NHS Information Authority

Business Continuity Planning Manual

Version 1

Business Continuity Planning Manual

CONTENTS

BUSINESS CONTINUITY PLANNING

INTRODUCTION

Business Continuity Planning (BCP) can help NHS organisations to reduce the effects of disruption upon services, systems and business processes caused by service interruptions and failures. Whatever the cause, the consequences of such interruptions and failures should be analysed. Business Continuity Planning can reduce the effects of these to an acceptable level. This can be best achieved through the application of a combination of preventive and recovery controls.

Contingency and recovery plans for each of the organisation's core services, key systems and business processes should be developed, wherever possible forming an integral part of existing management processes. They should be regularly maintained and tested to enable implementation when circumstances dictate. Following any implementation they should be evaluated and reviewed.

The purpose of this document is to give clear guidance to enable all NHS organisations including strategic health authorities, special heath authorities, trusts and agencies to develop their own effective business continuity plans. It aims to provide a common basis and understanding for identifying key assets, assessing the risks and their impacts and following the development of those plans to test, implement and maintain them. A framework of management tasks for undertaking the necessary planning processes towards developing organisation-wide business continuity plans is set out in this document both in summary and detail.

Within the development of business continuity plans, it is vital that they contain both contingency and recovery components, defining the organisation's arrangements for achieving acceptable interim levels of service and for how full services will be resumed. Each NHS organisation needs to ensure that there are adequate and robust plans developed to meet differing contingencies and core service requirements. Plans should address acceptable and sustainable service levels, options for fallback, systems recovery and co-ordination arrangements covering three main business areas:

a) Service Continuity: Ensuring that at all times and in all circumstances, an organisation can continue to operate its core services to at least a minimum pre-determined level.

b) IM&T Continuity: Ensuring the continuity or recovery of an organisation's IM&T systems within required time-scales, following interruption to or failure of critical processes.

c) Major Incidents: These have a high impact on the services, systems and business processes of one or more NHS organisations and possibly other agencies as well. Such plans are the subject of separate detailed guidance issued by the Department of Health. They are included in summary form within this document because of similarities in the approach and the occasional difficulty in identifying the boundaries between them.

To be effective, all NHS organisations should take an integrated approach towards Business Continuity Planning, addressing all three business areas. Wherever possible this should draw on work already undertaken in these areas and capitalise upon existing continuity plans.

The development of such plans should be driven by senior management together with all relevant stakeholders and the approach agreed by the organisation's management board, with one board member being given overall responsibility for the process. Key responsibilities for managing and implementing developed business continuity plans should be assigned to appropriate senior managers. All potentially affected employees should be aware of their own roles and responsibilities and what actions they are expected to take in the event of interruptions to their business activities. To achieve this, organisations should provide adequate skills training and awareness.

Business Continuity Planning also presents the opportunity for NHS organisations to review their business approach, examine processes, improve procedures and practices and thereby improve the organisation's resilience to loss of, or interruption to their services and systems, as well as reducing the probability of any disruption. However, changes in risk profiles are likely to affect the vulnerability of each organisation and therefore plans should be tested, reviewed and updated at regular intervals, at least on an annual basis. Any change to business continuity plans should take place under formal change control procedures.

The guidance also addresses the Department of Health's Information Security Programme requirements for compliance by NHS organisations with the Business Continuity Planning content of the *BS 7799 Code of Practice for Information Security Management*. To do so, NHS organisations should first have used the *ISO/IEC 17799 Toolkit* for successful and meaningful completion of the gap analysis process of the BS 7799 programme. That will support NHS organisations in addressing their existing and emerging information security needs, through the ongoing development and maintenance of the BS 7799 programme.

Many NHS organisations will be able to capitalise on the preparations and planning they undertook for Year 2000. The skills obtained and the knowledge gained from that exercise would come in very useful when developing business continuity plans. That is particularly so where the personnel who were engaged in that operation remain and where the documentation, principally the inventories, the risk register and the list of critical suppliers, can be updated and maintained.

NHS organisations do need to recognise that the drawing up of business continuity plans does require an investment of resources. Larger organisations, such as hospital trusts, may find it necessary to appoint a part-time or full-time co-ordinator to undertake preparatory tasks or to contract with external companies to undertake some or many of the tasks for them. That decision may depend upon the availability of appropriate and skilled resources and the ability to capitalise on previous planning activity. It should be recognised that as the scope of these tasks is organisation-wide, for larger organisations this may take up to two years to complete.

BACKGROUND

Business Continuity Planning forms an integral part of Corporate Governance for NHS organisations. Corporate Governance has been defined by the Audit Commission as "The systems and processes by which health bodies lead, direct and control their functions, in order to achieve their organisational objectives, and by which they relate to their partners and the wider community". To achieve their objectives, NHS organisations need to be capable of ensuring the continuity of their critical infrastructure, core services, systems and essential business processes.

Best practice in Corporate Governance has developed over the last decade. In the UK, the Committee on the Financial Aspects of Corporate Governance reviewed this in 1991 and as the development of governance structures has progressed, financial controls have expanded to encompass all the activities of enterprises. The most notable recent UK report *"Internal Control – Guidance for Directors on the Combined Code"* was published in 1999. This requires companies listed on the London Stock Exchange to maintain a 'sound system' of internal control by means of conducting a thorough and regular evaluation of the risks to which the company is exposed. It further requires them to, at least annually, conduct a review of the effectiveness of that system and report to shareholders that they have done so.

Having already introduced a Statement on Internal Financial Control in 1997, HM Treasury updated these requirements by adopting the principles of the Turnbull Report for all government departments including the Department of Health. In order for a Statement on Internal Control to be provided on behalf of the NHS, the Department of Health have put in place a mechanism whereby the boards of all NHS organisations would provide individual assurances. These would then be aggregated in order for a collective NHS-wide assurance to be given. As there were already Corporate Governance mechanisms in place it was considered that the Statement on Internal Control would not impose any significant additional burden on NHS organisations.

To underpin the Statement on Internal Control there are three core standards (Governance, Financial Management and Risk Management) that provide clarity around the fundamental principles surrounding what is expected of NHS organisations. These standards are supported by eighteen organisational control standards that bring together existing legislative and mandatory conformance requirements in order for NHS organisations to review the adequacy of their control systems. Within the Emergency Planning and Information Management and Technology organisational control standards 'Business Continuity Planning' is extremely important.

1. SCOPE, AIMS AND OBJECTIVES

1.1 Scope

The Scope of this guidance encompasses the development, maintenance, implementation, monitoring and review of organisation-wide business continuity plans for NHS organisations.

1.2 Aims

The aims of providing this guidance are to:

a) underpin the effective governance of NHS organisations;

b) provide the Management Boards of NHS organisations with a framework for undertaking the development of business continuity plans.

1.3 Objectives

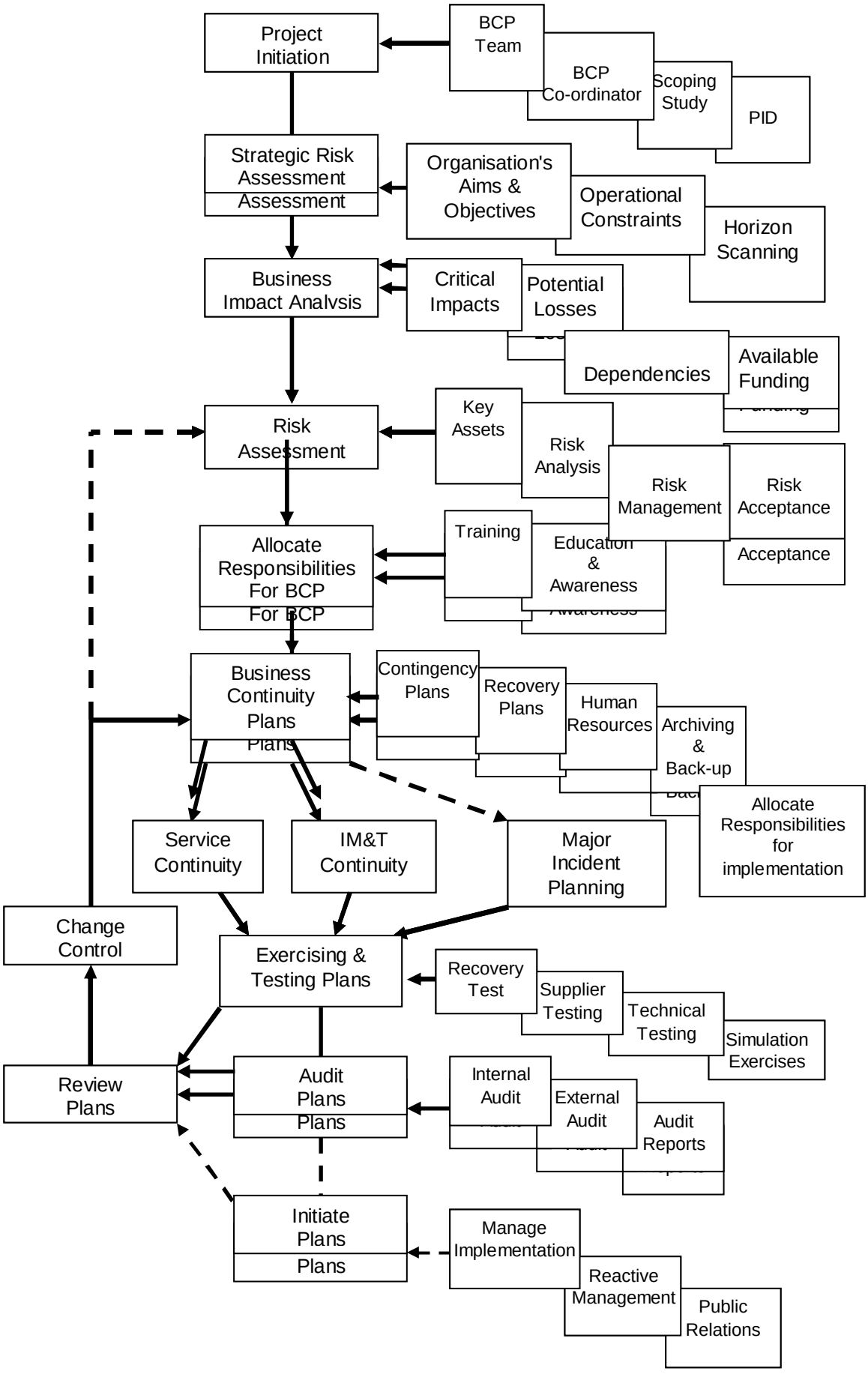
The key objectives of developing this Business Continuity Planning Guidance have been to:

a) provide NHS organisations with the method for counteracting interruptions to their services, systems and business processes;

b) assist NHS organisations to ensure the protection of their core services, systems and business processes from the effects of major failures or disasters;

c) assist NHS organisations to make an effective response to emergency situations or incidents.

BUSINESS CONTINUITY PLANNING FRAMEWORK



2. BUSINESS CONTINUITY PLANNING PROCESS

NHS organisations should have full management board support and be adequately resourced for undertaking the development and maintenance of business continuity plans. That work should take the form of a managed process throughout the organisation and is achieved by undertaking a series of structured management tasks:

2.1 Developing Business Continuity Plans

Action	Management Task
Project Initiation	The purpose of Project Initiation is to ensure that the business case, plans and budgets for the project are agreed and that there is a robust project infrastructure in place to manage it, all documented in a Project Initiation Document (PID).
Strategic Risk Assessment	Involves matching the organisation's primary aims and objectives with current operational performance and future constraints, to identify the services that are most at risk and which should be considered first.
Business Impact Analysis	Analysing critical services and supporting functions to determine the effect that interruption or disruption may have upon them.
Risk Assessment	Gaining knowledge of the risks affecting the continuing provision of services, systems and business processes and allocating priorities to them. This is done so that measures against those risks can be taken where they will be most effective. Business Continuity Planning will be necessary for risks that are considered acceptable.
Allocation of Responsibilities	Responsibilities should be allocated both to those developing the Business Continuity Plans and those personnel who will test and implement them. Key personnel need to have confidence in their ability to manage after an incident and in their competence in using contingency and recovery plans.
Business Continuity Plans	Business continuity plans, including Contingency and Recovery Plans should be developed to maintain or restore operational services, systems, business processes and supporting infrastructure within defined time scales, following interruption to, or failure of, core services, systems and critical business processes
Service Continuity Planning	Planning for the management of risks to ensure that at all times and in all circumstances an organisation can continue to operate their operational services to, at least, a minimum pre-determined level.
IM&T Continuity Planning	Planning to ensure an organisation can continue to operate its IM&T systems, or restore IM&T operations within required time-scales, following interruption to or failure of, critical processes.
Major Incident Planning	Planning for effective response to emergency situations or incidents, which may be serial, multiple, or single, often effecting a large area, more than one organisation and a broad range of agencies and services.
Exercising and Testing of Plans	Business Continuity Plans should be tested regularly to ensure that they are up to date and effective and that all relevant personnel are exercised in the operation of the plans.
Auditing of Plans	Auditing of Business Continuity Plans should be carried out on an annual basis to ensure that those plans remain current and viable and take account of any organisational changes.
Implementation	Business Continuity Plans should only be implemented when threats to services, systems and business processes materialise and an incident declared. Only in these circumstances would Business Continuity Plans normally be put into effect.
Review	Business Continuity Plans should be subject to regular review and update, to ensure their continuing effectiveness.
Change Control	Procedures to ensure that changes required as a result of the review process are reflected in business continuity plans.

These actions and associated management tasks are explained in fuller detail in the following sections (2.2 to 2.12).

2.2 Project Initiation

The purpose of Project Initiation is to ensure that the business case, for the work to be undertaken, has been accepted by the Organisation's Management Board and that project plans and budgets for the project are approved. As this represents a major investment of resources for any NHS organisation, there needs to be a robust project infrastructure in place to manage it. The task of developing, maintaining and reviewing Business Continuity Plans should be the responsibility of a dedicated Business Continuity Planning Team. The Business Continuity Planning process is organisation-wide and an essential component of every NHS organisation's risk management strategy. Indeed the Department of Health recently stated that "boards can only properly fulfil their responsibilities if they have a sound understanding of the principal risks facing the organisation."

Therefore, the Business Continuity Planning Team should operate under the authority of the organisation's board, executive or senior management team. It should be composed of senior managers in the organisation with direct responsibility for operational services and resources, which fall within the scope of the business continuity plans. Because of the dependency on buildings and services, and on supplies of equipment, goods and services, consideration should be given to including senior managers from Estates and Supplies functions as team members.

In recognition of its contribution towards effective risk management within the organisation, the Business Continuity Planning Team should be linked to other relevant existing groups or committees within the organisation, including both Clinical Governance and Risk Management committees. An exemplar organisational structure is shown at the end of this section.

Development of Business Continuity Plans should take the form of a properly constituted project with allocated time-scales and budget. A recognised project management methodology such as PRINCE or PRINCE2 should be used to ensure the organisation's ability to deliver the Business Continuity Plans to budget and specification.

The Business Continuity Planning Team should appoint a co-ordinator to undertake the development of the Business Continuity Plans in conjunction with directorates, departments and business functions and to be responsible for their ongoing maintenance and testing. The co-ordinator, while working for and within the Business Continuity Planning Team, will manage the development of the contingency and recovery plans. There should be access to up-to-date guidance relevant to the different aspects of Business Continuity Planning.

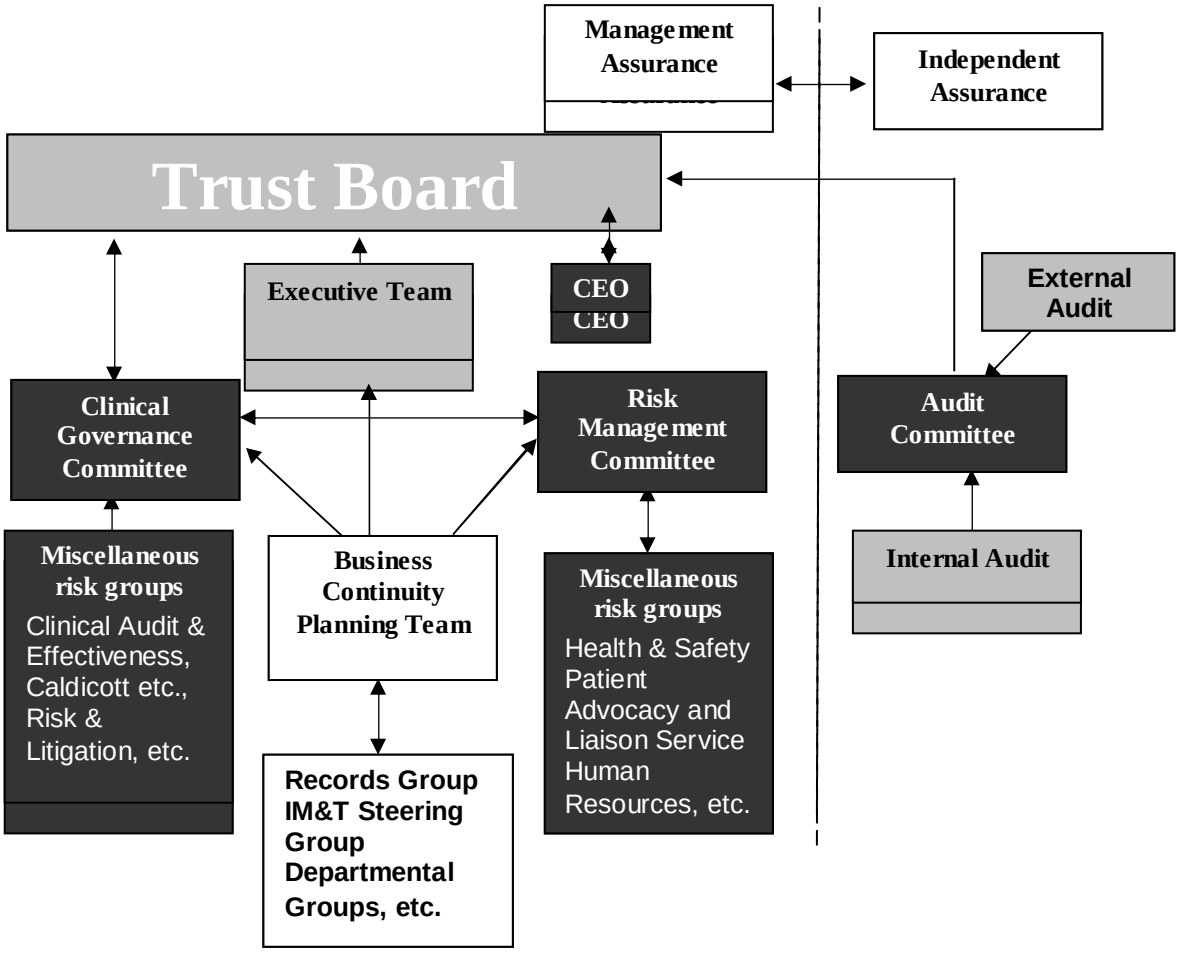
He/she will recruit contingency and recovery teams as necessary and supervise their work, as well as liase with other existing groups within the organisation as necessary. These will probably include the records group, IM&T Steering Group and departmental groups. Each plan should then be developed in a way which is consistent with the Business Continuity Planning framework.

Project Initiation should include a scoping study to estimate the effort and time required to arrive at fully comprehensive business continuity plans and to allocate adequate resources for its completion. It is important that these resources are made available, as sketchy plans can be worse than none at all, due to the false sense of security that this generates.

A Project Initiation Document (PID) should be produced, prior to work commencing as a basis for managing the project and assessing the outcomes. The PID should enable the Business Continuity Planning Team to ensure that the project has a sound basis before asking the organisation's management board to make any major commitment to commencing the work of the development project. The PID would also act as a base document against which the Team Co-ordinator can assess progress, change management issues and on-going viability.

As new systems are developed or changed and as services are introduced or amended, consideration should be given to the effect on the Business Continuity Plan. The Plan should be adapted as necessary to ensure that essential services will still be maintained following any incident. New projects should therefore include Business Continuity Planning within their own project plan.

Exemplar Organisational Structure



2.3 Strategic Risk

Prior to undertaking the task of developing business continuity plans each organisation should first take a more strategic top down approach by questioning the realism of the organisation's vision, aims and objectives. That involves matching the organisation's vision and strategic objectives with current and future operational constraints. It is necessary to do so because the strategy is the means by which the organisation sets out to achieve its vision, aims and objectives. That strategy in turn needs to reflect and be reflected by the organisation's operational activities. Often these are subject to constraints and influences and any commissioning of new, expanded or enhanced operational activities may involve complex or difficult inter-relationships. The result of the whole is a multi-dimensional problem, the extent of which is sometimes difficult to comprehend.

There are three broad categories of risk to be considered:

a) risks to the organisation, particularly the risk of failure in achieving its aims and objectives;
b) risks to individuals, including patients, stakeholders and the public;
c) risks arising from non-compliance with policy, standards, codes of practice, regulations and legislation.

Strategic risk assessment should address all three as any of these areas of risk can prevent an organisation from achieving its aims and objectives.

The task of assessing strategic risk should be similarly carried out under the authority of the organisation's board, executive or senior management team. The person best suited to owning the strategic risk process is the representative of the organisation's board, executive or senior management team appointed to oversee the work of the business continuity team and the development of business continuity plans. This ensures that the task of assessing strategic risk furnishes the organisation with an ongoing process for managing its business as a whole.

The strategic risk process involves considering the risk management implications of each of the organisation's operational activities and their inter-relationships with each other. It is not an overwhelming process, but some organisations may require specialist help to get it started. The overall effects are complementary to Business Continuity Planning, because the process considers likelihood and impact.

Non-Executive directors can play an important part in helping to identify strategic risk and provide an independent perspective on the level of risk faced and the adequacy of existing or proposed measures to address that risk.

Assessing strategic risk, including horizon scanning, can bring about an improvement in the long-term prospects for an effective business strategy and can also form the basis for the effective development of Business Continuity Planning. This is because the business needs of each of the organisation's operational activities and its inter-relationships are considered, together with the people responsible for managing and providing them. Examining business objectives and strategy can define the criticality of various business operations, which in turn may significantly influence infrastructure requirements.

Horizon scanning involves the systematic examination of potential threats, opportunities and likely future developments, which are at the margins of current thinking and planning. The principal aim of Horizon Scanning is to provide advanced notice of new and emerging health technologies or new applications of existing ones, particularly if there are significant economic implications associated with their introduction. This involves obtaining information from a variety of sources, including published material, contact with researchers/experts, pharmaceutical companies/manufacturers and liasing with similar overseas/foreign agencies. These interventions are then evaluated from a clinical and economic viewpoint in an attempt to estimate their potential impact on the healthcare system.

2.4 Business Impact Analysis

Business Impact Analysis (BIA) is the technique that involves senior management in determining more precisely what the risks are arising from any disruption to an organisation's critical services, identified through the strategic risk process, together with their associated systems and business processes. This is a very important step in the analysis phase, as risk assessments cannot provide all of the information needed for contingency or recovery planning, except for IM&T where this can be achieved by using the *NHS ISO/IEC 17799 Toolkit.*

2.5 Risk Assessment

The purpose of risk assessment is to establish a priority of risks so that the most serious can be addressed first. For IM&T this will be best achieved by using the *NHS ISO/IEC 17799 Toolkit* and by taking into account risks assessed and prioritised by risk management groups. The risks so identified need to be managed to reduce them to an acceptable level.

The management of risk can employ risk avoidance (using an alternative operation that bypasses the risk altogether), risk reduction (such as installing measures that reduce vulnerability) or risk transfer (so that the risk is borne by some other body; insurance is a case in point). However, some risks classed as acceptable will remain and Business Continuity Planning will be necessary to ensure that when threats materialise, actions can be taken to ensure that the essential services, systems and business processes continue to function. Risk assessment should include the following steps:

Action	Management Task
Key Assets Identification	To identify and list all those key assets associated with the business area(s) selected for review. (This should have been undertaken for IM&T assets as part of the *ISO/IEC 17799 GAP Analysis*). Each key asset should be assigned a value using the assigned value scale.
Threat assessment	To identify all those threats associated with the key assets and assign a value to them using the assigned value scale according to the probability of the occurrence of those threats.
Vulnerability assessment	To assess all the vulnerabilities associated with the key assets and assign a value to them, using the assigned value scale, according to how easily they might be exploited by the threats.
Impact analysis	To identify the impacts resulting from interruption, disruption, non-availability and disaster scenarios that can effect NHS organisations and to use techniques to quantify and qualify such impacts.
Risk Analysis	To determine the value of any risk according to the values ascribed to the threat, vulnerability and impact, using the assigned value scale. Also to establish the critical functions, the priorities for contingency and recovery and inter-dependencies in order that time-scales for contingency and recovery options can be set.
Identification and selection of security measures	For each of the key assets identify the control objectives that are relevant to each assessed risk.
Risk management	Applying the identified control measures so as to reduce the risk to an acceptable level.
Risk acceptance	Risks that are categorised as acceptable must then be addressed by the Business Continuity Plan.

The process of risk assessment is explained in greater detail in Chapter 4.

2.6 Allocate Responsibilities

Responsibilities should be allocated both for preparing the business continuity plans and for putting them into effect. In the first place responsibility will lie with the Business Continuity Planning Team and its Co-ordinator, who will work with the line managers in drawing up workable plans. The decision to implement the plan will be taken by the Business Continuity Planning Team and responsibility for implementation will lie with the Co-ordinator and relevant line managers. The same people should be involved with plan testing.

The successful development and where necessary, implementation of business continuity plans is dependent upon a continuity culture being embedded throughout the organisation. Personnel and others involved with the organisation need to have confidence in their ability to manage after an incident and their competence in using contingency and recovery plans. To achieve this there should be provision within the individual organisation's annual business plan for:

a) a programme of training in their roles and use of specialist facilities and equipment, for those directly involved in executing business continuity plans;

b) an education and awareness programme to ensure wider understanding and adoption of the plans;

c) participation in testing of the plans. Those who participate in developing and/or testing the plans will be better equipped to deal with an emergency if one arises.

Such an education and awareness training programme could be built into a wider programme of security awareness, applicable to all staff. It is important that all staff are aware of the need to undertake special work on the rare occasions when emergency conditions apply after an incident.

Awareness should extend to external stakeholders and third parties upon which the NHS organisation is dependent in both normal operating and reactive scenarios. Such programmes could be built into employee and supplier induction processes and contracts.

2.7 Business Continuity Plans

Business continuity plans should be developed to maintain or restore services, systems, business processes and supporting infrastructure within defined time scales following interruption to, or failure of, core services, systems and critical business processes. Those business continuity plans should take into account the following:

a) identification and agreement of all responsibilities and emergency procedures;

b) implementation of emergency procedures to facilitate contingency and recovery plans to operate effectively within required time-scales. (Particular attention needs to be given to the assessment of external business dependencies and the contracts in place);

c) documentation of agreed procedures and processes;

d) appropriate education of staff in the agreed emergency procedures and processes including reactive management (see 2.10);

e) testing and updating of the plans;

f) the planning process should focus on the required business objectives;

g) the planning process should also focus on the resources that are required to enable this to occur, including staff, as well as fallback arrangements for data and information processing facilities.

Business continuity plans need to be unambiguous and in sufficient detail to ensure there are no doubts in the minds of those people who have to put such plans into practice. It should be borne in mind that those implementing plans might be working under highly stressful conditions. As far as possible, their actions should be specified in detail and the decisions required should be few.

A single framework of business continuity plans should be maintained using a common format, to ensure that all plans are consistent and to identify priorities for testing and maintenance. Each plan should specify clearly the conditions under which it will be activated, as well as detail of the individuals responsible for executing each component of the plan. When new requirements are identified, established emergency procedures, e.g. evacuation plans or any existing fallback arrangements should be amended as appropriate. Where different approaches may be required for different services, business functions or parts of the organisation, it is recommended that supplementary sections are appended to each plan, as necessary, dealing with the specific requirements of each service or system.

Each plan should be the responsibility of a named individual, who has access to the appropriate business resources. It should spell out the responsibilities of the teams, describing which team member is responsible for executing which component of the plan; back-up nominees should also be identified. All contingency and recovery plans should be managed by the Co-ordinator and the Business Continuity Planning Team.

Emergency procedures, including arrangements for alternative services, technical support, manual fallback procedures and plans for the resumption of services, should be the responsibility of service managers.

A Business Continuity Planning framework should consider the following:

a) the 'triggers' which cause the plan to be implemented. These are the conditions to be met before each plan is activated;

b) the processes that need to be followed (how to assess the situation, how much interruption can be tolerated, who is to be involved, etc.);

c) emergency procedures, describing the actions to be taken following an incident which jeopardises human life and/or critical services;

d) existing major incident plans in NHS organisations, which should already include plans for preserving the continuity of essential emergency services, should be impacted on service and IM&T continuity planning development processes, to ensure comprehensive coverage and consistency.

e) the arrangements for any salvaging, submitting and verifying of any insurance claims and obtaining compensation for damage and increased cost of working;

f) the arrangements for informing patients and potential patients, managing public relations and effective liaison with appropriate public authorities, e.g. police, fire service and local government and for handling the media;

g) fallback procedures which describe the actions to be taken to move core services, essential business activities and their support services, to alternative temporary locations.

h) gaining access to any stand-by site, and invoking back-up arrangements to bring supporting business processes back into operation within the required time-scales;

i) incorporating those emergency arrangements and fall-back procedures, wherever possible, into the organisation's everyday working structures and processes;

j) arrangements for the staff and contractors during the contingency or recovery period such as office accommodation, transport, hotel accommodation as necessary;

k) keeping users informed as to the limited services available during a contingency and advising them if they need to rely on temporary equipment and other sources of information, such as using manual records;

l) resumption procedures which describe the actions to be taken to return to normal business operations;

m) maintenance schedules specifying how and when the plan will be tested and the process for maintaining the plan;

n) awareness and training activities designed to create understanding of the business continuity processes amongst staff that will have to put such plans into practice.

2.8 Testing Plans

Business continuity plans should be tested regularly to ensure that they remain relevant and workable. An untested plan can be worse than useless since it purports to provide assurance, but no one can tell if it will be effective when required. Testing should be carried out on at least an annual basis (preferably six monthly), when any significant change has occurred in the services, the systems in use, the environment in which they work or in the facilities to be used in a contingency.

Testing should also be done when there is a significant change in the plan itself. A variety of testing methods should be used. Such testing should be planned, and then carried out and the results recorded. Any shortfall or defects in the plans, highlighted by testing, should be corrected as soon as practicable and the changes also recorded. Testing is covered more fully in Chapter 12.

2.9 Auditing of Business Continuity Plans

Auditors, acting from an independent point of view, should carry out the annual auditing of Business Continuity Plans. That is to ensure that those plans remain current and viable and take account of any organisational changes. The main action points should be:

a) setting the scope of the audit and its objectives;

b) assessing and selecting the methods to be used;

c) developing a schedule of the audit activities;

d) auditing the administrative aspects of the contingency plans and recovery programme;

e) auditing the plan's structure, content and action sections;

f) auditing the plan's documentation and control procedures.

Both internal and external auditors should take the responsibility for auditing the Business Continuity Plans.

2.10 Implementing Business Continuity Plans

Reactive management will be invoked whenever there is an unscheduled interruption to the provision of core services, systems or business processes. At this time a decision will be taken whether to use Business Continuity Plans. An incident will arise whenever an unanticipated situation has occurred which causes an interruption to essential services, systems or business processes.

The following steps will be taken:

a) emergency action where necessary to ensure the safety of life;

b) assessing the impact of the occurrence;

c) highlighting the problem immediately to appropriate levels of management;

d) identifying the options for correction;

e) determining whether to invoke business continuity plans or any part of them or to take other actions. The decision will depend on how long the interruption is expected to continue;

f) ensuring that all actions taken are co-ordinated.

g) holding a review after the event to assess any residual problems.

Following resolution of any serious interruption to, or cessation of service the risks should be re-assessed to identify any new threats and vulnerabilities or any changes in known risks such as an increased probability of occurrence.

For handling any incident there is a need to identify components of a proactive public relations programme, to address some or all of the following:

a) preparing communication statements for all stakeholders;

b) advising affected members of external groups (patients, public, local community groups);

c) briefing relevant external agencies (suppliers. local authorities, companies, voluntary agencies);

d) preparing statements for the media (press, radio, and television).

It is recommended that a member of the Business Continuity Planning Team be given responsibility for handling all aspects of public relations. This will avoid conflicting messages being issued.

2.11 Maintaining and Reviewing Business Continuity Plans

Business continuity plans should be maintained by being subject to regular review and update, to ensure their continuing effectiveness. Responsibility should be assigned for regular reviews of each business continuity plan to an individual acting under the control of Business Continuity Planning Team and the Co-ordinator.

The identification of changes in business arrangements not yet reflected in the business continuity plans should be followed by an appropriate update of the plan. This formal change control process should then ensure that the updated plans are distributed and reinforced by regular reviews of the complete plan. Examples of situations that might necessitate updating plans include:

a) changes in business objectives or strategy;

b) service changes;

c) the acquisition of new systems or replacement or upgrading of operational systems;

d) the acquisition of new hardware for IM&T systems;

e) relocation of facilities and resources;

f) changes in key personnel or their roles;

g) response to changes in legislation or national guidance;

h) changes in contractors, suppliers or services;

i) changes in processes;

j) changes in risk;

k) changes in back-up and stand-by arrangements;

l) deficiencies found during testing.

2.12 Change Control

Any changes to the scope or detailed content of business continuity plans can, unless they are carefully controlled, impact on the total effectiveness of those plans. Procedures should be included within the organisation's change management programme to ensure that business continuity matters are appropriately addressed. Responsibility should be assigned for the identification of changes in business arrangements not yet reflected in each plan and the assessment of how the plan should be amended to accommodate them.

That assessment should be undertaken before any management decision is taken and any changes are made to the plans. A formal change control process therefore needs to be in place to assess the likely effect of any such changes, their significance for all plans, with time schedules and their likely impact on resource requirements. The plans should then be changed and the updated plans distributed, with appropriate training, where necessary.

There should be multiple, controlled copies of the business continuity plans, held in widely separate locations. At least one should be kept at the remote back-up and stand-by locations. This will ensure that, in the event of a widespread disaster, at least some copies can be found.

All updates should be logged in a central register. It is important to keep all copies updated to the same level. This will be the responsibility of the holders of individual copies, who will be advised by the co-ordinator of the changes to be entered. All changes should be recorded and the version number of the plan logged on each copy.

3. BUSINESS IMPACT ANALYSIS

3.1 Introduction

Examining Strategic Risk should have defined the criticality of various business operations for the organisation and identified their critical functions, systems and business processes. Undertaking risk assessment can provide knowledge of the threats and vulnerabilities (risks) affecting the continuing provision of such services and their associated systems and business processes and for determining measures against those risks, according to their priority and the value of assets.

Although risk assessments are a very important step in the analysis phase they cannot provide all of the information needed for recovery planning, except for IM&T where this can be achieved by using the *NHS ISO/IEC 17799 Toolkit*. Business Impact Analysis (BIA) therefore is the technique that needs to be used first. It involves senior management's input to understand more precisely what risks there are to the organisation from any disruption to the identified critical services and their associated systems and business processes.

While overall responsibility for developing appropriate contingency and recovery strategies lies with the organisation's management board, the information needed for effective planning needs to come from all levels of management throughout the organisation. Accurate data on all business functions is very important to this process, however information departments within NHS organisations are unlikely to be able to provide all the information that will be needed.

3.2 Business Impact Analysis Process

The BIA process involves dialogue with both managers and key staff. This approach helps to ensure that:

a) the "critical" and "unacceptable" impacts are identified;

b) the degree of potential loss (and various other unwanted effects) which could occur, is not just covering direct service loss, but other issues, such as financial loss, loss of reputation, regulatory effects, etc;

c) the single points of dependency that could initiate these impacts are defined;

d) available funding for Business Continuity Planning development is targeted where it is most needed.

This forms the main consideration in defining the direction, scope and appropriate strategies for developing contingency and recovery plans.

There are a number of advantages in taking the BIA route in that it can raise awareness of continuity issues amongst staff at all levels within the organisation. That can help with gaining consensus and support from all areas of the organisation, including from those who would not have understood the importance of organisation-wide contingency and recovery plan development, testing, and maintenance.

3.3 Business Impact Analysis Method

The methods used for BIA usually involve collecting information from managers and key staff on the likely effects of interruptions or disruption to services, their associated systems and business processes. This is usually achieved through structured interview, workshop, or questionnaires, or a combination of these. Where the interview or workshop approach is taken, often "what if" scenarios can be successfully employed as a basis for discussion.

The objective of taking any of these approaches is to assess both the quantitative and qualitative impact of disruptions on critical services by trying to determine:

a) the likely disruption to the continuity of service and operations;

b) the likelihood of violating appropriate legislation, regulations or standards;

c) the likely effects on key personnel both in practical terms and morale;

d) the effects of losing physical assets or information;

e) the financial effects of disruption (additional staff or buy-in costs, loss of assets, loss of revenue etc);

f) the environmental effects of such disruption;

g) what the public perception of these effects will be.

There is a need to determine:

a) the availability, status and relevance of any existing continuity plans;

b) the essential time frame for the recovery of critical business functions;

c) the essential time frame for the recovery of their support functions, applications and systems based on their level of criticality to those services;

d) the sequence in which they need to be recovered based on parallel activities with interdependencies;

e) minimum resource requirements for that recovery;

f) other information that needs to be collected includes legal and other regulatory requirements and considerations.

Once the Business Impact Analysis has been completed the next step for NHS organisations should be to undertake a full Risk Assessment, utilising the information gained from the Business Impact Analysis.

4. RISK ASSESSMENT

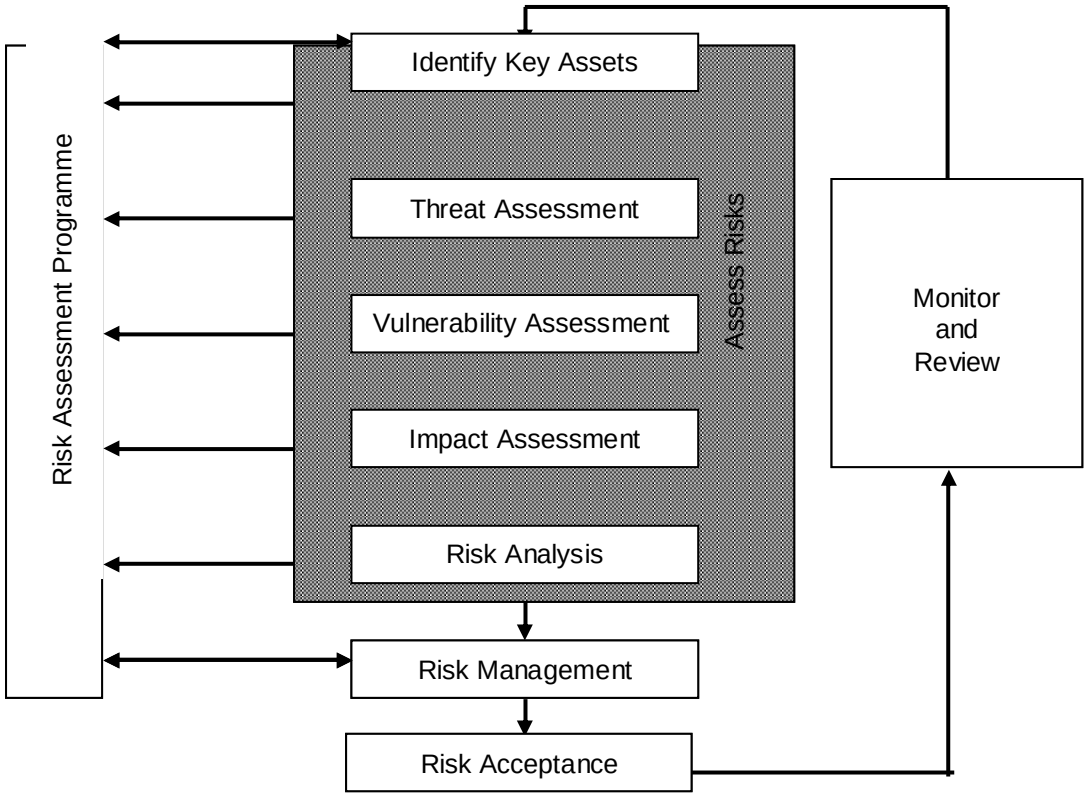
4.1 Introduction

A risk is the potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset or group of assets, and hence directly or indirectly to the organisation. Thus measures of risks are determined from the combination of anticipated impacts and assessed levels of related threats and associated vulnerabilities. Risk assessment will include the identification of 'principal risks' as defined by the Department of Health.

The objective is to identify and assess the risks to which an NHS organisation and its assets are exposed, in order to identify and select appropriate and justified security controls. This is an important stage in the development of Business Continuity Plans. Risk assessment should comprise all parts of the organisation that can be jeopardised by major incidents, business interruptions and failures. It should cover the whole organisation and not just be focused on one area, such as information processing facilities.

Risks are made up of the values of the partial or complete loss of the assets, the likelihood of threats occurring to cause impacts on the organisation's business and the ease of exploitation of the vulnerabilities by the identified threats. The application of controls to reduce those risks constitutes risk management.

The diagram below provides an overview of the Risk Assessment process documented in this section:



Risk Assessment Overview

4.2 Key Assets

The first stage in the Business Continuity Planning development process is identifying key assets. Assets are anything of value which is key to business processes within the business areas under review. These may include information or other resources and which may require to be protected by technical or non-technical countermeasures. They should be identified and recorded in an inventory, listed in the following categories:

Asset type	Examples of assets
Clinical assets	Medical devices
Physical assets	Buildings, property, equipment (power supplies, air-conditioning units), furniture, accommodation.
Information assets	Information itself, the means of holding and processing information, the confidentiality of the information held.
Communication assets	Telephones and faxes, postal services, internal communications.
Staff	All members of staff including voluntary staff and temporary or contract personnel.
Client assets	Patients and other people to whom the organisation is providing a service.
Service assets	Services provided from outside such as power, communications, water supplies and road access.

For IM&T systems, these should already have been identified and be contained within the Information Asset Register, compiled as part of the Security Improvement Programme with the *NHS ISO/IEC 17799 Toolkit (Gap Analysis)*. Some assets will include other assets; for example, a computer centre would include servers and communication devices. Information assets should be categorised into one of four groups:

Asset type	Examples of assets
Physical assets	Central application server, local file server, workstations, printers, local area networks (LAN), wide area networks (WAN), communications management equipment, tele-medicine equipment, magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), furniture, accommodation.
End user services	Updating administrative, clinical or patient care data, distributing patient or administrative records, electronic mail, electronic reporting, system interfaces, batch updates, downloading reference data.
Software assets	Application software, system software, supporting software, development tools and utilities.
Data assets	Data for diagnostics, data for direct patient care, central patient records clinical support and administration.

(Reference: *NHS ISO/IEC 17799 Toolkit*)

4.3 Threat Assessment

Assets are subject to many kinds of threats. A threat has the potential to cause an unwanted incident, which may result in harm to an organisation, its services, systems, business processes and/or assets. This harm can occur from a direct or an indirect attack on one or more of an organisation's assets in the form of their unauthorised destruction, unavailability, loss, modification, corruption, misuse or breach of confidentiality, whether originating from accidental or deliberate sources or events. A threat would need to occur, possibly exploiting a vulnerability (see below) of the organisation, in order to cause such harm.

Examples of threats are given below. These are all taken from *ISO/IEC 17799 Part 1* and so refer to IM&T systems. However, similar threats can affect all assets. For example, an individual masquerading as an authorised person can gain access to any area and cause damage to assets or a breach of confidentiality.

Personnel Threats

Threats	Likely impact
Masquerading of identity	Confidentiality, integrity impaired, physical damage
Staff shortage due to annual leave, sickness or industrial action	Availability impaired
Theft or wilful damage by insiders	Confidentiality, integrity, availability impaired
Theft or wilful damage by outsiders	Confidentiality, integrity, availability impaired
User error	Confidentiality, integrity, availability impaired
Use of computer software in an unauthorised way	Confidentiality, integrity impaired
Use of electronic network facilities in an unauthorised way	Confidentiality, integrity impaired

Physical and Environmental Threats

Threats	Likely impact
Fire	Availability impaired
Power failure	Availability, integrity impaired
Water damage	Availability impaired

Threats to Computers and Networks

Threats	Likely impact
Communications failure	Availability impaired
Communications infiltration	Confidentiality, integrity, availability impaired
Communications interception	Confidentiality, integrity, availability impaired
Hardware maintenance error	Availability impaired
Introduction of virus or disruptive software	Integrity impaired and availability
Misuse of system resources	Confidentiality, integrity, availability impaired
Network hardware failure	Availability impaired
Network software failure	Integrity, availability impaired
Network management failure	Availability impaired
Network access by unauthorised users	Confidentiality, integrity, availability impaired
Operations error	Confidentiality, integrity, availability impaired
Repudiation	Legal risks
Software maintenance error	Integrity impaired and availability

4.4 Vulnerability Assessment

Vulnerabilities are weaknesses associated with an organisation's assets. These weaknesses may be exploited by a threat causing unwanted incidents that may result in loss, damage or harm to those assets. Vulnerability in itself does not cause harm; it is merely a condition or set of conditions that may allow a threat to affect an asset.

Examples of vulnerabilities are given below. Again, these are all taken from *ISO/IEC 17799 Part 1* and so refer to the IM&T systems. However, similar threats can affect all assets. For example, staff shortage can have a severe effect on any of the services provided by the organisation.

Personnel Security

Vulnerability	Exploitation
Insufficient trained personnel	Staff shortage due to annual leave, sickness or industrial action
Unsupervised work by external contractors	Theft, sabotage or espionage
Insufficient security training	Staff error in general
Lack of security awareness	User errors
Poorly documented software	Staff error in general
Lack of monitoring mechanisms	Use of software in an unauthorised way
Lack of policies for the correct use of telecommunications media and messaging	Use of network facilities in an unauthorised way
Inadequate recruitment procedures	Wilful damage

Physical and Environmental Security

Vulnerability	Exploitation
Inadequate physical access control to buildings, offices etc	Wilful damage or theft
Lack of physical protection for the building, doors, and windows	Theft, wilful damage, espionage
Location in an area susceptible to flood	Flooding
Unprotected storage	Theft or corruption of media
Insufficient maintenance/faulty installation of storage media	Unavailability, corruption or loss of data
Susceptibility of equipment to voltage variations	Power fluctuation. Unavailability, corruption or loss of data
Unstable power grid	Power fluctuation. Unavailability, corruption or loss of data

Computer and Network Management

Vulnerability	Exploitation
Unprotected communication lines	Eavesdropping, communications failure
Poor joint cabling	Communications infiltration or breakdown
Lack of identification and authentication Procedures	Masquerading of user identity
Transfer of passwords in clear	Network access by unauthorised users
Lack of proof of sending or receiving a message	Repudiation
Dial-up lines	Network access by unauthorised users
Unprotected sensitive traffic	Eavesdropping
Single point of failure	Failure of communications services
Inadequate network management	Traffic overloading
Lack of care at disposal	Theft or breach of confidentiality
Uncontrolled copying	Theft, breach of confidentiality or breach of copyright leading to legal sanctions
Unprotected public network connections	Use of software by unauthorised users

System Access Control/Systems Development and Maintenance

Vulnerability	Exploitation
Complicated user interface	Operational staff error
Disposal or re-use of storage media without proper erasure	Use of software by unauthorised users
Lack of audit-trail	Use of software in an unauthorised way
Lack of documentation	Operational staff error
Lack of effective change control	Software failure
Lack of identification and authentication Mechanisms like user authentication	Masquerading of user identity
Lack of identification and authentication Procedures	Masquerading of user identity
No 'logout' when leaving the workstation	Use of software by unauthorised users
No or insufficient software testing	Software malfunction
Poor password management (easily guessable passwords, storing of passwords, insufficient frequency of change)	Masquerading of user identity
Unclear or incomplete specifications for developers	Software failure
Uncontrolled downloading and using of software	Corrupted data and non-availability of system
Unprotected password tables	Masquerading of user identity
Software errors	Use of software by unauthorised users
Wrong allocation of access rights	Use of software in an unauthorised way

4.5 Impact Assessment

For every asset or group of assets, the impact of each combination of assets and threats should be assessed. The aim is to arrive at an indication of the wider effects should the threat occur and succeed. At this stage we are not concerned with the probability of the threat succeeding, just the impact if it does.

The method of impact assessment may vary from one organisation to another. A guide is provided by the following tables, which are based on the methodology employed by the CCTA's Risk Assessment Management Methodology (CRAMM) software.

This assesses impact according to the effect on personal safety, personal information (Data Protection Act 1998 etc.), legal obligations, law enforcement, commercial and economic interests, financial loss, public order and management and business operations. The impacts are rated from 1 to 10 with 10 representing the most serious. Some of the values are omitted for certain impacts.

Impact assessment will normally be carried out by the business continuity plan co-ordinator or by a risk assessment specialist. However, the opinion of the person most concerned should be sought to establish the level of impact. This will be the line manager, who will be able most easily to determine the effect of an asset not being available.

The level of impact may of course vary with the amount of time that an asset is unavailable.

Impact type	Value	Effect
Personal safety	1	Could lead to an individual's minor injury
	2	Could lead to several individuals' minor injuries
	3	Probability of an individual's minor injury
	4	Probability of several individuals' minor injuries
	6	Probability of an individual's injury (not a minor one)
	7	Probability of several individuals' injuries (not minor)
	8	Probability of threats to life
	9	Probability of an individual's death
	10	Probability of widespread loss of life
Personal information	1	Minor distress to an individual
	2	Serious distress to an individual
	3	A breach in regulatory or ethical requirements or a failure to observe declared policy on protection of information – leading to minor embarrassment to an individual
	4	A breach in regulatory or ethical requirements or a failure to observe declared policy on protection of information – leading to significant embarrassment to an individual or minor embarrassment to several individuals
	5	A breach in regulatory or ethical requirements or a failure to observe declared policy on protection of information – leading to serious embarrassment to an individual
	6	A breach in regulatory or ethical requirements or a failure to observe declared policy on protection of information – leading to serious embarrassment to several individuals
Legal obligations	3	Damages or penalties up to £2,000
	4	Damages or penalties up to £10,000
	5	Damages or penalties up to £50,000 or a custodial sentence up to two years
	6	Damages or penalties up to £250,000 or a custodial sentence up to ten years
	7	Unlimited Damages or penalties or a custodial sentence over ten years
Law enforcement	3	May facilitate the commission of a crime or prejudice its investigation (not DPA)
	4	May cause the investigation of a crime or a trial to be abandoned (not DPA)
	7	May facilitate the commission of a serious crime or prejudice its investigation
	8	May cause the investigation of a serious crime or a trial to be abandoned
Commercial and economic interests	1-8	These all refer to competition and are inappropriate to an NHS organisation
	9	Could substantially undermine the commercial interests or the financial viability of the organisation
Financial loss or disruption of activities	1	Losses up to £9,999
	2	Losses from £10,000 to £29,999
	3	Losses from £30,000 to £99,999
	4	Losses from £100,000 to £299,999
	5	Losses from £300,000 to £999,999

Impact type	Value	Effect
	6	Losses from £1,000,000 to £2,999,999
	7	Losses from £3,000,000 to £9,999,999
	8	Losses from £10,000,000 to £29,999,999
	9	Losses above £30,000,000
	10	The organisation will cease to exist
Public order	1	Is likely to cause very localised or community level protest
	3	Is likely to cause limited or localised unrest
	6	Probable demonstrations, significant lobbying or localised industrial action
	7	Probable industrial action with national publicity
	8	May cause industry wide industrial action
Management and business operations	1	Inefficient operation of one part of the organisation
	3	Undermining of the proper management of the organisation and its operation
	5	Impeding effective management of the organisation
	6	Disadvantage to the organisation in its negotiations with outsiders
	7	Will seriously impede the development or operation of the organisation's policies or substantially disrupt significant operations.
Loss of goodwill	2	Local embarrassment within the organisation
	3	Adverse effect on stakeholders, suppliers, regulatory bodies, government or the public with local adverse publicity
	5	Adverse effect on stakeholders, suppliers, regulatory bodies, government or the public with national adverse publicity
	7	Adverse effect on stakeholders, suppliers, regulatory bodies, government or the public with widespread adverse publicity

Additionally, an NHS organisation should consider the effect on the services it provides and the repercussions in its public image. Some of these are listed below. No attempt has been made to ascribe values for these impacts. The values should be decided by each organisation.

Impact Type	Value	Effect
Services		Poor handling of correspondence
		Short delays in treatment
		Considerable delays in treatment
		Prolonged delays in treatment
		Treatment impossible
Morale		Staff morale suffers
		Complaints from staff
		Widespread complaints from staff
		Representations from trades unions
		Ballot on industrial action
		Industrial action
		Staff leaving in small numbers
		Staff leaving in great numbers
Public image		Letters in the local press
		Adverse reports in the local press
		Adverse reports in the national press
		Questions asked in the House of Commons
		Embarrassment to the Minister
		Resignation of a senior manager
		Resignation of more than one senior manager

Within IM&T, the impacts may be classified as:
a) destruction of assets;
b) denial of use;
c) disclosure;
d) incorrect modification (whether accidental or deliberate).

When assessing impact the most serious impact of those listed above or others should be the one that is used to arrive at a final assessment. The worst-case scenario should be considered. For example, if business operations would be disrupted at the end of the month but not at other times, the end of the month should be the time for which assessment is made.

4.6 Risk Analysis

The risk is calculated from the analysis of threats, vulnerabilities and impacts on key assets. Where the risk is unacceptable, steps should be taken to reduce it by applying measures to reduce the impact, threat or vulnerability to an acceptable level.

The risk will be determined by an algorithm, based on ascribing values to the risk, that is based on the values already ascribed to the threat, vulnerability and impact. There is no universally appropriate formula for this process, but it approximates to:

Risk = Threat x Vulnerability x Impact

Thus, a threat, which had a high impact, might still be rated highly although its occurrence would be relatively rare. Conversely, a frequent threat (especially where the organisation was vulnerable) could be rated highly even though its impact was only minor.

The Department of Health defines Principal risks (sometimes known as 'key risks') as those which have significant potential to impair or affect the operational or financial ability of the organisation to deliver ongoing services and may be strategic or operational in nature. A properly carried out risk analysis will identify the principal risks among others and the following risk management will ensure that any risks so identified are adequately addressed.

Many NHS organisations are developing single incident reporting systems. Therefore, all incidents affecting the continuity of services, systems and business processes, should also be reported using unified incident reporting procedures. Likewise, NHS organisations are also encouraged to take into account for Business Continuity Planning purposes, risks and incidents identified through local incident reporting systems and risk management programmes.

NHS organisations may also find it expedient to standardise the values ascribed to impact, threat and vulnerability and thus the risk within Business Continuity Planning to those used for local risk management programmes. This includes qualitative measures of the likelihood and consequence of risk and the evaluation of severity and prioritisation of risks.

4.7 Risk Registers

Risk assessment provides a practical and methodical procedure for identifying and evaluating risks. All risks identified through risk assessment for Business Continuity Planning should also be reported. Reported risks, whether based on assessments or incidents, should then be prioritised for inclusion on the corporate risk register(s) together with appropriate identified controls, action plan and any contingency measures.

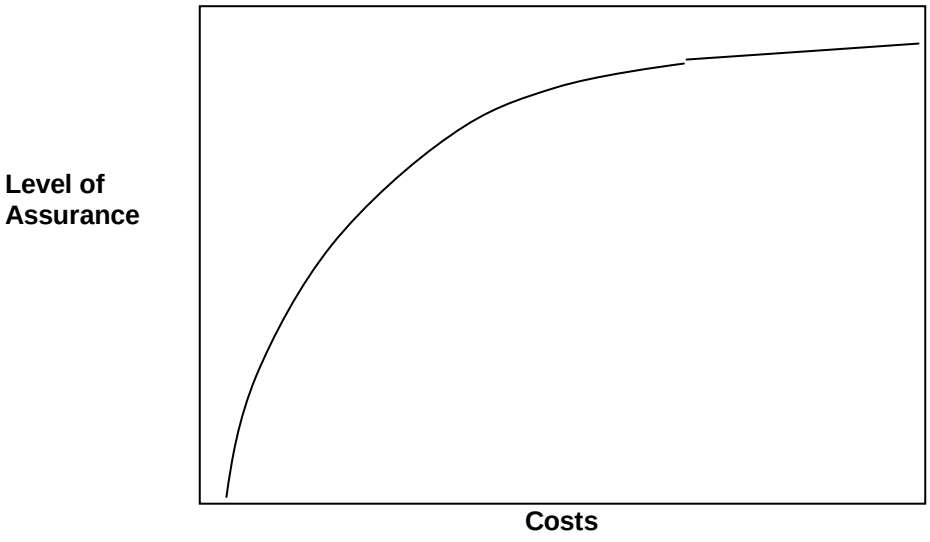
The Department of Heath, as stated in the Guidelines for Implementing Controls Assurance in the NHS (1999), required NHS organisations, to have centrally managed risk registers, with minimal risk registers in place by 31st March 2001. Such risk registers were to and still should contain risks of all kinds and should be capable of producing regular reports on identified risks. Dependent upon the size and the complexity of the organisation, risk registers may be corporate and comprehensive or may consist of a number of registers, covering individual functions or departments, which then link into an organisation-wide risk register.

4.8 Risk Management

Risks will be managed by putting into place measures that will reduce the risk, transfer it or avoid its occurrence altogether. Risk management is the practice of reducing the identified risks to an acceptable level. The risk analysis process will identify the most serious risks and these should be tackled first. However, it is virtually impossible to reduce a risk to zero.

4.9 Risk Acceptance

The following diagram shows non-quantitatively, the level of assurance achieved by spending on risk management measures. In effect, mathematically speaking, 100% assurance can never be achieved as the diagram shows. Assurance and expenditure are a straight line that can be closely approached by a curve, but never met. For that reason there will always be some risks that are deemed acceptable.



These risks may be rated lowly because of their low probability, because the impact is seen as light, because precautions have already been taken to recover from them or because alternative arrangements are in place. Examples of these are:

Threat	Reason for Acceptance	Residual risk
Flood	Building is in a high position. Flood considered a remote possibility	Water tanks above may still burst
Loss of electrical power	Back-up generator in place	Both power source and generator may fail simultaneously (particularly if the generator is not fully tested.)
Loss of recent computer data	Back-up taken daily	Updates during the day will be lost
Computer network failure	Network has proved reliable in the past	Unforeseen attack e.g. rodents gnawing the cables
Computer software failure	Change control in place	Urgency of change leads to control being by-passed.

Business Continuity Planning is necessary to address the residual risks that are deemed unacceptable. However well the risk is managed there will always be some area that, if a threat should succeed, will need exceptional steps to be taken. Business continuity plans should list those steps so that the essential services, systems and business processes of the organisation can continue.

Its application will depend on the result of the impact assessment carried out as part of the risk assessment process. This will determine those assets that are essential and those that are merely desirable. While the impact assessment will form an integral part of the risk assessment process, it should be reconsidered once it is decided to accept certain risks. In the latter case, the point is not so much “can the threat occur?” as “what will the effect be if it does?” If the threat does occur, the threat rating is 100%. The business continuity plan will be there to ensure that the essential business functions are in place if such an eventuality arises.

So at the end of the risk assessment process, the impact assessment should be revisited to ensure that action is applied where it is needed. The action taken will then address the substitution or replication of the assets deemed essential, depending on the time that any interruption persists. The impact assessment should consider all business processes, and not just be limited to information processing facilities.

The impact assessment and the design of the business continuity plan should be carried out with full involvement from the 'owners' of the key assets, resources and processes within the business areas. Depending on the outcomes a strategy should be developed to determine the overall approach to business continuity. There should be managed processes in place for developing and maintaining business continuity throughout organisations, which should bring together the following key elements, which reiterate the steps described above:

a) identify those key assets associated with each business area;

b) develop an understanding of the main risks that the organisation is facing:

c) understand the impact which any interruptions are likely to have on the business of the organisation (smaller incidents, as well as serious incidents);

d) formulate and document a business continuity strategy consistent with the agreed business objectives and priorities;

e) formulate and document business continuity plans in line with the agreed strategy;

f) set up teams of relevant personnel to develop business continuity plans and put them into practice when necessary;

g) regularly test and update the plans and processes;

h) ensure that the management of business continuity is incorporated in the individual organisation's processes and structure;

i) assign responsibility for co-ordinating the business continuity management process at an appropriate level within the organisation.

5. ORGANISATIONAL ROLES AND RESPONSIBILITIES

5.1 Introduction

Whilst individual NHS organisations retain responsibility for developing business continuity plans for their organisation, current guidance defines overall responsibility for ensuring the development of major incident, service continuity and IM&T continuity plans.

5.2 Major Incident Planning

Following changes to health service organisation, set out in *Shifting the Balance of Power: The Next Steps (Department of Health: February 2002)* the overall responsibility for the health of the population passed from Health Authorities to Primary Care Trusts (PCTs). As a result arrangements became necessary to ensure that the emergency planning function, previously carried out by Health Authorities, was effectively taken forward by Primary Care Trusts.

The Department of Health wrote to Chief Executives of Primary Care Trusts and Health Authorities on 9 April 2002, referring to the Primary Care Trust Function Regulations. These had been amended from 1st April 2002 in order to remove the bar on PCTs exercising the powers delegated to them by Health Authorities, e.g. under sections 2 - 5 of the NHS Act 1977, to carry out planning for major incidents.

It then became the responsibility of PCT Chief Executives to ensure those plans and arrangements are in place within their own PCT and collaborative arrangements with neighbouring NHS organisations and partner agencies. Regional Directors of Public Health were charged with having to be satisfied that their health community could participate effectively in the multi-agency response arrangements for dealing with major incidents including public health emergencies. That included health chairing and coordination of the Joint Health Advisory Cell (JHAC) at a police main base station in the event of a chemical, biological, radiological or nuclear (CBRN) incident and the provision of at-site officers, when appropriate.

The first response to major incidents is normally by Ambulance Services NHS Trusts and Acute Trusts who have expertise and training to handle casualties in the immediate aftermath. These mechanisms have operated well for many years with Police, Fire, Local Authority, the voluntary sector and a range of partner agencies involved in local planning groups. Chief Executives of Ambulance Services NHS Trusts and Acute Trusts should ensure that their trusts have appropriate up-to-date major incident plans that have been tested in accordance with DH guidance, the co-ordination of the operational response being managed through the usual control mechanisms involving Ambulance Control.

5.3 Service Continuity

The Department of Health issued guidance to Strategic Health Authority Directors of Planning on 8th November 2002, delivering a new three-year planning cycle for health and social care. That guidance built on the Planning & Priorities Framework guidance, *Health Improvement and Modernisation Plans (HIMPs) Requirements for 2002,* which was issued to Primary Care Trusts on 2 October 2001. That guidance set out Primary Care Trust responsibilities for the development of the local health improvement and modernisation plan (HIMP). These set out local targets for the delivery of NHS priorities in line with National Service Frameworks, and Local Modernisation Review. They also recognise and take forward work on the health improvement and health inequality agenda.

Primary Care Trusts take the lead in developing the local HIMP, which is constructed in conjunction with other local organisations, e.g. hospital trusts and local authorities. Primary Care Trusts are then accountable for the delivery of the local HIMP to the local Strategic Health Authority.

Primary Care Trusts, as lead NHS organisations, are expected to become responsible for the flow of the majority of NHS funding (75% by 2004) and commensurate with it an increase in responsibility for commissioning services. It is intended that the majority of the commissioning of health care services, including hospital and community health services, will be done by Primary Care Trusts.

Primary Care Trusts therefore have a responsibility for ensuring that local providers, including hospital and community health services, have developed and maintained up-to-date plans for managing risks. Also ensuring that at all times and circumstances, each organisation can continue to operate the planned operational services to, at least, a minimum pre-determined level.

The creation of Care Trusts from 2002, to co-ordinate local health and social care services, commissioning and delivering primary/community health care and social care for various client groups present an additional challenge. These trusts, which are authorised by the Secretary of State under Section 45 of the Health and Social Care Act 2001, build upon existing NHS/Local Authority partnerships, but provide for individual organisations to remain accountable for their own services, provided as a component of a Care Trust. The board of Care Trusts will have a responsibility for ensuring that each contributing organisation can continue to operate the planned operational services to, at least, a minimum pre-determined level.

5.4 IM&T Continuity

Information for Health introduced Local Implementation Strategies (LIS), through which local NHS organisations and local authorities would be required to agree actions, fund and implement IM&T developments on a community-wide basis. The original guidance on developing those Local Implementation Strategies (LIS) was published in *Implementing Information for Health* (number 2) issued in August 1999.

The first three LIS iterations were based on local health communities centred on health authorities, which had the responsibility for ensuring that a LIS was produced for and supported by the NHS organisations within the authority boundary. *Shifting the Balance of Power: The Next Steps (Department of Health: February 2002)*, changed the organisational responsibilities for assessing and managing Local Implementation Strategies for IM&T. Strategic Health Authorities are now responsible for developing management arrangements that best suit local circumstances. They are also responsible for the performance management of local NHS IM&T implementation programmes to meet national targets.

By definition, therefore, Strategic Health Authorities now have responsibilities for ensuring that local NHS organisations develop plans to ensure that each organisation can continue to operate IM&T systems, or restore IM&T operations within required time-scales, following interruption to or failure of, critical processes to systems that address national priorities.

NHS organisations retain individual overall responsibility for ensuring the development of IM&T continuity plans for ensuring that they can continue to operate local systems, or restore IM&T operations within locally defined time-scales, following interruption to or failure of, critical processes.

6. ALLOCATE RESPONSIBILITIES FOR BUSINESS CONTINUITY PLANNING

6.1 Introduction

The developing of organisation-wide business continuity plans in NHS organisations forms an essential component of their risk management strategies and requires the full support of management boards with delegated authority and adequate resourcing. That work should take the form of a properly constituted project with allocated time-scales and budget, using a recognised project management methodology such as PRINCE2. This should help to ensure the organisation's capability to deliver their business continuity plans to budget and specification. In setting up an organisational framework to undertake the necessary planning, delegation and control, it is important to identify roles, allocate responsibilities and provide the authority to enable them.

6.2 Business Continuity Planning Team

The task of developing, maintaining and reviewing business continuity plans should be the responsibility of a dedicated Business Continuity Planning Team operating under the authority of the organisation's board, executive or senior management team.

The Business Continuity Planning Team should be composed of senior managers in the organisation with direct responsibility for operational services and resources, which fall within the scope of the business continuity plans. It is recommended that the team is comprised of no more than eight persons and led by an individual having adequate authority, seniority and influence at Board level within the organisation. All team members should be able to contribute to the task of developing, maintaining and reviewing business continuity plans by committing resources in the form of user expertise, technical effort, financial investment and their high level of decision-making ability.

Whilst the composition of Business Continuity Planning teams may vary between organisations, according to local business culture and need, the subject area would suggest representation of certain functional requirements involving clinical, estates, finance and human resources.

The NHS Information Authority has developed two-day Business Continuity Planning training programmes, especially designed for members of Business Continuity Planning teams and their co-ordinators. The materials used in this programme will be available for local training and awareness programmes.

In recognition of its contribution towards effective risk management within the organisation, the planning team should be linked to other relevant existing groups or committees within the organisation, including both Clinical Governance and Risk Management Committees. An exemplar organisational structure is shown in section 2.2. The main responsibilities of the Business Continuity Planning Team are:

a) ownership of the Project Initiation Document (PID);
b) overseeing the selection of individuals to continuity and recovery planning teams;
c) authorising the commitment of resources;
d) monitoring progress with continuity and recovery plans;
e) reviewing and approving developed continuity and recovery plans;
f) undertaking periodic reviews of business continuity, contingency and recovery plans;
g) monitoring outcomes of exercising and testing of contingency and recovery plans;
h) reporting progress to the organisation's executive or senior management team.

The Business Continuity Planning Team should appoint a co-ordinator to work in conjunction with directorates, departments and business functions to undertake the development of the business continuity plans and to be responsible for ensuring their ongoing maintenance and testing. The Co-ordinator, while working for and within the Business Continuity Planning Team, will manage the development of the contingency and recovery plans. There should be access to up-to-date guidance relevant to the different aspects of Business Continuity Planning.

The Co-ordinator should liase with existing groups within the organisation such as the records group, IM&T Steering Group and departmental groups and recruit contingency and recovery teams as necessary and supervise their work. They should ensure that each plan is developed in a way, which is consistent with the overall Business Continuity Planning framework. The Co-ordinator should advise the Business Continuity Planning Team of any deviations from plans. The work of the Business Continuity Planning Team's Co-ordinator will require support to undertake the administration of the co-ordination and monitoring of development processes.

6.3 Contingency and Recovery Teams

Whilst the work of developing each plan should be supervised by the Co-ordinator on behalf of the Business Continuity Planning Team, each contingency and recovery plan should be the responsibility of a named individual. That person should have access to appropriate business resources and should spell out the responsibilities of the teams, describing which team member is responsible for executing which component of the plan. Because initiation of such plans may occur at any time, back-up nominees for these roles should also be identified and lists of team members updated regularly to take account of changes in personnel.

Each contingency and recovery team should comprise of specialists in each relevant field of the organisation's business and have defined limits of decision-making, including expenditure up to pre-determined limits, to obviate the need for constantly referring to senior management or a co-ordinating group.

7. CONTINGENCY PLANS

7.1 Introduction

Within the framework of business continuity plans there need to be contingency plans. They will provide for procedures and the preparation of critical facilities that can be used to give continuity of essential operations during the period of contingency i.e. up to the time when recovery plans can be implemented to ensure full operations can be restored.

7.2 Contingency Plans

Contingency plans for each service element can be activated in the event of an interruption to services occurring. Such plans should be designed to prepare an appropriate response to any set of circumstances.

Contingency plans should be aimed at restoring services to a pre-determined level and should have clear unambiguous "triggering events". The "triggering events" for contingency plans to be activated should be that the level of service falls below what is acceptable. However, It must be recognised that the level to which services can be affected will vary according to other circumstances. Therefore such plans should always reflect the worst-case scenario. For example, if the impact would be greatest when there was an epidemic in the area, that is the circumstance that should be anticipated; if the impact would be greatest when it was necessary to pay suppliers within a day, that is the scenario to be covered.

Dependent upon the impact of the interruption to services or systems, contingency plans may need to be implemented in stages:

a) Emergency stage: covering the initial response to a service interruption, often involving providing a "basic" level of service;

b) Back-up stage: covering provision of a "reduced" level of service.

The need to implement contingency plans and whether using a staged response or not will in most cases is tempered by the impact upon services and anticipated duration of the failure or interruption. For example, a failure in an IM&T system lasting 30 minutes is unlikely to necessitate the implementation of the full plan.

The aim in developing contingency plans must be to select corrective actions that are most suited to the local circumstances, based on:

a) specific physical requirements;

b) staffing requirements;

c) communications requirements;

d) possible alternative sources of delivering services;

e) the operational, political and financial implications;

f) specific professional or service quality requirements;

g) financial implications.

Contingency plans should detail the interim stand-by arrangements to be used to achieve the acceptable levels of service in the event of a service being impacted. Such plans should take the form of checklists, detailing the tasks that need to be carried out. They should cover the period from the "triggering event" to the implementation of the recovery plans.

7.3 Options

The Business Continuity Planning Team should ensure that there are clear escalation policies to deal with any additional pressures, which are above the normal or expected levels, but below the levels requiring a major incident response as defined in the Major Incident Plans.

Options for restarting the service might include:

a) rearranging services and/or working practices within the organisation and reallocating staff and equipment;

b) effecting the temporary closure of the affected or other service(s) to release staff, equipment and facilities;

c) transferring affected or other service(s), including staff, equipment etc to other sites or neighbouring NHS organisations;

d) commissioning staff, equipment, or service(s) from other NHS or private healthcare organisations or commercial suppliers.

Selecting the appropriate option(s) requires an assessment of the implications of providing either the minimum or sustainable levels. Those implications include professional requirements, quality standards, resource, financial, operational and political implications, human, communications requirements, logistical etc. for the affected or other services and their related supporting processes.

7.4 Content of Contingency Plans

Contingency plans will be used under unfamiliar circumstances and it is probable that the people putting them into effect will be under severe stress. Therefore the plans need to be as comprehensive and as detailed as possible to avoid placing unnecessary decision making on the shoulders of the people involved at the time.

In particular, contingency plans should address:

a) scope of the plan;
b) assumptions and boundaries;
c) definition of a contingency;
d) how to convene the Business Continuity Planning Team;
e) criteria for invoking the contingency plan i.e. triggers;
f) initial contacts, such as suppliers, insurers and stand-by facilities;
g) names and contact details of contingency teams;
h) responsibilities of the contingency teams;
i) how to obtain back-up material;
j) how to obtain access to stand-by facilities;
k) contacts for the continuing contingency such as salvage specialists, equipment suppliers, re-builders;
l) priority of services;
m) means of restoring immediate minimum service;
n) means of restoring service to an acceptable level;
o) location of spare equipment and supplies;
p) staff requirements and how to meet them. (e.g. information, advice, accommodation, transport);
q) requirements of patients and other stakeholders and how to meet them (as above)
r) lists of suppliers;
s) handling publicity and public relations;
t) testing plan and record;
u) record of invocations;
v) lists of persons holding copy plans;
w) update procedure and list of updates.

NHS organisations vary in their composition and organisational structure, so some flexibility in approach may be required.

7.5 Contingency Teams

Small management teams should be created, with membership drawn from relevant business areas and/or system specialists, to develop, activate and co-ordinate the implementation of each contingency plan. Organisations should take steps to identify those personnel capable of participating and leading in such teams.

The persons chosen should have a good knowledge of the relevant service, system and business area involved and be capable of providing the immediate management to implement the contingency plan and offering an acceptable level of service.

Organisations will need to provide members of contingency teams with carefully planned and delivered training programmes so that they understand their roles and the roles of others. Also they need to understand the systems and procedures for their contingency plan and how available resources should be used.

Periodic exercising and testing of contingency plans would help to increase the competence and effective capability of team members. For this reason they should be involved in the testing of the plan and should give comments on the outcome of the tests.

8. RECOVERY PLANS

8.1 Introduction

Following the implementation of contingency plans, there also need to be plans for the restoration of full services and systems. These constitute recovery plans.

8.2 Recovery Strategy

A recovery strategy needs to be defined which employs a logical but relevant and practical approach towards business recovery requirements. There needs to be agreement on the recovery methods to be employed.

Recovery plans should detail the arrangements necessary for achieving the full restoration of services, within pre-determined timeframes, to defined, sustainable levels of service. The "triggering events" for recovery plans will be the implementation of contingency plans.

Procedures for recovery should take into account:

a) time-scales for full recovery which should be determined by the business and/or legal requirement;

b) for IM&T systems, identifying a starting point for processing the back-up data or the data produced under the contingency plan;

c) the most suitable sequence of restoring from back-up or other data;

d) ensuring compatibility between the current system and the media on which the required data are stored;

e) steps to ensure that the restoration of full services take into account any changed circumstances.

8.3 Content of Recovery Plans

Recovery plans need to be as comprehensive and detailed as possible, but broad enough to address a number of different options for recovery. They should include:

a) scope of the recovery plan;
b) definition of recovery;
c) names and contact details for members of recovery teams;
d) how to convene the recovery team;
e) checklists of responsibilities for members of recovery teams;
f) criteria for invoking the recovery plan;
g) initial contacts, such as suppliers and stand-by facilities;
h) how to locate back-up;
i) how to obtain access to stand-by facilities;
j) contacts for specialists, equipment suppliers etc;
k) priority for restoring services;
l) means of restoring to a sustainable level;
m) location of spare equipment and supplies;
n) staff requirements;
o) requirements of patients and other stakeholders;
p) handling publicity and public relations;
q) testing plan and record;
r) record of invocations;
s) lists of persons holding copies of plans;
t) update procedure and list of updates.

8.4 Recovery Teams

Just as with contingency plans, small management teams should undertake development, activating and co-ordinating of the implementation of each recovery plan. Unlike contingency teams, there will be time to schedule the deployment of recovery teams. Membership of those teams may have the emphasis on "technical" skills, appropriate to the business area, and the "hands-on" experience to ensure their successful implementation. To ensure adequate resources for such an intensive undertaking, recovery teams may involve using expertise external to the organisation. Those persons should have a good knowledge of the business area involved and be capable of providing the level of support required at short notice.

Just as with contingency planning, organisations need to provide members of recovery teams with carefully planned and delivered training programmes so that they understand their roles and the roles of others. Also they need to understand the systems and procedures for their recovery plan and how available resources should be used.

9. SERVICE CONTINUITY PLANNING

9.1 Service Continuity

All the services provided by NHS organisations are important to the health of their local population. However when unforeseen incidents occur there may be some interruption to the delivery of those services. As a first reaction to such incidents, the management boards of affected NHS organisations may need to take some decisions on “scaling down” or transferring of normal services. Service continuity planning provides the method of managing the risks of such incidents occurring and their effects on services.

This will involve the management boards of NHS organisations identifying those services or departments for which there are statutory, professional regulatory or service requirements to maintain them at pre-determined operational levels. Those levels for "critical" services should be at least the minimum level that can be provided on a short-term basis within legal, health and safety and professional regulatory requirements. For some services either minimum or sustainable levels may already be defined as part of an existing service level agreement, service specification or contractual arrangement. For acute hospital trusts these may include accident and emergency services, coronary care units, intensive care units, surgical wards and related clinical services such as radiology, pathology, operating theatres, pharmacy etc.

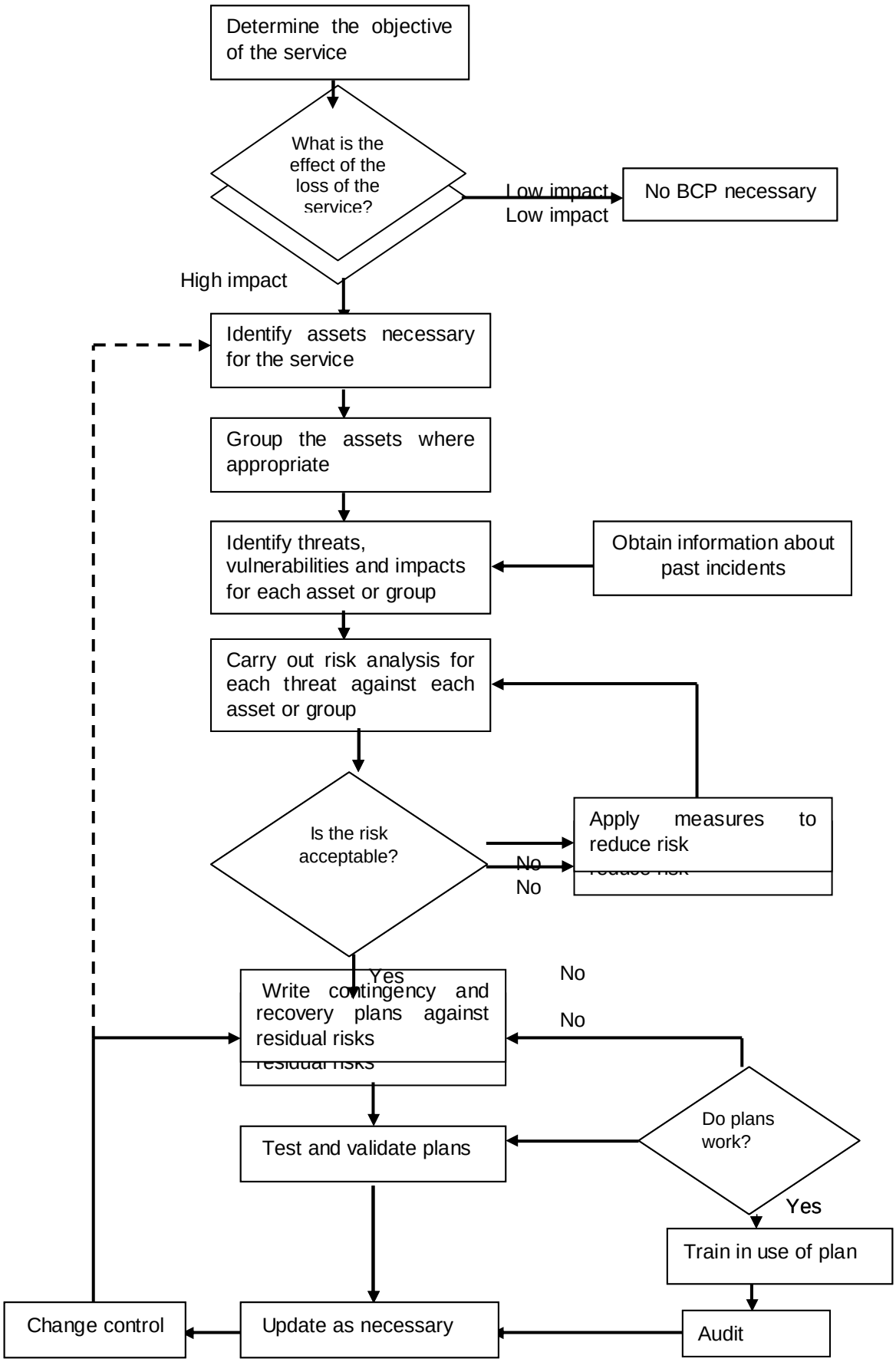
Management boards of NHS organisations may also need to take account of ethnic, religious and cultural needs as well the needs of priority groupings e.g. children, elderly or mental health patients in taking decisions about the temporary relocation, reduction or curtailment of services. Where patients are being discharged from hospital, additional transport facilities may be required including hospital cars and taxis and additional resources in the community, including district nursing and social services, need to be in place.

For management boards to make accurate decisions about the capability of their organisation to maintain the continuity of identified “critical” services, it is necessary to base those decisions on accurate information on the sequences of activities or transactions, which, together, enable the normal delivery of those services. This should include concise statements of their purpose, outline of service(s) provided, current volume of activity, resources utilised, internal and external dependencies and essential quality standards (including time dimensions). As examples of external dependencies, management boards should consider the provision of electricity, gas, oil, water and communications and the supply of medical necessities such as sterile material, pharmaceuticals and operating packs.

Management boards need to take account of those functions and facilities that support those services as some or many of these services may themselves be at risk during an emergency. They will therefore need to ensure that there will be adequate continuity from support functions such as estates management, medical equipment, IM&T, catering and domestic services. Each of these supporting processes may have a number of inputs or outputs, which can be in the form of information, materials or activity. Most processes will require equipment, facilities, procedures and skilled personnel. These often need to be available together, but possibly in varying combinations, supplied by a number of different “critical” services.

The chain of activities involved, including all inputs and outputs, and all the dependencies should be mapped in order to assess the degree of “criticality” for each supporting process and the implications for both contingency and recovery plans drawn up. These should define the minimum and sustainable levels for the critical services that can be maintained for defined periods of time without necessarily having the full range of support processes available.

The flow chart on the next page shows the service continuity planning framework.



SERVICE CONTINUITY PLANNING FRAMEWORK

9.2 Risk Assessment

The identified "critical" services and their supporting functions need to be subjected to risk assessment. The purpose being to identify and assess the risks to which those critical services, their supporting functions and assets are exposed, in order to identify and select appropriate and justified control measures. This is an important stage in the development of Business Continuity Plans. Risks are a function of the values of the assets, the likelihood of threats occurring to cause impacts on the organisation's business and the ease of exploitation of the vulnerabilities by the identified threats. The application of controls to reduce the risks constitutes risk management.

Whilst NHS organisations may take measures to minimise such risks it will not always possible to anticipate all such situations, and, in any case, preventive action may be prohibitively expensive, such as replacing entire systems or medical equipment. Therefore NHS organisations should also identify options for recovery in the event of major disruption, being where the situation is critical and service delivery has or would be in danger of falling below the accepted minimum levels.

Details of Risk Assessment methodology is set out in section 4 of this document.

9.3 Options for Restart

In order to restart services at minimum acceptable levels (contingency) or at sustainable (recovery) levels it is appropriate to select the most appropriate corrective actions to address each particular type of risk, from which detailed contingency and recovery plans can be developed, taking into account local circumstances. The options should be investigated and implementation plans should be developed, activated and co-ordinated by a small team drawn from relevant business areas to ensure their practicality.

9.4 Testing and Review

Service continuity plans should be fully reviewed on at least an annual basis or more frequently where needs are indicated by service changes or improvement changes highlighted from experience of their implementation and use. This is to ensure that planning and existing training arrangements highlight changes that are needed or further training required. This is also necessary to ensure that there is still full commitment from within the organisation and contractors or suppliers, to the plan.

As far as possible disruption to the provision of utilities should be minimised by agreeing priority status with the utility suppliers. This can be done through NHS Supplies. For some supplies, such as oil and water, the threat of disruption can be eased by having adequate levels of reserves held on site.

10. IM&T CONTINUITY PLANNING

10.1 Context

Information Governance provides NHS organisations with the structure that links the data it collects, the processes the data then goes through and the resources that support the data, to the organisation's information strategies and objectives. It integrates the various practices of planning, implementing, delivering and maintaining IM&T services. To achieve its objectives, senior managers of NHS organisations must understand the status of their own information systems and decide what control objectives and activities are needed. Management must then ensure that an internal control system or framework is in place which supports the business processes, making it clear how each individual control activity satisfies the information requirements and how they impact on resources.

To achieve that level of control NHS organisations must satisfy information security requirements, including the confidentiality, integrity, and availability of their data and information. The information security management standard relevant for all NHS organisations is the *Code of Practice for Information Security Management*, usually known as BS 7799 (1999), which replaced the IM&T Security Manual *"Ensuring Security and Confidentiality in NHS Organisations"*. Management must also optimise the use of available resources, including data, application systems, technology, facilities and people as one of the high-level control objectives is ensuring that IM&T support for business processes is continuous.

IM&T Business Continuity Planning forms part of BS 7799 (Section 11) and is also a core component of NHS organisations' corporate risk management programmes. It forms an essential component of an organisation's business activities and is aimed at counteracting serious interruptions to information systems. The development and maintenance of IM&T business continuity plans should be based on an analysis of the threats, vulnerabilities and impacts that may effect the organisation and its information systems. Those business continuity plans should contain both contingency and recovery components. They should define the organisation's arrangements for achieving both an acceptable interim level of service and the timely restoration of full services. Such plans should be tested, reviewed and updated at regular intervals, on at least on an annual basis.

10.2 Risk Assessment

The identified "critical" services and their supporting functions need to be subject to risk assessment. The purpose being to identify and assess the risks to which those critical services, their supporting functions and assets are exposed in order to identify and select appropriate and justified control measures. This is an important stage in the development of business continuity plans. Risks are a function of the values of the assets, the likelihood of threats occurring to cause impacts on the organisation's business and the ease of exploitation of the vulnerabilities by the identified threats. The application of controls to reduce the risks constitutes risk management.

Whilst NHS organisations may take measures to minimise such risks (threats) it will not always possible to anticipate all such situations, and, in any case, preventative action may be prohibitively expensive, such as replacing entire systems or medical equipment. Therefore NHS organisations should also identify options for recovery in the event of major disruption, being where the situation is critical and service delivery has or would be in danger of falling below the accepted minimum levels. Details of Risk Assessment methodology is set out in section 4 of this document.

10.3 Restoring System Integrity

To restore IM&T system integrity it needs to be ensured that where current files are corrupted a system can restart processing by re-building databases from back-up or archived copies. This is essential for systems for which operational continuity is critical to end-users. This would normally involve returning to the last checkpoint (date stamp), then reprocessing any data after the point of failure.

However, the successful outcome of such recovery depends heavily on the availability of up-to-date and complete back-up data and use of checklists. Any shortfall in current back-up availability could lead to inconsistent data or coding following implementation. Tests should be carried out to ensure that files/databases are not only correctly restored but that they are usable. Standard housekeeping routines should be regularly tested to ensure that they function correctly.

10.4 Back-up

Maintaining the integrity and availability of essential data and information through back-up, is vital and therefore it is essential that the organisation has well-defined procedures for undertaking it. The back-up sequencing needs to be consistent with the needs of the business area and compatible with recovery plans. BS 7799-1 clause 8.4.1 recommends a minimum three generations of business data be kept. However, the number of copies must be affected by the frequency of update and the necessity to restore up-to-date information. It is also important to keep sufficient back-up copies to allow restoration to be made after a serious error has been found in the current data; this may take a few days. Where there is a network environment this should be based on full server back-up plus a number of incremental updates in defined daily, weekly or monthly cycles. At least some of the recent back-up must be kept in secure storage remotely from the original data. This will ensure that a single disaster will not destroy all copies of the data. The security arrangements covering back-up data must be as good as those for the original data.

Back-up should include copies of the software held under the same secure conditions as the data and be available for use should a contingency plan arise. However, the Copyright, Designs and Patents Act (1988) does not normally permit back-up copies for other purposes. See Intellectual Property Rights (10.5) below.

All back-up and procedures for restoring from back-up must be documented. The documents in hard-copy form must be readily available in a contingency situation.

NHS organisations should consider entering into escrow agreements so that the source code of commercial software can be obtained in the event of the supplier being no longer able or willing to maintain the software. However, NHS organisations need to check the viability of using back-up media and have sufficient knowledgeable resources on restoration procedures.

10.5 Intellectual Property Rights

Appropriate procedures should be implemented to ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright, design rights or trademarks. Copyright infringement can lead to legal action, which may involve criminal proceedings. Legislative, regulatory and contractual requirements may place restrictions on the copying of proprietary material. In particular, they may require that only material that is developed by the organisation, or that is licensed or provided by the developer to the organisation, can be used.

Whilst an organisation may take ownership of the disk or CD upon which computer software is delivered, proprietary software products are usually supplied under a licence agreement that does not give ownership of the software itself. Such licence agreements often limit the use of the products to a specified number of machines. However, it is always permissible to create copies intended purely for back-up.

The Copyright, Designs and Patents Act of 1988 makes it illegal to copy computer software without the copyright owner's, or software developer's permission. Also the United Kingdom Software Regulations 1992 provide that certain acts of copying and adaptation (including error correction) are permitted unless prohibited by contract.

Therefore NHS organisations should consider implementing the following controls:

a) checking all existing software contracts;

b) publishing a software copyright compliance policy which defines the legal use of software and information products;

c) issuing standards for the procedures for acquisition of software products;

d) maintaining awareness of the software copyright and acquisition policies, and giving notice of the intent to take disciplinary action against staff who breach them;

e) maintaining appropriate asset registers;

f) maintaining proof and evidence of ownership of licences, master disks, manuals, etc;

g) implementing controls to ensure that any maximum number of users permitted is not exceeded;

h) carrying out checks that only authorised software and licensed products are installed;

i) providing a policy for maintaining appropriate licence conditions;

j) providing a policy for disposing or transferring software to others;

k) using appropriate audit tools;

l) complying with terms and conditions for software and information obtained from public networks.

10.6 Review

IM&T Continuity Plans need to be reviewed frequently, but at least on an annual basis. Those plans may need to be reviewed more frequently where needs are indicated by changes in the services that systems support, where new systems are implemented or where the need for changes has been highlighted by experience of implementation and use. This is essential to ensure that plans and training remain valid or to highlight changes that may be needed. Such review is also necessary to ensure that there is still full commitment within the organisation and that contractors or suppliers are still relevant and committed.

11. MAJOR INCIDENT PLANNING

11.1 Introduction

All NHS organisations play a crucial role in responding to major incidents and therefore are required to have Major Incident Plans. Dependent upon the nature of such incidents, other responders could include the fire service, police, local authority, coastguards, industry, voluntary agencies, central government and the armed forces. The overall aim of major incident plans is to achieve an effective response to emergency situations or incidents, regardless of their cause. Such incidents may be serial, multiple or single, often effecting a large area, involving more than one organisation and a broad range of agencies and services.

Examples of such situations are major accidents, disease outbreaks, chemical incidents, radiological incidents etc. Major incidents are classically triggered by sudden major transport or industrial accidents. However they can start in a number of ways such as a major chemical or nuclear release and begin in one category and evolve to another; therefore response will similarly need to evolve. They may also build slowly from a series of smaller incidents. There is sometimes no clear starting point for a major incident and the point at which it becomes 'major' may only be clear in retrospect. In all cases NHS organisations need to have a thoroughly prepared emergency response to manage the incident and mitigate its effects. Occasionally there may be a need for the extensive planning for casualties from war episodes or terrorist action, might require the NHS to mount an exceptional response.

All NHS organisations can become involved. Ambulance services, acute hospitals providing mobile medical teams and acting as receiving hospitals, not just in A&E, but throughout the hospital, community services and primary care teams looking after those affected by a major incident and in their lead role in public health incidents.

External incidents can also have an effect on staff availability as transport or the domestic life of the personnel can suffer. Some staff may be called on for emergency duties, such as special constables or Territorial Army. The threat of staff shortage can be lessened by the willingness of staff to cover in the case of shortage and at times of difficulty this willingness will largely depend on the state of personnel relations. Part of Business Continuity Planning is the fostering of good relations before, during and after any disruption.

11.2 Internal Incidents

Major incident plans should include schemes for dealing with major incidents within the NHS organisations themselves or by external incidents that impair their ability to work normally. Fire, breakdown of utilities, major equipment failure, hospital-acquired infections or violent crime may paralyse the provision of services and jeopardise safety arrangements in the short term and erode staff morale and public confidence in the longer term.

11.3 Responsibilities

Following the changes to the health service in England in April 2002, Primary Care Trusts took over statutory responsibility for major incident planning from health authorities in October 2002, although transitional arrangements had effectively been in place since April 2002. Strategic Health Authorities now have responsibility for co-ordination of response to more widespread incidents.

The Department of Health's Emergency Planning Co-ordination Unit leads NHS planning for major incidents in England.

11.4 Planning

Major incident planning is part of Business Continuity Planning and the same principles apply as to all continuity plans for incidents that disrupt the normal working of NHS organisations, including:

- assessing the potential risks;
- taking steps to reduce those risks.
- developing contingency and recovery plans;
- defining key roles and responsibilities;
- training staff to respond effectively to those plans;
- undertaking preparations;
- ensuring staff are properly equipped;
- ensuring safety and protection;
- control and co-ordination;
- communications;
- media;
- exercising plans;
- reviewing plans and performance;
- evaluating response and amending or updating plans.

11.5 Risk assessment

The purpose of risk assessment for major incident planning is to identify and assess those risks to which the emergency services, their supporting functions and assets are exposed, in order to identify and select appropriate and justified control measures. This is an important stage in the development of major incident plans. Risks are a function of the values of the assets, the likelihood of threats occurring to cause impacts on the organisation's services and the ease of exploitation of the vulnerabilities by the identified threats. The application of controls to reduce the risks constitutes risk management.

Whilst NHS organisations can take measures to minimise such risks (threats) it will not always be possible to anticipate all such situations. In some cases, preventative action may be outwith the control of the organisation, involve several different agencies e.g. ambulance, fire, police, local authority services or because of their magnitude, be prohibitively expensive. Therefore NHS organisations should also identify options for recovery in the event of such threats being realised. This could include major disruption, being where the situation becomes so critical that delivering such services have or would be in danger of falling below the accepted minimum levels.

11.6 Testing and review

Plans must be sufficiently flexible to deal with a range of situations that are likely to increase in significance, duration, complexity and unpredictability. Those plans also need to be compatible with those of other potential responders to a major incident and should be tested and reviewed on at least an annual basis, or more frequently where needs are indicated by heightened alert or service changes and improvement changes highlighted from their implementation. There should be a full live exercise held at least every three years (every year for ambulance services). This is to ensure that planning and existing training arrangements remain valid or to highlight changes that are needed or further training required. This is also necessary to ensure that there is still full commitment within the organisation and related agencies, to the plan.

11.7 Audit

Major Incident Plans should be subject to an external audit by the Health Emergency Planning Advisor (HEPA) or other suitably qualified person.

11.8 Facing the Challenge

A Report "*Facing the Challenge*", which was presented by the Comptroller and Auditor General to the House of Commons in November 2002, highlighted a number of deficiencies in major incident planning in NHS organisations, including:

– Many acute and ambulance trusts were shown to have deficiencies in their major incident planning and testing procedures, particularly relating to communications and the handling of the media and some were not well prepared for new or increased threats.

– Although many acute trusts had identified new or increased risks in relation to chemical, biological, radiological and nuclear emergencies and mass casualty incidents, few of them had revised their major incident plans or tested them in that regard.

– Need to improve inter-agency arrangements with neighbouring NHS trusts, other emergency services and managers of sites with the potential for mass casualty and chemical, biological, radiological and nuclear emergencies.

12. EXERCISING AND TESTING

12.1 Testing Business Continuity Plans

The contingency element of the business continuity plans should be tested at least annually. They should be maintained by regular reviews to ensure that they are up to date and effective and also to ensure that all members of the team undertaking the contingency and recovery (and other relevant staff) are aware of the plans. Testing should be scheduled and conducted in a way that does not put essential business functions of the organisation at risk. The testing methods should be practical, cost-effective and appropriate and designed to promote confidence.

The test schedule for a contingency plan should indicate how and when each element of the plan should be tested. It is recommended that specific components of the plan should be tested separately. Sometimes components of a plan fail, due to incorrect assumptions having been made, oversights, changes in services, systems, equipment, processes or personnel. The rate of organisational and technical change increases the vulnerability of such plans and leads to obsolescence.

12.2 Types of Testing

A variety of techniques should be used in order to provide assurance that a contingency plan will operate as required. The selected techniques should reflect the nature of the specific contingency plan. These techniques include:

a) tabletop testing of various scenarios, discussing the business recovery arrangements using examples of incidents;

b) simulations and walk-through, particularly for training people in their post-incident management roles;

c) technical recovery testing (both modular and full), ensuring equipment or systems (e.g. medical devices, information systems) can be restored effectively;

d) testing communications at least every six months including communications methods and equipment, including call-out procedures for key personnel;

e) testing recovery at an alternative site, running services, systems or business processes in parallel with recovery operations away from the main site;

f) tests of supplier facilities and services, ensuring externally provided services and products will meet the contracted commitment;

g) complete rehearsals announced and unannounced (presuming that it is safe for patients and staff to do so), testing that the organisation, personnel, equipment, facilities and business processes can cope with incidents.

12.3 Test Plan

Testing of technical equipment (e.g. systems) should not be undertaken without preparation. It is recommended that a Test Plan be drawn up at the outset. The time invested in planning for the technical testing of the recovery of equipment or system will be reflected in its operational running and therefore in the eventual cost of using it.

The test plan defines the details of the testing. The following should be defined in the test plan:

a) what is to be tested;

b) the software (and version) and equipment or hardware to be used for testing;

c) available technical documentation;

d) the frequency of testing and when it should be carried out;

e) the purpose of the testing and objectives;

f) how the testing will be carried out:

g) test control procedures (e.g. setting up);

h) scheduling of any "live" data to be used;

i) who should be involved to carry out the tests:

j) methods, techniques and tools required;

k) established test evaluation criteria and output results

l) test adjudication procedures;

m) any constraints in the test programme;

n) procedures for fault recording and follow-up.

12.4 Recovery Testing

Recovery testing is concerned with the testing of the procedures, both manual and system, for dealing with recovery from any incident, including service, process or technical problems. The recovery of any service or system to an acceptable operating level should be tested, including:

a) restoring integrity;

b) transition to and from the degraded state;

c) manual back-up procedures.

Recovery testing will follow contingency plan testing or implementation.

12.5 Developing Test Scenarios

Organisations need to create realistic scenario, which approximate to the types of incidents they may experience and the types of problems that are likely to be associated with those incidents.

12.6 Benefits of Exercising and Testing

The exercising and testing of business continuity plans provides benefits for both the organisation and all those involved, including:

a) a means of motivating staff and building their confidence;

b) an opportunity for assessing performance under controlled conditions;

c) an opportunity to assess likely impacts and review plans;

d) a chance to test changes to plans;

e) identification of training needs;

f) demonstrating the organisation's commitment for stakeholders.

13. IMPLEMENTATION OF THE BUSINESS CONTINUITY PLAN

13.1 Control and Co-ordination

Effective response to the implementation of one or more of business continuity plans requires a controlled and well co-ordinated approach. For if the interruptions to services, systems or business support is organisation-wide or over an extensive operational area, there may be several locations affected. In such larger incidents it may be appropriate for key personnel to report to one control point, located in a pre-arranged and advertised location (e.g. boardroom or training room), with one co-ordinator of the overall response.

Pre-arranged control points selected by NHS organisations need to be equipped with adequate and diverse means of communication and have access to essential services such as food, drink and toilets. Each organisation should select and equip a duplicate control point at another site or in a peripheral building, at least 1 kilometre from the main site, to address any issues of unavailability.

For major incidents NHS organisations need to understand that they may form just a part of a tiered response structure of which they do not hold the lead. NHS organisations or other agencies should establish their own tactical level of management for obtaining resources, determining priorities in their allocation, planning and co-ordinating tasks.

Initiation of the service continuity or IM&T continuity plans should be the responsibility of the Business Continuity Management Team and the Co-ordinator on their behalf. The first step should be, through consultation with relevant senior personnel and suppliers, to undertake an assessment of the probable nature of any incident and to determine the steps that should be taken to achieve recovery.

The Business Continuity Management Team should then take steps to oversee the management of the contingency and recovery efforts and facilitate support for the department(s) or business functions concerned and the restoration of "normal" services. Individual members of the Business Continuity Management Team may be involved with the implementation of contingency or recovery procedures for affected department(s) or business functions and take responsibility for any interfaces with other department(s) or business functions.

The Business Continuity Management Team should also take responsibility for any additional support (in the form of additional equipment and personnel or ancillary services), that may be needed from outside for affected department(s), business functions or the organisation. The Business Continuity Team, through its Co-ordinator, should remain "active" until any recovery is complete.

Such hierarchies are created for the purpose of achieving objectives and therefore are only temporary structures existing only for the duration of the emergency. Their composition does not fit comfortably with and may cut across existing line structures.

13.2 Communications

Good communications are the key to mounting an effective response to any incident, without them responding groups or individuals cannot work as teams. NHS organisations need to ensure there are robust and diverse means of communication, in case there are shortfalls within their existing communication systems e.g. because of the failure of electricity supplies and transport systems. Telephone switchboards within NHS organisations are often central to a planned response to a business failure. Wherever possible there should be limited back-up telephone switchboard facilities available off-site, at another site or in a peripheral building at least 1 kilometre from the main site.

Under emergency conditions, assuming total exchange line or switchboard failure there needs to be provision for direct dialling facilities, mobile telephones, and separate facsimile copier facilities. For GTPS subscribers there is national provision for maintaining outgoing call services for landlines and for incoming calls to be received, during major crises. For protecting communications by mobile telephone in such emergencies where cell phones become overloaded, there is a similar preference scheme in ACCOLC.

Email provides rapid communication facilities for disseminating information to a large number of individuals or organisations, using NHSnet and locally networked email systems. However NHS organisations and other agencies need to ensure that their systems are sufficiently robust and key staff adequately trained to use these facilities effectively under pressure.

Under some circumstances there may be a need to make use of radio communications. These can be provided by other participating services (e.g. ambulance services, local authority or police) or by RAYNET, a network of amateur radio enthusiasts who are widely acknowledged for their expertise and facilities. However, it is understood that the use of portable radios or mobile telephones may have an affect on the performance of some medical devices. Therefore NHS organisations are advised to use these with caution, particularly within hospital sites. The *Medical Devices Agency Bulletin 9702*, published in 1997, contains guidance on this matter.

Assuming the availability of telephone switchboard facilities when any elements of the Business Continuity Plan have to be initiated, it may be necessary to cascade alerting messages to key personnel and agencies. Telephone switchboard staff, because of their role within major incident plans, should already be trained in such duties under existing guidance, including undertaking such communications exercises every six months. However they will need to be provided with all the information they need to undertake this, including key contact details and the nature of messages.

To augment such limited facilities and avoid overloading them, organisations should consider making use of "snowball" callout systems, whereby contacted staff or users contact others in a prescribed fashion. Organisations should also consider using written communications delivered by hand and messages broadcast by personal delivery and loudhailer. These may be perfectly adequate for internal needs.

Once facts about service, system or business support failures have been verified, there will be a need to use available communications media to inform affected departments or business functions, their personnel and patients etc, with accurate information, put across, wherever possible, in a positive way. This action, which should be undertaken by a specified member of the Business Continuity Management Team, should help to offset misinformation and rumour.

13.3 Public Relations and Media

Some of the disruption arising from service interruptions and failures, particularly where they take the form of major incidents, may attract media interest of a local, national or international scale. NHS organisations so affected have a responsibility for providing timely, accurate information at suitably frequent intervals and therefore it is recommended that a member of the Business Continuity Planning team be given responsibility for handling all aspects of public relations. This will avoid conflicting messages being issued, ensure that there is a reliable source of information for patients and the public whilst allowing the organisation involved to concentrate on the core business of providing contingency and recovery.

Other ways of providing information to patients and the public include help lines giving recorded messages or answers to questions from a set script. These may be provided through the Department of Health's information service or through local NHS Direct centres. This can be used to divert enquiries away from overburdened telephone switchboards.

14. SUPPLIES OF EQUIPMENT, GOODS AND SERVICES

14.1 Introduction

NHS organisations need to have specific procedures within their contingency plans for dealing with failures in equipment, shortages of supplies or the need for additional services, where the risk is considered critical or significant. Chief Executives of NHS organisations are ultimately responsible for ensuring the continuity of supply of essential goods and services in the lead up to and over the period of contingency and recovery.

Existing guidance advises that NHS organisations should not, unless otherwise specifically advised by the Department of Health, stockpile to levels exceeding their historic demand pattern over the previous 12 months by 10% or more. Instead NHS organisations should work collaboratively with NHS Supplies and its contracted suppliers to ensure more objective ways of ensuring the availability of essential supplies.

14.2 Consumables

NHS organisations on average hold about two weeks stock of consumable products, which will usually be adequate for dealing with any occurrence falling within the scope of local major incident, service continuity and IM&T continuity plans. The emergency service provided by NHS Logistics also enables delivery of consumable products within a maximum of five hours should shortages occurs. For mass casualty incidents however it would not be appropriate to expect local NHS facilities to hold the level, or necessarily the type, of stocks necessary for dealing with such events and the Department of Health have established national reserve stocks for this purpose.

14.3 Equipment

There may be circumstances arising from a contingency when equipment needs replacing at short notice and the question arises whether purchases can be made without recourse to the normal rules of public procurement. Current guidance is that where the value of a contract for services or goods is likely to exceed the current threshold then procedures laid down in the EU Directive must still be followed.

Where the value does not exceed the threshold the organisation's Standing Financial Instructions should be used and adhered to. It is for each NHS organisation to decide if the case for the waiving of Standing Financial Instructions or for single tender action is sufficiently compelling.

14.4 Utilities

As far as possible the disruption in provision of gas should be minimised by the priority status agreed for eligible NHS sites over the millennium period. That effectively means that in the unlikely event of supply reductions registered sites would be the last to be affected and the first to be reconnected when supplies resume. These sites were registered with the Department of Trade and Industry and suppliers through NHS Supplies with whom details should be checked. (Reference: *Silver Bullet March 1999*)

There is not a scheme currently for assuring priority status for electricity supplies for NHS organisations. Regional Electricity Companies do maintain lists of protected sites, but not for sites that have emergency generator facilities such as NHS hospital trusts.

For other supplies, such as oil and water, having suitably large reserves on site can ease the threat of disruption.

14.5 Fuel

There are no formal mechanisms for ensuring that NHS organisations or their essential employees have access to priority fuel supplies in the event of fuel supply shortages. *HSC 1999/129* issued in March 1999 suggests that NHS organisations consider making arrangements for priority supply with local fuel filling stations. That is unless they have opportunities to secure or hold stocks themselves, commensurate with appropriate safety legislation, or have access to fuel stocks held by other NHS organisations in an emergency.

15. EDUCATION AND TRAINING

15.1 Introduction

The successful development and where necessary, implementation of business continuity plans is dependent upon a continuity culture being embedded throughout the organisation. Any incident, but particularly major incidents, can place heavy demands on NHS organisations and may involve individuals working in unfamiliar roles and environment. The personnel of those organisations and others involved need to develop confidence in their ability to manage after an incident and their competence in using contingency and recovery plans. So training, testing and exercising are essential elements in any organisation, in order for staff to become suitably prepared to deal with any incident. Such training involves ensuring that staff have the right skills and knowledge to undertake the roles expected of them following any incident. It should be aimed at familiarising all relevant staff and other stakeholders with any special equipment or systems. Those skills and knowledge should be tested by appropriate exercises.

Assessing such training needs forms part of an ongoing cycle of quality improvement. Therefore, it is essential to assess the skills of individuals who plan for or respond to any incident and whether they have the required skills. Organisations need a carefully planned and delivered incident training programme so that staff and other stakeholders understand their roles and the roles of others. Also they need to understand the systems and procedures for each continuity plan, how available accommodation should be utilised and where equipment is kept and how to use it. There must be a justified expectation of being able to perform to an agreed standard and this implies undertaking the necessary preparations

15.2 Developing training programmes

Training for ensuring business continuity will involve a significant investment in time and other resources. Therefore individual organisations need to ensure that they fully realise the benefits from such investment. That can be achieved by ensuring that staff and other stakeholders know what to do and how to do it, that training is planned and managed efficiently and effectively. If training is poorly targeted or badly executed, that investment may not be realised. Therefore the following should be considered when developing business continuity training programmes:

a) identifying those staff and other stakeholders who require training;
b) identifying their training needs and the content of that training;
c) prioritising those training needs;
d) identifying appropriate and available methods for providing that training;
e) making provision for new personnel to have their part in business continuity plans explained as part of their induction programme;
f) updating training in the light of needs created by organisational changes, outcomes of testing or exercises, identifying new causes of incidents or other changes.

15.3 Skill /knowledge levels

The NHS Information Authority's Ways of Working with Information Programme promotes *Health Informatics Competency Profiles for the NHS (2001)*, which identify the need for a range of skills and knowledge levels. Those profiles represent national guidance to assist local implementation in a framework of national consistency. Included within these competency profiles are specific recommendations, which can be used as the basis for determining the scope and content of a generic awareness training programme for all staff groups within NHS organisations.

Expert	Full skills and knowledge required by staff who need the ability to deal with all aspects of business continuity
Advanced	Specialist skills and knowledge required on business continuity in order to carry out their role without specialist support or supervision
Intermediate	Moderate skills and knowledge of business continuity required to be used with specialist support or supervision
Basic	Basic awareness of business continuity with few basic skills required

15.4 Evaluation

Evaluating the training provided, on an ongoing basis, is an important tool to ensure that the approach taken and that the training content is currently valid and useful. This ensures that the energy and investment in the training has a real "pay-off" for the organisation.

Training can be evaluated in a number of ways and at different levels, including:

a) the reaction of individual participants following training;
b) the effect the participants learning has on departmental plans and preparations;
c) the performance of departments and individuals in exercising and testing.

16. HUMAN RESOURCES

16.1 Introduction

Human resources constitute one of the main dependencies for addressing the effects of service interruptions and failures upon the services, systems and business processes used by NHS organisations. There therefore need to be robust plans to ensure their timely availability and deployment. However there can be no single model for dealing with the range of possible incidents that NHS organisations may face and need to respond to, therefore it is essential that plans for the engagement and deployment of human resources remain suitably flexible to meet a range of options.

16.2 Policies

NHS organisations need their human resource policies to reflect the flexible deployment of their staff and agreements with other organisations for support, in the event of and for the duration of, an adverse event or incident. These policies should include:

a) undertaking skills audits to identify staff who have the capability of working outside of their current disciplines or flexibly across disciplines;

b) assessing the training needs those staff may have;

c) assessing the impact upon their existing roles;

d) arrangements for time off in lieu or compensation for staff involved with contingency and recovery;

e) arrangements for flexibility over annual leave to allow staff involved with contingency and recovery to carry-over accrued leave from one year to the next if necessary;

f) agreements with other NHS organisations for staff support e.g. staff from primary care trusts and mental health trusts providing support for acute trusts.

16.3 Former staff

NHS organisations should also consider putting into place plans to maximise the contribution of former staff. These could include those staff nearing retirement that would be willing to defer their retirement. The plans could also include staff who have recently retired and who are willing to be available for periodic training to update their skills and to be recalled, in the event of and for the duration of, an adverse event or incident.

16.4 Voluntary sector

Agreements may be made with voluntary organisations to support the services provided by NHS organisations in the event of and for the duration of, an adverse event or incident. Persons provided from outside organisations should be subject to the same security checks and confidentiality requirements as regular staff.

17. RECORDS AND ARCHIVING

17.1 Introduction

Ensuring the continuity of critical operational services, continued functioning of IM&T systems and the integrity of essential supporting business processes, within NHS organisations, is dependent upon the availability of records. A record, in this context, is anything that contains information, which has been created or gathered as a result of any NHS activity, whether clinical or non-clinical, by employees - including consultants, agency, contractor or casual staff. Such records may be held in any media, e.g. paper, microfiche, audio or videotapes, X-ray images, computer database, notes, email etc.

All NHS records are public records under the terms of the Public Records Act 1958 (as amended 1967). Chief Executives and senior managers of all NHS bodies are personally accountable for records management within their organisation and have a duty to make arrangements for the safekeeping of those records under the overall supervision of the Keeper of Public Records.

The storage of personal data in structured systems (manual or electronic) is also subject to the provisions of the Data Protection Act 1998. Because of the subject rights of access to information, NHS organisations must be in a position to produce the information requested within prescribed time-scales (20-40 days) or risk incurring fines or other penalties.

Such records may also be needed to allow an NHS organisation to prepare its defence against claims for alleged negligence. The Limitation Act 1980 defines statutory periods within which legal action for personal injury may be brought, although these periods run from the date of discovery of an injury, which could be many years after.

There may also be clinical reasons for preserving records beyond these limits. Clinicians may recommend that some or all of patient records should be kept for longer than the minimum periods for clinical reference in the event of the patient re-attending. Some clinicians may want every record to be kept until the patient is known to have died. In some specialities, professional bodies have published advice on clinical criteria for record retention e.g. *The retention of medical records with particular reference to medical genetics* published by the Clinical Genetics Committee of the Royal College of Physicians (RCP) in 1998.

17.2 Records Management

Records management is a corporate function and responsibilities for it must be clearly defined and assigned and made known throughout the organisation. NHS organisations need to ensure they have a Records Manager, not just medical records, in place.

According to *HSC 1999/053* all NHS organisations should have drawn up and agreed an organisational records management strategy by April 2001, for which implementation should have been well in hand by April 2002. A model framework is set out in the Public Record Office document *Records Management: Human Resources (1999)*. That strategy should have identified the resources needed to ensure that records of all types are properly controlled, trackable, readily accessible and available for use, and eventually archived or otherwise disposed of.

NHS organisations are also held accountable, through clinical governance procedures, for the storage and retrieval of personal information. Therefore, the organisation's 'Caldicott Guardian' is ideally the board member who should be responsible for approving and ensuring the business continuity plans for handling the management, archiving and back-up of confidential personal information held in records of all types.

17.3 Records Storage

Records management strategies should address the need for appropriate physical storage conditions and handling processes for records. These should take into account the specific physical and chemical properties of such records and the need to protect them from unauthorised access, loss or destruction and from theft and disasters such as fire, flood and other risks.

Decisions should be made on appropriate storage conditions for ensuring records are properly managed, protected and accessible to authorised users. Such conditions can be determined by conducting risk analysis to determine storage and handling options, taking into account:

a) the volume of records and growth rate;
b) usage;
c) security requirements;
d) access and retrieval requirements;
e) costs of storage options;
f) retention requirements.

Special consideration should be given to records that are particularly critical for business continuity. They may require to be given additional protection, even duplication, to ensure their accessibility in the event of an incident or disaster.

17.4 Electronic Records

Building the Information Core: Implementing the NHS Plan (Department of Health: 2001) set out detail on how the NHS Plan and the information strategy for the NHS was to be taken forward. The Department of Health's National Strategic Programme for *Delivering 21st Century IT Support for the NHS* (2002) provides the shift to more corporate, national approaches towards the Electronic Staff Record and Health Records Infrastructure.

The National Strategic Programme also proposes an initial review of the application of electronic records, including the update of the Electronic Patient Record (EPR) and the Electronic Health Record (EHR). It also addresses the requirements for an Integrated Care Records Service (ICRS) to support the provision of care to the standards set out in the National Service Frameworks for Cancer, Diabetes, Mental Health and Older People. These developments impose the need to ensure that the long-term record is preserved either in electronic format or by transferring to another medium (usually paper or microfilm).

17.5 Safeguarding Electronic Media

To safeguard business activities it is important to maintain the integrity and availability of essential data and information stored on electronic media. It is important to ensure that each item can be positively identified, is logged correctly and is held securely. Back-up data should be held in separate locations to the systems they back-up and at very least in fireproof storage. However, such back-up media may still deteriorate quickly and therefore needs to be refreshed periodically.

The longer term storage requirements of critical data need to be checked, for while such data on electronic media may be held securely, they may be kept in unsuitable storage or operating environments, where they may suffer extensive damage. There needs to be careful control and monitoring of the temperature, relative humidity and ventilation in storage areas and regular maintenance of heating and ventilation systems. The table below shows temperatures and relative humidity (RH).

Specialist advice on the preservation of electronic records is provided in guidelines issued by the Government's Public Record Office *Management, Appraisal and Preservation of Electronic Records,* Volume 2, Section 5 (1999).

Device	Operating	Non-operating	Long term
Magnetic tape reel 12.7 mm	18 to 24oC 40 to 60% RH	5 to 32oC 20 to 80% RH	18 to 22oC 35 to 45% RH
Magnetic tape cassettes 12.7 mm	18 to 24oC 45 to 55% RH	5 to 32oC 5 to 80% RH	18 to 22oC 35 to 45% RH
Magnetic tape cartridges	10 to 45oC 20 to 80% RH	5 to 45oC 20 to 80% RH	18 to 22oC 35 to 45% RH
Magnetic tape - 4 & 8 mm helical scan	5 to 45oC 20 to 80% RH	5 to 45oC 20 to 80% RH	5 to 32oC 20 to 60% RH
Optical disk Cartridges (ODC)	10 to 50oC 18 to 80% RH	-10 to 50oC 5 to 90% RH	18 to 22oC 35 to 45% RH
CD-ROM	10 to 50oC 10 to 80% RH	-10 to 50oC 5 to 90% RH	18 to 22oC 35 to 45% RH

17.6 Safeguarding of Organisational Electronic Records

The Trust's important electronic business records should be protected from loss, destruction and falsification. Some of them (e.g. financial records) may need to be securely retained to meet statutory or regulatory requirements, as well as to support essential business activities. Examples of this are records that may be required as evidence that an organisation operates within statutory or regulatory rules or to ensure adequate defence against potential civil or criminal action or to satisfy auditors. The time period and data content for retention of such electronic records may be set by national law or regulation under the terms of the Public Records Acts of 1958 and 1967.

Records should be categorised into record types, e.g. accounting records, database records, transaction logs, audit logs and operational procedures, each with details of retention periods and type of storage media, e.g. paper, microfiche, magnetic or optical. Any related cryptographic keys associated with encrypted archives or digital signatures should be kept securely and made available to authorised persons when needed.

17.7 Safeguarding of Electronic Patient Records

When patient data is held in electronic format, the storage of it can be threatened by issues of stability and integrity. Data can disappear or the ability to read and understand them can be lost. Electronic media such as magnetic tapes, diskettes and hard disks can break, be destroyed, get lost or simply deteriorate. There is, as yet, little experience of their durability. Therefore, when data are kept for a long time, they should be copied to new media at intervals.

However, merely retaining the media does not guarantee that the data will be available when required. As computer hardware and software are upgraded, older, yet still-functioning media cannot automatically be used with current hardware or software and therefore it may no longer be possible to read the stored data. With the development of technology, trusts must be prepared to transfer old data to new media, whenever necessary. Data structures must also be converted or else unstructured data must be used.

Electronic patient documents must be available throughout their whole life cycle and future defence in law may depend on establishing both that there were clear policies on electronic records management in force, and that the hardware and software were operating correctly. Guidance is available from PD 0008:1999: *Code of practice for legal admissibility and evidential weight of information stored electronically* (1999) and its associated compliance handbook issued by the British Standards Institute. Also an ISO standard is in preparation that will provide guidelines for managing this task.

Where electronic patient records are stored permanently on magnetic tape, cassette or optical disks, the data should be recorded in two copies, preferably on different media and they should be physically stored in two different locations.

17.8 Archiving of records

Less frequently used or archived records should be moved to more effective and space efficient storage options:

a) mobile racking and warehouse-type units;

b) off-site secure storage and retrieval services;

c) microfilm, microfiche and digital scanners to capture and store images;

d) picture archiving for diagnostic imaging.

However, retrieval arrangements should be agreed before archiving. Contracts for non-NHS agencies or staff must require that patient information is stored and retrieved according to specified security and confidentiality standards and Data Protection guidelines.

If any records are to be kept for more than 30 years after the last date on which the records were active, the Public Records Acts 1958 and 1967 require that approval be sought from the Keeper of Public Records. Those records and records identified for permanent preservation must be stored within "places of deposit" approved by the National Archive (formerly Public Record Office).

17.9 Freedom of Information Act 2000

The Freedom of Information Act (November 2000) gives a general right of access to all types of recorded information held by public authorities, including NHS organisations, with full access from January 2005. The Act provides some exemptions to that right, but in the main places obligations on public authorities.

The National Archive (formerly Public Records Office) issued in October 2002 a *Model Action Plan for Developing Records Management Compliant with the Lord Chancellor's Code of Practice under section 46 of the Freedom of Information Act 2000.* That Model Action Plan for Health Authorities sets out practices on the review and transfer of public records to places of deposit. Storage areas will need to be secure and free from damp, high humidity and temperature fluctuations. Full recommendations are given in the British Standard BS5454: *Recommendations for Storage and Exhibition of Archival Documents* (2000).

NHS organisations need to take cognisance of these practices when formulating their business continuity plans and ensure compliance before full access rights come into force in January 2005. Under the Model Action Plan NHS organisations have until 30th June 2004 to ensure that they have a business recovery plan in place for records management.

18. COMPLIANCE

18.1 Compliance with Legal Requirements

It is essential that the organisation avoid any breaches of any criminal and civil law, statutory, regulatory or contractual obligations. The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements. Advice on specific legal requirements should be sought from the organisation's legal advisers, however these do include the following mentioned in this guidance:

Public Records Acts 1958;
National Health Service Act 1977;
Limitations Act 1980;
Copyright, Designs and Patents Act 1988;
Data Protection Act 1998;
Freedom of Information Act 2000;
Health and Social Care Act 2001.

18.2 Identification of Applicable Legislation

All relevant statutory, regulatory and contractual requirements that NHS organisations and their employees are required to observe should be explicitly defined and documented for each plan. The specific controls and individual responsibilities to meet these requirements should be similarly defined and documented.

18.3 Clinical Negligence

NHS organisations are advised to consider the effects that reductions in service provision arising from major incidents, service interruptions and failures will have on their membership of the Clinical Negligence Scheme for Trusts (CNST) and to take account of service continuity contingency and recovery plans in their clinical risk assessment.

18.4 Departmental Requirements - Service Continuity

Department of Health requirements and guidance on the role of Chief Executives of NHS Organisations in assuring the operational continuity of services, including:

HSC 1998/091	Operational Continuity of Primary Care Services- The Year 2000 Problem.
HSC 2001/014	Arrangements for Whole System Capacity (Emergency, Elective and Social Care).

18.5 Departmental Requirements - Major Incidents

Department of Health requirements and guidance on the role of Chief Executives of NHS Organisations in planning for major incidents includes:

HSC 1998/197 Planning for Major Incidents (1998);
Emergency Care Strategy Team (2000);
Emergency Planning: UK Reserve National Stock for Major Incidents (2001);
Primary CareTrust Functions (Amendment) Regulations (2002);
Primary Care Trusts: Emergency Planning Function (2002).

18.6 Standards

There are a number of UK and International standards relevant to business continuity, including:

BS 4783 Storage, transportation and maintenance of media for use in data processing and information storage, 1988-94 (See Section 7.4 on the safeguarding of organisational records);

BS 5454 Recommendations for the storage and exhibition of archival documents;

BS 5588 Fire precautions in the design and construction of buildings, 1983 (amended 1989);

BS 5839 Fire detection and alarm systems in buildings, 1983-95;

BS 6266 Code of practice for fire protection for electronic data processing installations, 1992;

BS 7083 Computer rooms - guide for accommodation and operating environment of information technology equipment, 1989;

BS 7799 Code of Practice for Information Security Management.

18.7 Policy and Guidance

There are a number of NHS guidance documents relevant to business continuity, contingency and recovery, including:

Caldicott Report (1998);

For the Record: Managing Records in NHS Trusts and Health Authorities (1999).

19. MAINTENANCE AND REVIEW OF PLANS

19.1 The Master Plan

It is recommended that an appropriate responsible person, who would normally be the Business Continuity Planning Team's Co-ordinator, hold one master set of the business continuity plans. The master set should include the framework and all the contingency and recovery plans based on the framework. Copies of the master plan should also be kept for back-up purposes. These copies should also be under the control of the co-ordinator and held securely in a peripheral building and off-site location.

19.2 Other Copy Plans

There should be multiple, controlled copies of all contingency and recovery plans. These should be held securely by named responsible individuals in widely diverse locations, including off-site. That may include some individuals keeping copies at their homes while other copies will be held at stand-by and back-up locations. The purpose of this is to ensure that at least one copy will be available at short notice even if a major disaster strikes the organisation's main buildings.

The Business Continuity Planning Team's Co-ordinator will keep a record of where each copy plan is held and who is responsible for it. Plans should only be issued when they are relevant to the holder. There is no need for every holder to keep a copy of every contingency and recovery plan in use.

19.3 Identifying the Plans

Each copy of each planning document i.e. framework, contingency or recovery plan should carry an issuing number and be marked with the version number and date. A table should be provided in each plan to show when each version came into effect and the reason for the change from the previous version.

19.4 Updating the Plans

Changes will be required whenever a review or a test shows that the existing plan is defective or when changes in the environment necessitate a change in the plans. The Business Continuity Planning Team's Co-ordinator should initiate the changes using standard change control procedures. The master plan (including back-up copy) should be changed first, then the copies of individual plans by the co-ordinator issuing the holders with amended sheets as necessary, together with a new header page (complete with version number) and an updated table detailing the changes made. The holder should then be responsible for inserting the corrected sheets into each plan that he holds. This should be done as soon as possible after receiving the updates. The co-ordinator should record the updates issued together with the name of the holder.

APPENDIX A - SOURCES OF FURTHER INFORMATION

Information Security Policy Guidance

Alistair Donaldson
NHS Security Policy & Standards Manager
Department of Health
Information Policy Unit
Room 1N35A
Quarry House
Quarry Hill
Leeds LS2 7UE
Tel: 0113-254-6231
Fax: 0113-254-6015
Email: alistair.donaldson@doh.gsi.gov.uk
Website: www.doh.gov.uk/ipu/security/

Business Continuity/National Lead NHS BS 7799 Programme

Tom Lillywhite
National Security Risk Manager
NHS Information Authority
1st Floor, Block B
Tavistock House
Tavistock Square
London
WC1H 9HR
Tel: 020 7391 8000
Fax: 020 7388 6511
Email: tom.lillywhite@nhsia.nhs.uk

NHS Information Authority Helpdesk

Security and Data Protection Helpdesk
NHS Information Authority
Aqueous II
Aston Business Park
Rocky Lane
Birmingham B6 5RQ
Tel: 0121 333 0420
Fax: 0121 333 0421
Email: helpdesk3@nhsia.nhs.uk
Website: www.nhsia/nhs.uk or nww.nhsia.nhs.uk

European Standards information

European Committee for Standardisation (CEN)
CEN TC 251/WG III
Central Secretariat
Rue de Stassart 36
B-1050
Brussels
Website: www.centc251.org

International Standards information

International Standards Organisation (ISO)
ISO/TC 215 WG4
Secretariat
ANSI (ASTM)
100 Barr Harbor Drive
West Conshohocken
PA
19428
Website: www.medis.or.jp/iso/tc215wg4.html

British Standards information

British Standards Institution
389 Chiswick High Road
London
W4 4AL
Tel: 0181 996 9000
Fax: 0181 996 7448
Website: www.bsi.org.uk

Business Continuity Information

The Business Continuity Institute
PO Box 4474
Worcester
WR6 54A
Email: TheBCI@btinternet.com

Survive!
107-111, Fleet Street
London
EC4A 2AB
Switchboard: 020 7936 9026
Fax: 020 7936 9126
Email: survive@survive.com
www.survive.com

APPENDIX B - ABBREVIATIONS

ACCOLC	Access Overload Control
A&E	Accident and Emergency
ANSI	American National Standards Institute
AS/NZS	Australian & New Zealand Standard
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BS	British Standard
BSI	British Standards Institute
BSI-DISC	BSI unit for Delivering Information Solutions to Customers (which ceased to exist from the end of 2002).
C	Centigrade
CASU	Controls Assurance Support Unit
CBRN	Chemical, Biological, Radiological or Nuclear
CCTA	Central Computer & Telecommunications Agency
CD	Compact Disc
CD-ROM	Compact Disc - Read Only Memory
CEN	European Committee for Standardisation
CEO	Chief Executive Officer
CNST	Clinical Negligence Scheme for Trusts
COACH	Canadian Organisation for Advancement of Computers in Health
CRAMM	CCTA's Risk Assessment Management Methodology
DB	Device Bulletin
DH	Department of Health
DPA	Data Protection Act
DTI	Department of Trade and Industry
EHR	Electronic Health Record
EPR	Electronic Patient Record
EU	European Union

GMITS	Guidelines for the Management for IT Security
GPKA	Government Public Key Authority
GTPS	Government Telephone Preference Scheme
HEPA	Health Emergency Planning Advisor
HIMP	Health Improvement and Modernisation Plan
HL7	Health Level 7
HM	Her Majesty's
HO	Home Office
HMSO	Her Majesty's Stationery Office
HSC	Health Services Circular
ICA	Institute of Chartered Accountants
ICRS	Integrated Care Records Service
IEC	International Electro-technical Commission
IMG	Information Management Group (now NHSIA)
IM&T	Information Management and Technology
ISBN	International Standard Book Number
ISO	International Standards Organisation
IT	Information Technology
JHAC	Joint Health Advisory Cell
LAN	Local Area Network
LIS	Local Implementation Strategy
LSE	London Stock Exchange
MDA	Medical Devices Agency
mm	Millimetre
NHS	National Health Service
NHSIA	National Health Service Information Authority
NHSLA	National Health Service Litigation Authority
ODC	Optical Disk Cartridges
PCT	Primary Care Trust

PD	Published Document
PHLS	Public Health Laboratory Service (now Health Protection Agency)
PID	Project Initiation Document
PRINCE	Projects IN Controlled Environments
PRO	Public Records Office (now National Archive)
RAYNET	Radio Amateurs Emergency Network
RCP	Royal College of Physicians
RH	Relative Humidity
TC	Technical Committee
UK	United Kingdom
WAN	Wide Area Network
WG	Working Group

APPENDIX C - GLOSSARY

Term	Definition	Reference
Agency	Any government department, authority or other body, established in relation to public purposes.	GPKA
Algorithm	A set of rules which if followed, will give a prescribed result.	
Archive	To store back-up files and any associated journals, usually for a given period of time.	ISO/IEC 2382-08
Asset	Anything that has value to the organisation.	GMITS Part I ref. [31]
Audit	An (external) investigation to determine compliance to specifications, standards and pre-determined agreements.	ISO/IEC 2382-08
Authentication	The act of verifying the claimed identity of an entity.	ISO/IEC 2382-08
Availability	Ensuring that authorised users have access to information and associated assets when required.	ISO/IEC 17799
Back-up Procedure	A procedure to provide for data restoration in case of a failure or disaster.	ISO/IEC 2382-08
Business Impact Analysis	The process of analysing business functions and the effect that specific types of disruption may have upon them	
Business Processes	Series of operations or courses of action, undertaken by, or on behalf of an organisation and linked to its objectives.	
Change Control	Assessing the impact of potential changes, their importance and affects, and therefore determines whether to authorise them for incorporation.	
Clinical Governance	A framework through which NHS organisations are accountable for continuously improving the quality of their services and safeguarding high standards of care by creating an environment in which excellence in clinical care will flourish.	Department of Health "A First Class Service" 1998
Confidentiality	Ensuring that information is accessible only to those authorised to have access.	ISO/IEC 17799
Consequence	The outcome of an event expressed qualitatively or quantitatively.	
Contingency	an unexpected event, which threatens to disrupt the continuity of normal business activities.	
Contingency Plan	A planned course of action to be followed after an unexpected event, which threatens to disrupt the continuity of normal business activities.	
Continuity	Maintained without interruption.	
Corporate Governance	The systems and processes by which health bodies lead, direct and control their functions, in order to achieve their organisational objectives, and by which they relate to their partners and the wider community	Audit Commission
Criticality	The degree of importance assigned.	
Data	A representation of facts, concepts or instructions in a suitable manner for communication, interpretation or processing.	COACH

Destruction	The process of rendering an asset completely unusable	COACH
Disaster	Accidental, natural or malicious events, which threaten or disrupt normal operations or services for sufficient time to have significant effects on the organisation's business.	
Events	Incidents or situations, occurring in particular places during particular intervals of time.	
Frequencies	Measures of rates of occurrence.	
Hardware	Physical equipment used to process, store or transit computer programs or data.	COACH
Horizon scanning	The systematic examination of potential threats, opportunities and likely future developments, which are at the margins of current thinking and planning.	
Impact	The result of an unwanted incident. The embarrassment, harm, financial loss, legal or other damage which could occur in consequence to a particular security breach.	GMITS Part I ref. [3] CEN/HL7
Incident	Any event which may be, or lead to a disaster	
Information	The meaning that humans assign to data by means of known conventions that are applied to the data.	COACH
Information Security	Preservation of confidentiality, integrity and availability of information.	ISO/IEC 17799
Integrity	Safeguarding the accuracy and completeness of data and information and processing methods.	ISO/IEC 17799
Interruption	Act that prevents an authorised service or activity from proceeding to specification.	
Likelihood	Qualitative description of probability or frequency.	
Loss	A negative consequence, financial or otherwise.	AS/NZS 4360:1999
Major Incident	Any occurrence which presents a serious threat to the health of the community, disruption to the service or is likely to cause such numbers or types of casualties as to require special arrangements to be implemented by hospitals, ambulance services or health authorities.	Department of Health
Monitoring	Checking, supervising, observing critically or recording the progress of an activity, action or system on a regular basis, in order to identify change.	AS/NZS 4360:1999 (adapted)
Patient	An individual who receives a health product or service from a healthcare provider or health service enterprise.	COACH
Principal Risk	Those risks which impact on the achievement of an organisation's core objectives.	
Probability	The likelihood of a specific event or outcome.	
Project Initiation Document	A logical document, the purpose of which is to bring together the key information needed to start a project on a sound basis and to convey that information to all concerned within a project.	PRINCE 2

Records	Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business	BS/ISO 15489:2001
Records Management	Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.	BS/ISO 15489:2001
Recovery	The restoration of an information system back to an error free and secure state from which normal operation can resume.	CEN
Recovery Plans	Formulated method for achieving the full restoration of services within a pre-determined timeframe	
Repudiation	The denial by a message sender that the message was sent, or by a message recipient that the message was received.	HL7
Residual risk	The remaining level of risk after controls or risk treatment measures have been applied.	
Risk	An assessment of the probable impact on an asset by a particular threat exploiting a particular vulnerability. This can be viewed as: Risk = Impact x Threat x Vulnerability	ISO/IEC 2382-08
Risk acceptance	A managerial decision to accept a certain degree of risk, usually for technical or cost reasons.	ISO/IEC 2382-08
Risk Analysis	Involves the identification and assessment of risk against assets.	
Risk Assessment	Assessment of threats, impacts and vulnerabilities on organisational services and assets to enable measures to be taken to reduce the identified risks.	
Risk Management	The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects	
Risk Register	A management tool that enables an organisation to understand its comprehensive risk profile.	CASU
Safety	Freedom from unacceptable risk.	IEC: 1998
Service continuity	The management of risks to ensure that at all times and circumstances an organisation can continue to operate core services to, at least, a minimum pre-determined level.	
Services	Actions taken and/or resource provided in response to a specific identified demand or need.	
Software	Computer programs, procedures, associated documentation and data pertaining to the operation of a computer system.	COACH
Standards	Documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines, or definitions of characteristics to ensure that materials, products, processes and services are fit for their purposes.	ISO/IEC 2382-08: 1996

Stakeholders	People or organisations who may affect, or be affected by, or perceive themselves to be affected by, a decision or activity.	AS/NZS 4360:1999
Strategic risk	Match between an organisation's vision and strategic objectives with current and future operational constraints.	
Threat	A potential cause of an unwanted incident, which may result in harm to a system or organisation.	ISO 7498-2: 1989 GMITS Part I ref. [3]
Utilities	Companies providing essential services e.g. electricity, gas, and water.	Home Office
Vulnerability	A weakness of an asset or group of assets, which can be exploited by a threat.	GMITS Part 1 ref. [3]

APPENDIX D - REFERENCES

Source	Reference	Title	Year
DoH		Report on the Review of Patient-Identifiable Information (Caldicott Report)	1997
NHSE	HSC 1998/091	Operational Continuity of Primary Care Services -The Year 2000 Problem	1998
NHSE	HSC 1998/153	Using Electronic Patient Records in Hospitals: Legal requirements and good practice	1998
NHSE	HSC 1998/168	Information for Health: An Information Strategy for the Modern NHS	1998
NHSE	HSC 1998/197	Planning for Major Incidents: Fully revised and updated guidance	1998
NHSE	HSC 1998/225	Information for Health: Initial local implementation strategies	1998
NHSE	IMG E5519	The Silver Bullet Supplies Special : Number 1	
NHSE		Planning for Major Incidents	
NHSE	IMG E5498	Ensuring Security and Confidentiality in NHS Organisations	1999
NHSE	IMG E5572	Year 2000 Bulletin No.3	1999
NHSE	HSC 1999/012	Caldicott Guardians	1999
NHSE	HSC 1999/026	Year 2000 Problem: NHS Supplies Year 2000 Supply Chain Assurance Scheme	1999
DoH	HSC 1999/053	For the Record: Managing records in NHS Trusts and Health Authorities	1999
NHSE	HSC 1999/065	Clinical Governance: in the new NHS	1999
NHSE	HSC 1999/123	Governance in the New NHS: Controls assurance statements 1999/2000	1999
NHSE	HSC 1999/129	The Year 2000 Problem: Utilities provision over the millennium period	1999
NHSE	HSC 1999/192	Leadership for Health: The Health Authority Role	1999
NHSE	HSC 1999/200	Information for Health: Full local implementation strategies	1999
NHSE	HSC 2000/009	Data Protection Act 1998: Protection and Use of Patient Information	2000
DoH		Emergency Care Strategy Team	2000
DoH		The NHS Plan: A plan for Investment, A plan for Reform	2000
NHSE	HSC 2001/005	Governance in the New NHS: Controls assurance statements 2000/2001 and establishment of Controls assurance Support Unit	2001
DoH	HSC 2001/014	2001/2002: Arrangements for Whole System Capacity (Emergency, Elective and Social Care)	2001
DoH		Emergency Planning	2001
DoH		Emergency Planning: UK Reserve National Stock for Major Incidents	2001
DoH		Building the Information Core: Implementing the NHS Plan	2001
DoH		Health Improvement and Modernisation Plans (HIMPs) Requirements for 2002	2001
DoH		Emergency Planning and response to Major Incidents	2002
DoH		Emergency Planning: Management of equipment and Modesty Pods as part of the UK Reserve National Stock for Major incidents	2002
DoH		The New NHS	2002
DoH		Shifting the Balance of Power: The Next Steps	2002
DoH		Building the Information Core: Implementing the NHS Plan An Information Toolkit to support Local Implementation Strategies (LIS) for 2002/03	2002

Source	Reference	Title	Year
DoH		Delivering 21st Century IT Support for the NHS: National Strategic Programme	2002
DoH		Fire Service Industrial Action - Action to be taken by NHS Trusts	2002
DoH		Primary Care Trusts: Emergency Planning Function	2002
DoH		Planning for Major Incidents: Process over next 3 months	2003
NHS Estates		NHS Preparedness for Floods	2002
NHSIA		ACCess OverLoad Control for Cellular Radio Systems	2002
NHSIA	649/743	NHS ISO/IEC 17799 Toolkit (Version 2.1)	2001
NHSIA	2001-IA-511	Health Informatics Competency Profiles for the NHS	2001
NHSLA		CNST Clinical Risk Management Standards	2002
NHSLA		Risk Pooling Schemes for Trusts	2002
HMSO		Facing the Challenge: NHS Emergency Planning in England	2002
HO		Business as Usual - Handbook for Managers	1999
HO		The Exercise Planners Guide	1999
HO		How Resilient is your business to disaster?	2000
HO		UK Resilience Dealing with Disaster	2000
DTI		Business Continuity Management - Preventing Chaos in a Crisis	1999
CASU		Risk Management Core Standard	2001
CASU		Governance Standard	2002
CASU		Emergency Planning Organisational Controls Standard	2002
CASU		Information Management & Technology Organisational Controls Standard	2002
CASU		Records Management Organisational Controls Standard	2002
BSI	BS 4783	Storage, Transportation and Maintenance of Media for Use in data processing and information storage	1994
BSI-DISC	PD 3000-5	Guide to BS 7799	1998
BSI	BS/ISO 17799	Code of Practice for Information Security Management	1999
BSI	BS 7799-2	Specification for Information Security Management Systems	1999
BSI	PD 0008	Code of practice for legal admissibility and evidential weight of information stored electronically	1999
BSI	BS 5454	Recommendations for storage and exhibition of archival documents	2000
BSI	BS/ISO 15489	Information and Documentation - Records Management	2001
ISO	ISO/TC 215 WG4/N115	Security Requirements for Archiving of Health Records	2002
PRO		Management, Appraisal and Preservation of Electronic Records Vol 2	1999
PRO		Records Management: Human Resources	1999
PRO		Storage of semi-current Records: Standards for the management of Government Records	1999
PRO		Model Action Plan for Developing Records Management	2002
PRO		Hospital Patient Case Records: A guide to their retention and disposal (Revised)	2002
MDA	DB 9702	Electromagnetic Compatibility of Medical Devices with Mobile Communications	1997
LSE		Report on the Committee on the Financial Aspects of Corporate Governance (Cadbury Report)	1992
RCP		The Retention of Medical Records With Particular Reference to Medical Genetics	1998
CCTA		Managing Successful Projects with PRINCE 2	1998

Source	Reference	Title	Year
ICA	ISBN 1 84152 010 1	Internal Control: Guidance for Directors on the Combined Code (Turnbull Report)	1999
PHLS		Service Continuity Planning	1999