, or IP network communications	ENISA

Terminology	Explanation	Source
OFF-SITE LOCATION	A site at a safe distance from the primary site where critical data (computerised or paper) and/ or equipment is stored from where it can be recovered and used at the time of a Business Continuity incident if original data, material or equipment is lost or unavailable	The BCI
OFF-SITE STORAGE	Any place physically located a significant distance away from the primary site, where duplicated and vital records (hard copy or electronic and/or equipment) may be stored for use during recovery	The BCI, modified by ENISA
OPERATIONAL EXERCISE	See Exercise	ENISA
OPERATIONAL IMPACT	An impact which is not quantifiable in financial terms but whose effects may be among the most severe in determining the survival of an organisation following a disaster	UK Financial Sector Continuity
OPERATIONAL IMPACT ANALYSIS	The risk that deficiencies in information systems or internal controls will result in unexpected loss. The risk is associated with human error, system failures and inadequate procedures and controls.	ENISA
OPERATIONAL RISK	The risk of loss resulting from inadequate or failed procedures and controls	ENISA
OPERATIONAL TEST	A test conducted on one or more components of a plan under actual operating conditions	ENISA
ORDERLY SHUTDOWN	The actions required to rapidly and gracefully suspend a business function and/or system during a disruptio	The Disaster Recovery Journal, modified by ENISA
ORGANISATION	A company, firm, association, group, enterprise, a corporate entity; a firm, an establishment, a public or government body, department or agency; a business or a charity or other legal entity or part thereof, whether incorporated or not, which has its own functions and administration	The BCI, with modifications from HB 292-2006

Terminology	Explanation	Source
OUTAGE	Period of time that a service, system, method or business function is expected to be unusable or inaccessible which has a high impact on the organisation, compromising the achievement of the organisation's business objectives. An outage is different to 'downtime' where method or system failures happen as a part of normal operations, and where the impact merely reduces the short-term effectiveness of processes	The BCI
OUTSOURCING	The transfer of business functions to an independent (internal and/or external) supplier	The BCI
PEER REVIEW	A review of a specific component of a plan by personnel (other than the owner or author) with appropriate technical or business knowledge for accuracy and completeness	
PERIOD OF TOLERANCE	The period of time in which a Business Continuity incident can escalate to a potential disaster without undue impact to the organisation	The BCI
PIPELINES SAFETY REGULATIONS 1996	UK Legislation on the management of pipeline safety, using an integrated, goal-setting, risk-based approach encompassing both onshore and offshore pipelines; includes the major accident prevention document, the arrangements for emergency plans and the transitional arrangements	The Health and Safety Executive (HSE)
PLAN ADMINISTRATOR	The individual responsible for documenting recovery activities and tracking recovery progress	ENISA
PLAN CURRENCY	Business Continuity Plans must be maintained (housekeeping) to an adequate state. Measures of how up-to-date BC and CMT plans are recorded. A good (recent) plan currency is vital if plans are to be reliable.	The BCI
PLAN MAINTENANCE	The management process of keeping an organisation’s Business Continuity Management plans up to date and effective. Maintenance procedures are a part of this process for the review and update of the BC plans on a defined schedule. Maintenance procedures are a part of this process.	The BCI, modified by ENISA
PLANNING ASSUMPTIONS	Descriptions of the types and scales of consequences for which organisations should be prepared to	ENISA

Terminology	Explanation	Source
	respond	
POST IMPLEMENTATION REVIEW	One or more reviews held after the implementation of a change to determine initially, if the change has been implemented successfully and subsequently, if the expected benefits have been obtained	ENISA
PRE-POSITIONAL RESOURCE	Material (i.e. equipment, forms and supplies) stored at an off-site location to be used in business resumption and recovery operations (associated terms: pre-positioned inventory)	The BCI
PREVENTATIVE MEASURES	Measures put in place to lessen the likelihood of a Business Continuity Incident	The BCI
PROBABILITY	Extent to which an event is likely to occur. See likelihood	ENISA
PRIORITY	Sequence in which an incident or problem needs to be resolved	ENISA
PRIORITISATION	The ordering of key business activities and their dependencies are established during the BIA and Strategic-planning phase. The Business Continuity Plans will be implemented in the order necessary at the time of the event.	ENISA
PROBABILITY	The measure of chance of occurrence expressed as a number	HB 292-2006
PROCESS	An organised set of tasks which uses resources to transform inputs to outputs	ENISA
PROCESS OWNER/MANAGER	An individual held accountable and responsible for the workings and improvement of one of the organisations defined processes	ENISA
PROGRAM	An organised list of instructions that, when executed, causes a computer to behave in a predetermined manner. Programs contain variables representing numeric data, text or graphical images and statements that instruct the computer what to do with variables.	ENISA
PROGRAMME	A portfolio of projects and other activities that are planned; initiated and managed in a co-ordinated way in order to achieve a set of defined business objectives	ENISA
PROJECT	A temporary organisation created for the purpose of delivering one or more business products according to a specified business case	ENISA
PROJECT MANAGEMENT	The techniques and tools used to describe, control and deliver a series	The BCI

Terminology	Explanation	Source
	of activities with given deliverables, time-frames and budgets	
PROTECTIVE SECURITY	The safeguarding of physical and personnel welfare or information	NASP; National Association of Security Professionals
QUALITATIVE ASSESSMENT	The process for evaluating a business function based on observations and does not involve measures or numbers. Instead, it uses descriptive categories such as customer service, regulatory requirements, etc to allow for refinement of the quantitative assessment. This is normally done during the BIA phase of planning.	The BCI, modified by ENISA
QUALITY ASSURANCE	Confirming the degree of excellence of a product or service, measured against its defined purpose. This might involve a number of techniques. For documentation it might involve inviting informed comment; for software, a method of formal testing, trialling or inviting public feedback on a beta version; for hardware, performance against specified test; for management process, comparison with a standard such as BSI5000.	ENISA
QUANTIFICATION	The objective measure of the seriousness of risk or impact, often measured in financial or regulatory terms	The BCI
QUANTITATIVE ASSESSMENT	A form of assessment that analyses the actual numbers and values involved. This type of methodology typically applies mathematical and statistical techniques and modelling.	The BCI
QUICK SHIP	See Drop Ship	ENISA
THE RADIATION (EMERGENCY PREPAREDNESS AND PUBLIC INFORMATION) REGULATIONS 2001 (REPPIR)	Implemented in the UK, the articles on intervention in cases of radiation (radiological) emergency in Council Directive 96/29/Euratom, also known as the BS596 Directive. The Directive lays down the basic safety standards for the protection of the health of workers and the general public against the dangers arising from ionising radiation. The REPPIR also partly implement the Public Information Directive by subsuming the Public Information for Radiation Emergencies Regulations 1992 (PIRER) on informing the general public about health protection	The Health and Safety Executive (HSE)

Terminology	Explanation	Source
	measures to be applied and steps to be taken in the event of an emergency.	
RDD	Radiological Dispersion Device. Commonly known as a "dirty bomb", designed to disperse radioactive material, with or without explosives.	NASP; National Association of Security Professionals
RECIPROCAL AGREEMENT	Agreement between two organisations (or two internal business groups) with similar equipment/environment that allows each one to recover at the others location	The Disaster Recovery Journal, modified by ENISA
RECOVERABLE LOSS	Financial losses due to an event that may be reclaimed in the future, e.g. through insurance or litigation. This is normally identified in the Risk Assessment or BIA.	The BCI
RECOVERY	Implementing the prioritised actions required to return the key business activities and support functions to operational stability following an interruption or disaster	ENISA
RECOVERY CENTRE	Location or area that a business unit relocates to in order to recover their key business activities	ENISA
RECOVERY EXERCISE	An announced or unannounced execution of Business Continuity Plans intended to implement existing plans and / or highlight the need for additional plan development	ENISA
RECOVERY MANAGEMENT TEAM	A team of people, assembled in an emergency, who are charged with recovering an aspect of the enterprise, or obtaining the resources required for the recovery	ENISA
RECOVERY PERIOD	The time period between a disaster and a return to normal functions, during which the disaster recovery plan is employed	ENISA
RECOVERY PLAN	A plan to resume a specific essential operation, function or process of an enterprise	ENISA
RECOVERY POINT OBJECTIVE (RPO)	The point in time to which systems and data must be recovered after an outage (e.g. end of previous day's processing). RPOs are often used as the basis for the development of backup strategies and as a determinant of amount of data that may need to be recreated after the systems of functions have been recovered.	HB 292-2006

Terminology	Explanation	Source
RECOVERY SERVICES AGREEMENT/CONTRACT	A contract with an external organisation guaranteeing the provision of specified equipment, facilities, or services, usually within a specified time period, in the event of a business interruption	ENISA
RECOVERY SITE	A designated site for the recovery of business unit, technology, or other operations, which are critical to the enterprise	ENISA
RECOVERY STRATEGY	A pre-defined, pre-tested, management-approved course of action to be deployed in response to a business disruption, interruption or disaster	ENISA
RECOVERY TEAM	A group of individuals given responsibility for the co-ordination and response to an emergency or for recovering a process or function in the event of a disaster	ENISA
RECOVERY TIME OBJECTIVE (RTO)	The period of time within which systems, applications, or functions must be recovered after an outage (e.g. one business day)	The BCI, modified by ENISA
RECOVERY TIMELINE	The sequence of recovery activities, or critical path, which must be followed to resume an acceptable level of operation following a business interruption. The time-line may range from minutes to weeks, depending upon the recovery requirements and methodology.	The BCI, modified by ENISA
RECOVERY WINDOW	The time-scale within which time sensitive function or business units must be restored, usually determined by means of a Business Impact Analysis.	ENISA
REDUNDANCY	Where a system has been designed to eliminate single points of failure	ENISA
RENDEZVOUS POINT	Point to which all vehicles and resources arriving at the outer cordon are directed	ENISA
RESIDUAL RISK	The level of uncontrolled risk remaining after all cost-effective actions have been taken to lessen the impact and probability of a specific risk or group of risks, subject to the organisations risk appetite	The BCI, modified by ENISA
RESILIENCE	The ability of an organisation to absorb the impact of a business interruption, and continue to provide a minimum acceptable level of service	The BCI
RESOLUTION	An action that will resolve an Incident, i.e. allow the users to carry	ENISA

Terminology	Explanation	Source
	out their business functions. This may be a temporary workaround.	
RESOURCE REQUIREMENTS	The minimum level of resources which are required by the critical processes to support the recovery activities. These could include personnel, premises, technology, equipment and materials. Where there is a difference between desired requirements and what can be supplied, it is identified in a Gap Analysis.	ENISA
RESPONSE	The reaction to an incident or emergency to assess the damage or impact and to ascertain the level of containment and control activity required	The BCI
RESTART	The procedure or procedures that return applications and data to a known start point. Application restart is dependent upon having an operable system.	The BCI
RESTORATION	Process of planning for and/or implementing procedures for the repair of hardware, relocation of the primary site and its contents, and returning to normal operations at the permanent operational location	ENISA
RESUMPTION	The process of planning for and/or implementing the restarting of defined business processes and operations following a disaster. This process commonly addresses the most critical business functions within BIA specified time-frames.	The BCI, modified by ENISA
RESIDUAL RISK	Risk remaining after Risk Treatment	ENISA
RESUMPTION	The phase of an incident which follows Business Continuity and restores the organisation's operations to normal functioning	ENISA
RISK	The chance of something happening that will have an impact upon objectives. It is measured in terms of impact and likelihood.	HB 292-2006, modified by ENISA
RISK ACCEPTANCE	An informed decision to accept the consequences of likely events based on risk criteria	ENISA
RISK ANALYSIS	Determination of the likelihood and impact of each risk occurring. Risk Analysis provides the basis for risk evaluation, risk treatment and risk acceptance	ENISA, modified by ENISA
RISK APPETITE	Willingness of an organisation to accept a defined level of risk	The BCI, modified by ENISA
RISK ASSESSMENT /	Process of identifying the risks to an	ENISA

Terminology	Explanation	Source
ANALYSIS (RA)	organisation, assessing the critical functions necessary for an organisation to continue business operations, defining the controls in place to reduce organisation exposure and evaluating the cost for such controls	
RISK AVOIDANCE	An informed decision not to become involved in a risk situation	The BCI
RISK CATEGORIES	Risks of similar types are grouped together under key headings, otherwise known as risk categories	The BCI, modified by ENISA
RISK CONTROLS	All methods of reducing the frequency and/or severity of losses including exposure avoidance, loss prevention, loss reduction, segregation of exposure units and non-insurance transfer of risk	ENISA
RISK ESTIMATION	Process used to assign values to the probability and impact of a risk occurring	ENISA
RISK EVALUATION	The process of determining the significance of risk	ISO/IEC Guide 73, modified by ENISA
RISK MANAGEMENT (RM)	Structured ongoing development and application of management culture, policy, procedures and practices to the tasks of identifying, analysing, evaluating and controlling the response to risk	BS 25999-1, modified by ENISA
RISK MITIGATION	Implementation of measures to deter specific threats to the continuity of business operations, and/or respond to any occurrence of such threats in a timely and appropriate manner	The BCI modified by ENISA
RISK PROFILE	The combined result of impact and probability	The BCI, modified by ENISA
RISK REDUCTION OR MITIGATION	The implementation of the preventative measures which Risk Assessment has identified	The BCI modified by ENISA
RISK REGISTER (ORGANISATIONAL)	Tool that captures and describes risks as they are identified and their profile, together with risk ownership, actions where required, date when the risk was raised, review dates, dates when actions were completed and the date the risk was closed	ENISA
RISK REGISTER (IT)	A Risk Register owned by ICT used to capture and describe IT related risks. Often the most critical will be escalated to the organisational Risk Register.	ENISA
RISK REGISTER (PROCESS)	A Risk Register owned by the business process used to capture and describe process related risks. Often	ENISA

Terminology	Explanation	Source
	the most critical will be escalated to the organisational Risk Register.	
RISK TRANSFER	A common technique used by Risk Managers to address or mitigate potential exposures of the organisation. A series of techniques describing the various means of addressing risk through insurance and similar products	The BCI modified by ENISA
RISK TREATMENT	A systematic process of deciding which risks can be eliminated or reduced by remedial action and which must be tolerated	ENISA
ROLL CALL	The process of verifying that all employees, visitors and contractors have been safely evacuated and accounted for following an evacuation of a building or site	The BCI
SALVAGE and RESTORATION	The act of performing a coordinated assessment to determine the appropriate actions to be performed on impacted assets. The assessment can be coordinated with insurance adjusters, facilities personnel, or other involved parties. Appropriate actions may include: disposal; replacement; reclamation; refurbishment; recovery, or receiving compensation for unrecoverable organisational assets.	ENISA
SCENARIO	A pre-defined set of Business Continuity events and conditions that describe, for planning purposes, an interruption, disruption, or loss related to some aspect(s) of an organisation's business operations to support conducting a BIA, developing a continuity strategy, and developing continuity and exercise plans.	The BCI
SCOPE	Generally, the extent to which a method or procedure applies. The scope of Configuration Management may not, for example, extend to Customer information (other than on an as informed basis) and the scope of a Change Management procedure may not apply to urgent changes. Also a key concept in outsourcing as it defines which activities are covered by the base contract and which are separately chargeable.	ENISA
SECOND LEVEL/LINE SUPPORT	Technical resources (sometimes based within the Service Desk) called upon by Incident and Problem	ENISA

Terminology	Explanation	Source
	Management to assist in the resolution of an Incident, restoration of service, identification of a Problem or Known Error, the provision of a work-around or the generation of a Change	
SECURITY	All aspects relating to defining, achieving and maintaining data confidentiality, integrity, availability, accountability, authenticity and reliability	ISO/IEC WD 15443-1
SECURITY REVIEW	A periodic review of policies, procedures, and operational practices maintained by an organisation to ensure that they are followed and effective	The BCI
SELF INSURANCE	The pre-planned assumption of risk in which a decision is made to bear loses that could result from a Business Continuity event rather than purchasing insurance to cover those potential losses	The BCI, modified by ENISA
SERVICE CATALOGUE	The creation of a Service Catalogue (according to the ITIL Framework) is used as a starting point for the implementation of the Service Level Management process. A Service Catalogue lists all of the services which IT provides to the business. This catalogue should list the services from a user's perspective.	ITIL
SERVICE LEVEL AGREEMENT (SLA)	A formal agreement between a service provider (whether internal or external) and their client (whether internal or external), which covers the nature, quality, availability, scope and response of the service provider. The SLA should cover day-to-day situations and disaster situations, as the need for the service may vary in a disaster.	The BCI
SERVICE LEVEL MANAGEMENT (SLM)	The process of defining, agreeing, documenting and managing the levels of any type of services provided by service providers whether internal or external that are required and cost justified	ENISA

Terminology	Explanation	Source
SERVICE MANAGER	A senior manager, normally reporting to the IS director, who has overall responsibility for ensuring services are delivered in accordance with agreed business requirements. The Service Manager is also responsible for negotiating requirements with senior business representatives. The Service Manager is responsible for the Service Management Team and is usually a member of the high level CAB. The Service Manager should have a major say in the allocation of resources between services.	ENISA
SERVICE RESUMPTION	Restoring services to their Business-As-Usual state. Invoking BC may result in a temporary location or reduced level of personnel. It may also result in some business activities which are suspended.	ENISA
SILVER TEAM	Tactical level of management introduced to provide overall management of the response.	ENISA
SIMULATION EXERCISE	One method of exercising teams in which participants perform some or all of the actions they would take in the event of plan activation. Simulation exercises, which may involve one or more teams, are performed under conditions that at least partially simulate disaster mode. They may or may not be performed at the designated alternate location and typically use only a partial recovery configuration.	ENISA
SINGLE POINT OF FAILURE (SPOF)	The only (single) source of a service, activity and/or method, i.e. there is no alternative, whose failure would lead to the total failure of a key business activity and/or dependency	The BCI
SITE ACCESS DENIAL	Any disturbance or activity within the area surrounding the site which renders the site unavailable, e.g. fire, flood, riot, strike, loss of services, forensics. The site itself may be undamaged.	ENISA
SOCIAL IMPACT	Any incident or happening that affects the well-being of a population and which is often not financially quantifiable	UK Financial Sector Continuity
STAKEHOLDERS	All those who have an interest in an organisation, it's activities and it's achievements	BS 25999-1
STAND DOWN	Formal notification that the response	The BCI

Terminology	Explanation	Source
	to a Business Continuity event is no longer required or has been concluded	
STANDALONE TEST	A test conducted on a specific component of a plan in isolation from other components to validate component functionality, typically under simulated operating conditions	ENISA
STANDBY SERVICE	The provision of the relevant recovery facilities, such as cold-site, warm-site, hot-site and mobile standby	The BCI
STATUTORY SERVICES	Those services whose responsibilities are laid down by law e.g. Fire and Rescue Service, Coast Guard Service	The BCI
STRUCTURED WALKTHROUGH	Types of exercise in which team members physically implement the Business Continuity Plans and verbally review each step to assess its effectiveness, identify enhancements, constraints and deficiencies	The BCI
SUPPLY CHAIN	All suppliers, manufacturing facilities, distribution centres, warehouses, customers, raw materials, work-in-process inventory, finished goods, and all related information and resources involved in meeting customer and organisational requirements	ENISA
SWITCHOVER	Switchover is the capability to manually switch over from one system to a redundant or standby computer server, system, or network upon the failure or abnormal termination of the previously active server, system, or network. Switchover happens with human intervention, unlike Failover.	ENISA
SYNDICATION RATIO	The number of times that Work Area Recovery Facility seats are sold by the third party providers. Occupation at the time of an incident is on a first-comefirst-served basis.	The BCI, modified by ENISA
SYSTEM	Set of related technology components that work together to support a business process or provide a service.	The Disaster Recovery Journal, modified by ENISA
SYSTEM DENIAL	A failure of the computer system for a protracted period, which may impact an organisation's ability to sustain its normal business activities	The BCI
SYSTEM RECOVERY	The procedures for rebuilding a computer system and network to the condition where it is ready to accept data and applications, and facilitate network communications	The BCI, modified by ENISA
SYSTEM RESTORE	The procedures necessary to return a	The BCI, modified by

Terminology	Explanation	Source
	system to an operable state using all available data including data captured by alternate means during the outage	ENISA
TABLE TOP EXERCISE	One method of exercising plans in which participants review and discuss the actions they would take without actually performing the actions. Representatives of a single team, or multiple teams, may participate in the exercise typically under the guidance of exercise facilitators.	The BCI modified by ENISA
TASK	Generically, an activity or set of activities that might be defined as part of a process. When used within a phrase such as 'Standard Operational Task' it defines a well documented, controlled, proceduralised and, usually, low-risk activity. The procedure controlling the manner in which the task is carried out would be subject to formal Change Control.	ENISA
TASK LIST	Defined mandatory and discretionary tasks allocated to teams and/or individual roles within a Business Continuity Plan	The BCI
TERMS OF REFERENCE	A document that usually describes the purpose and scope of an activity or requirement	ENISA
TEST	A pass/fail evaluation of infrastructure (example-computers, cabling, devices, hardware) and\or physical plant infrastructure (example-building systems, generators, utilities) to demonstrate the anticipated operation of the components and system. A test can also be used to demonstrate whether all or parts of the Business Continuity Plan are fit for purpose. See Exercise	The BCI modified by ENISA
TEST AUDITOR	An appointed role that is assigned to assess whether the exercise aims/objectives are being met and to measure whether activities are occurring at the right time and involve the correct people to facilitate their achievement. See Exercise Auditor	ENISA
TEST CONTROLLER/FACILITATOR	The person who runs the test on the day in accordance with the Test Script. See Exercise Controller	ENISA
TEST PLAN	A document which states the scope and objectives of the test, and the roles, responsibilities and criteria for success. See Exercise Plan	ENISA

Terminology	Explanation	Source
TEST CO-ORDINATOR	The Test Co-ordinator is responsible for the mechanics of running the exercise. See Exercise Co-ordinator	ENISA
TEST OBSERVER	An exercise observer has no active role within the exercise but is present for awareness and training purposes. An exercise observer might make recommendations for procedural improvements. See Exercise Observer	ENISA
TEST OWNER	An appointed role that has total management oversight and control of the exercise and has the authority to alter the Exercise Plan. See Exercise Owner	ENISA
TEST REPORT	A report which is written following a test, to discuss the outcomes of the test and recommendations for amendments and further work. See Exercise Report	ENISA
TEST SCRIPT	A time-line for running the test. It details what activities should be occurring, the exact details of the activities, when they should occur and who is carrying out the activity. It will also state the criteria for success for each step. See Exercise Script	ENISA
THREAT	A combination of the risk, the consequence of that risk, and the likelihood that the negative event will take place.	ENISA
THREE-TIERED APPROACH	Strategic, Tactical and Operational incident management tiers. Also referred to as Gold, Silver and Bronze	ENISA
TOLERANCE THRESHOLD	The maximum period of time for which the business can afford to be without a critical function or process	The BCI
TOP MANAGEMENT	Person/s who direct and control and organisation.	BS 25999-1
TRAUMA COUNSELLING	The provisioning of counselling assistance by trained individuals to employees, customers and others who have suffered mental or physical injury as the result of an event	The BCI, modified by ENISA
TRAUMA MANAGEMENT	The process of helping employees deal with trauma in a systematic way following an event by proving trained counsellors, support systems, and coping strategies with the objective of restoring employees psychological well-being	The BCI modified by ENISA
UNEXPECTED LOSS	The worst-case financial loss or impact that a business could incur due to a particular loss event or risk.	The BCI, modified by ENISA

Terminology	Explanation	Source
	The unexpected loss is calculated as the expected loss plus the potential adverse volatility in this value.	
UNINTERRUPTIBLE POWER SUPPLY (UPS)	A backup electrical power supply that provides continuous power to critical equipment in the event that commercial power is lost. The UPS (usually a bank of batteries) offers short-term protection against power surges and outages. The UPS usually only allows enough time for vital systems to be correctly powered down.	The BCI, modified by ENISA
VALIDATION SCRIPT	A set of procedures within the Business Continuity Plan to validate the proper function of a system or process before returning it to production operation	ENISA
VBIED	Vehicle-Borne Improvised Explosive Device. A car or van filled with explosive, driven to a target and detonated.	NASP; National Association of Security Professionals
VENDOR	An individual or company providing a service to a department or the organisation as a whole	ENISA
VIRUS	An unauthorised programme that inserts itself into a computer system and then propagates itself to other computers via networks or disks	The BCI, modified by ENISA
VITAL RECORDS	Records essential to the continued functioning or reconstitution of an organisation during and after an emergency and also those records essential to protecting the legal and financial rights of that organisation and of the individuals directly affected by its activities	ENISA
VOIED	Victim Operated Improvised Explosive Device or booby-trap bomb.	NASP; National Association of Security Professionals
VOLUNTARY SECTOR	Organisational bodies, other than public authorities or local authorities, that carry out activities other than for profit	ENISA
VULNERABILITY	The existence of a weakness, or design or implementation error that can lead to an unexpected undesirable event, compromising the security of the computer system, network, application, or protocol involved.	ITSEC

Terminology	Explanation	Source
WARM (STANDBY) SITE	Partially equipped office space which contains some or all of the system hardware, software, telecommunications and power sources. The site may need to be prepared before receiving the system and recovery personnel. See Work Area Recovery Facility	ENISA
WORK AREA RECOVERY FACILITY (WARF)	An alternate processing site which is equipped with some hardware and communications interfaces, and electrical and environmental conditioning which is only capable of providing backup after additional provisioning of software or customisation is performed	The BCI modified by ENISA
WMD	Weapons of Mass Destruction. WMD encompasses nuclear, biological and chemical weapons.	NASP; National Association of Security Professionals
WORK AREA STANDBY	A permanent or transportable office environment, complete with appropriate office infrastructure	ENISA
WORK AROUND	A process of avoiding an incident or problem, either by employing a temporary fix or technique that means a Customer is not reliant on a CI that is known to cause failure	ENISA
WORKAROUND PROCEDURES	Alternative procedures that may be used by a functional unit(s) to enable it to continue to perform its critical functions during temporary unavailability of specific application systems, electronic or hard copy data, voice or data communication systems, specialized equipment, office facilities, personnel, or external services.	ENISA
Z-CARDS	A patented format for publishing information, up to an A3-sized page can be folded down to credit card size. This size means it is convenient to carry and can be stored in pockets, handbags, etc.	ENISA