

PUBLICLY AVAILABLE SPECIFICATION

PAS 77:2006

IT Service Continuity Management

Code of Practice



ICS code: 35.020

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

BSi

British Standards



Document Sharing Hub

This Publicly Available
Specification comes
into effect on
11 August 2006

© BSI 11 August 2006
ISBN 0 580 49047 5

Amd. No.	Date	Comments

Contents

Page

ii	Foreword
iii	Introduction
1	1 Scope
2	2 Terms and definitions
5	3 Abbreviations
6	4 IT Service Continuity management
7	5 IT Service Continuity strategy
13	6 Understanding risks and impacts within your organization
14	7 Conducting business criticality and risk assessments
15	8 IT Service Continuity plan
20	9 Rehearsing an IT Service Continuity plan
25	10 Solutions architecture and design considerations
27	11 Buying Continuity Services
29	Annex A (informative) Conducting business criticality and risk assessments
36	Annex B (informative) IT Architecture Considerations
38	Annex C (informative) Virtualization
39	Annex D (informative) Types of site models
43	Annex E (informative) High availability
48	Annex F (informative) Types of resilience
51	Bibliography

Foreword

This Publicly Available Specification (PAS) has been prepared by the British Standards Institution (BSI) in partnership with Adam Continuity, Dell Corporation, Unisys, and SunGard. Acknowledgement is given to the following organizations that have been involved in the development of this code of practice.

- Adam Continuity
- Dell Corporation
- SunGard
- Unisys

Contributors:

- Oscar O'Connor, Lead Author
- John Pollard
- Richard Pursey
- Andrew Roles
- Brian Hayden
- Douglas Craig
- Stafford Hunt

As a code of practice, this PAS takes the form of guidance and recommendations. It should not be quoted as if it is a specification and particular care should be taken to ensure that claims of compliance are not misleading.

This Publicly Available Specification has been prepared and published by BSI, which retains its ownership and copyright. BSI reserves the right to withdraw or amend this Publicly Available Specification on receipt of authoritative advice that it is appropriate to do so. This Publicly Available Specification will be reviewed at intervals not exceeding two years, and any amendments arising from the review will be published as an amended Publicly Available Specification and publicized in *Update Standards*.

This Publicly Available Specification is not to be regarded as a British Standard.

This Publicly Available Specification does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with this Publicly Available Specification does not of itself confer immunity from legal obligations.

Attention is drawn to the following statutory instruments and regulations:

- Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework, Basel. Bank for International Settlements Press and Communications, 2005.
- The Civil Contingencies Act 2004. Cabinet Office: The Stationery Office.
- The Data Protection Act 1998. British Parliament: The Stationery Office.
- The Higgs Report on the Role of Non-Executive Directors: Department of Trade and Industry: The Stationery Office, 2001
- The Sarbanes-Oxley Act, 107th Congress of the United States of America, 2002.
- The Turnbull Report on Corporate Governance: Department of Trade and Industry: The Stationery Office, 1998
- The Orange Book Management of Risk – Principles and Concepts: HM Treasury, 2004.

Introduction

This code of practice provides guidance on IT Service Continuity Management (ITSCM). It is intended to compliment, rather than replace or supersede, other publications such as PAS 56, BS ISO/IEC 20000, BS ISO/IEC 17799:2005 and ISO 9001 (see Bibliography for further information).

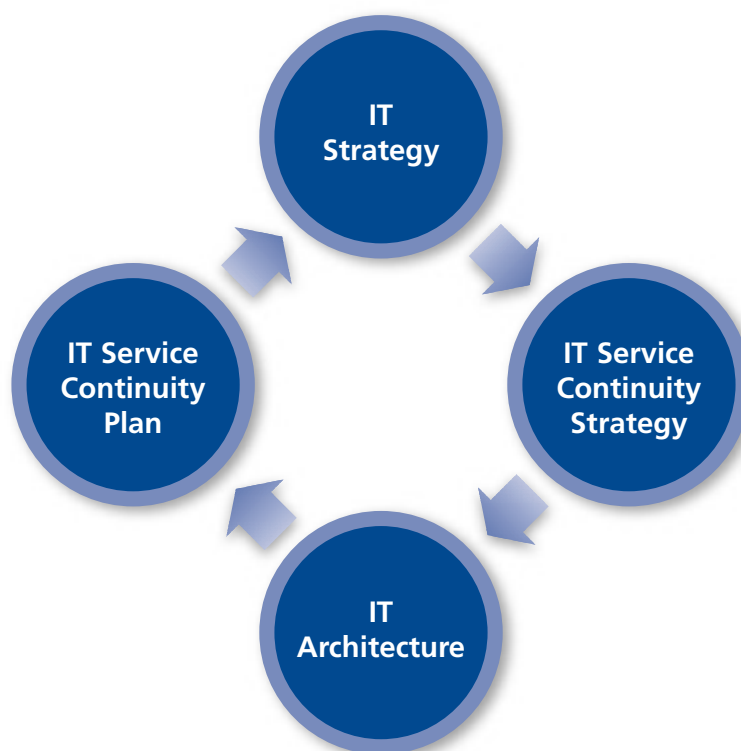
- PAS 56 provides guidance on best practice in Business Continuity Management, and while it mentions the need for IT Service Continuity it does not provide the detailed guidelines found in this code of practice;
- BS ISO/IEC 20000 provides guidance on best practice on Service Management and, as PAS 56, mentions IT Service Continuity, but not at the level of detail presented in this code of practice;
- BS ISO/IEC 17799:2005 provides detailed guidance on best practice in information security management, which is one aspect of IT Service Continuity Management. This code of practice does not directly address information security or physical and environmental security as these areas are covered by BS ISO/IEC 17799:2005;
- ISO 9001 provides guidance on best practice in Quality Management Systems. When implementing any recommendations found within this code of practice, the reader is encouraged to apply the quality assurance and control recommendations found in ISO 9001.

requirements and objectives set out in both the IT Strategy and ITSC Strategy. Once the architecture is defined, the organization can then define IT Service Continuity Plans for each element of the architecture. Feedback from (amongst many other sources) rehearsing the ITSC Plans can subsequently be used as input to the next iteration of the IT Strategy.

Many organizations believe that a loss of systems infrastructure will not happen to them or that a loss of such infrastructure will have a relatively low impact. However, while many of those organizations might believe that they have invested in adequate systems resilience, it is often apparent that such confidence is misplaced. In an age in which information technology is becoming evermore pervasive and increasingly critical within the day to day operations of many organizations, it is clear that the ability to continue to operate with any degree of success is likely to be severely compromised following loss of IT services. In addition it is evident that the duration of a tolerable IT outage is becoming ever shorter.

As Figure 1 suggests, there is a continuous cycle in the relationships between several important documents. The IT Strategy defines the organization's key policies and direction regarding information technology, systems and services. From this, the IT Service Continuity Strategy can be defined to ensure that the policies and standards for IT Service Continuity directly and explicitly support the objectives set out in the IT Strategy. This then enables the organization to define its IT Architecture based upon the

Figure 1 – The relationship between the IT Strategy, ITSC Strategy, IT Architecture and ITSC Plan



Whilst it is true that major events such as bombs, fires and floods make headline news, the majority of IT related incidents fall into the category of 'quiet calamities' that only affect an individual or a small subset of the organization. Examples of such common incidents include the theft of a mobile worker's notebook computer, the failure of an important business application and corruption of important or confidential data. These incidents have the potential to damage an organization's brand or public image and its reputation, not to mention its revenues and customer service. Such damage has the potential to destroy that organization unless appropriate action is taken to implement IT Service Continuity (ITSC).

In order to retain an appropriate sense of perspective, this document refers to 'incidents' and 'events' rather than 'disasters'. Since the Asian Tsunami of 2004 and Hurricane Katrina in 2005, the phrase 'disaster recovery' has taken on dimensions previously unknown and the authors felt it was inappropriate to describe the failure of IT systems, however disruptive, using the same language. Throughout the document the reader may encounter terminology which is used in other standards. To avoid ambiguity the reader should refer to the definition section to understand how such terminology is used in this document which may differ from other standards.

This document is intended to be read by a number of different audiences:

- Executive and Senior Management – to gain a high level understanding of the fundamental interdependencies between Corporate Governance, Business Continuity and IT Service Continuity in order to make better-informed investment decisions relating to ITSCM;
- Middle Management – to understand how decisions should be made regarding IT Service Continuity such that critical business processes survive disruption (ideally) or at the very least have the ability to recover from disruption in timescales required by the organization;
- IT Management – to understand the decision making processes required in order to ensure that IT Service Continuity strategies and plans fully support business priorities;
- IT Support and Operations – to gain a practical insight into how IT Service Continuity strategies should be drawn up and implemented in such a way as to add value to the organization as well as protecting it from IT-related incidents;
- Regulators, auditors, insurance and benchmarking organizations – to understand what best practice in IT Service Continuity Management implies for organizations so that these measures can be assessed as part of wider reviews of Corporate Governance and resilience.

This code of practice is designed for organizations of all shapes and sizes, whether in the private or public sectors.

It should not be regarded as a step-by-step guide to implementing IT Service Continuity Management but as guidance on the aspects of ITSCM which organizations should consider when investing in this area. Not all activities described herein will be applicable or appropriate for all organizations. In particular, small organizations should aim to use this code of practice as a reference guide in order to help them make informed decisions about what level of ITSCM would be appropriate for them given their individual characteristics. Throughout this code of practice certain terms have been used which may cause confusion. Such confusion is naturally not the intention of the authors, so the following guidance should be borne in mind when reading this document:

- The term 'business' is used when referring to the non-IT elements of an organization. This should not be taken to imply that this code of practice is aimed purely at private sector or commercial bodies. In each such instance, the term is used merely as convenient shorthand to avoid over-complicating the language used herein.
- This code of practice refers to 'rehearsing' ITSC Plans. Other publications in this field have referred to 'testing' and also to 'exercising'. The authors regard these terms as largely interchangeable and have opted to use the term rehearsing in this context as it implies not only testing that ITSC Plans are accurate and capable of being implemented, but also that the people required to implement them are guided, supported and provided with feedback on their own personal performance as well as that of the Plans. The authors did not feel that either of the other terms used in other publications quite conveyed the necessary emphasis on this aspect.
- The term 'data centre' is used to imply any location or facility where core information technology services are housed, whether that be the ultra-modern data centres that major organizations use or under the desk where a one-person business keeps its file server. No inference should be drawn regarding the applicability of guidance or recommendations to any type of non-data centre environment.

1 Scope

This Publicly Available Specification (PAS) explains the principles and some recommended techniques for IT Service Continuity management. It is intended for use by persons responsible for implementing, delivering and managing IT Service Continuity within an organization.

This PAS provides a generic framework and guidelines for a continuity programme including the following topics.

- What the required management structure, roles and responsibilities for implementing IT Service Continuity management are.
- How business criticality, risk assessments and business impact assessments should be performed to produce useable results.
- What business continuity plans contain and the steps required to respond to, and recover from, the identified risks within the context of specified business processes.
- How the development, rehearsal and deployment of the Business Continuity plan does not have to cost more in terms of money, risk or reputation than taking no action.
- Why a framework and capability should be developed for the organization to respond effectively to unexpected disruption.

This document is not intended to be used as step-by-step instructions for conducting any of the activities described herein. It is intended to provide an overview of a complete process on the assumption that information will already exist within the organization that would be identified by activities described in this document. Where this is the case, users of this document are encouraged to review the information in their possession to ensure that it includes all of the details required, and that it is up-to-date and accurate.

2 Terms and definitions

For the purpose of this PAS, the following terms and definitions apply.

2.1

abnormal service

level of service that deviates from the levels agreed for normal operations

NOTE Usually as a result of an incident causing disruption to normal service levels.

2.2

action plan

schedule of activities, lead times and dependencies of activities in order to address a particular requirement

2.3

asynchronous replication

periodic physical replication of data from one storage system to another

NOTE Typically over a wide area network.

2.4

atomic

requirement, transaction or objective which is self contained i.e. cannot be broken down further

2.5

audit log shipping

automated process for transferring records of transactions (audit logs) between primary and secondary systems

2.6

business continuity management plan

document that sets out to ensure resumption of critical business functions in the event of either an incident or unforeseen event that threatens the business

2.7

clustered system

two or more computer systems configured in such a manner that in the event of failure of a system or service run on it, operation is transferred to another system within the cluster

2.8

cold back-up site

provides the space but not the infrastructure needed to resume operations quickly

2.9

continuity procedures

set of predefined procedures to be followed in the event of an incident which disrupts normal service levels

2.10

data availability

measure a system's ability to deliver a predetermined level of data access during a system failure

2.11

dependency modelling

activity used to determine the inter-relationships and dependencies between functions and/or processes and how they affect the system or organization as a whole

2.12

disk imaging

method of copying a complete hard disk of a computer into a single file from which the gathered image can be distributed to a single or multiple computers to minimize the time and effort for the creation of computers that will have identical software and configurations to the original

2.13

domain

logical association of a defined environment and the assets within the pre-defined environment

2.14

downtime vs. cost vs. benefit model

model which analyses the costs of downtime and of the measures required to minimize downtime in the event of an incident and compares them against the benefits available to the organization from services being resumed

2.15

duplexed

ability to simultaneously send and receive data through a medium in both directions

NOTE When used to describe disk devices or disk connectivity it implies 'duplication' or 'mirroring'.

2.16

fail-back

return of service/operation from fail-over site

2.17

fail-over

ability for services offered by a component, server or system to automatically be undertaken by another component, server or system in the event of it's failure so that the impact of losing that device, server or system has a minimal impact on the service or services offered

2.18**failure modes and effects analysis (FMEA)**

structured quality method to identify and counter weak points in early conception phase of products and processes¹⁾

2.19**incident**

event that disrupts normal IT services

NOTE *This usage differs from that in ITIL [1].*

2.20**incident recovery**

activities required to respond effectively to an incident, with the primary objective being to ensure the resumption of normal service levels

2.21**I/O Processors**

allow servers, workstations and storage subsystems to transfer data faster, reduce communication bottlenecks, and improve overall system performance by offloading I/O processing functions from the host CPU²⁾

2.22**IP Address**

logical address of a system within an IP network

NOTE *The IP address uniquely identifies computers on a network. An IP address can be private, for use on a Local Area Network (LAN), or public, for use on the Internet or other WAN. IP addresses can be determined statically (assigned to a computer by a system administrator) or dynamically (assigned by another device on the network on demand).*

2.23**IT Architecture**

overall design of an organization's information technology and services including both physical and logical entities

2.24**IT Infrastructure**

physical devices which comprise an organization's information technology and services architecture

2.25**IT Service**

set of related information technology and probably non-information technology functionality, which is provided to end-users as a service

NOTE *Examples of IT services include messaging, business applications, file and print services, network services, and help desk services³⁾.*

2.26**IT Service Continuity Management**

supports the overall Business Continuity Management process by ensuring that the required information technology technical and services facilities (including computer systems, networks, applications, telecommunications, technical support and service desk) can be recovered within required, and agreed, business timescales

2.27**last mile telecoms provider**

organization responsible for the provision of telecommunications services from the national or local telecommunications infrastructure to a specific location

2.28**latency**

delay due to the time it takes to transmit data from one location to another

2.29**maintenance procedures**

procedures applied by an organization to ensure that their IT Infrastructure is maintained in optimum condition through both proactive and reactive measures

2.30**monte carlo analysis**

means of statistical evaluation of mathematical functions using random samples, often used in risk analysis of highly complex systems

2.31**Network Attached Storage (NAS)**

storage device that can be attached to the network for the purpose of file sharing

NOTE *In essence a NAS device is simply a file server.*

2.32**network protocol**

technological rules, codes, encryption, data transmission and receiving techniques which allow networks to operate

1) <http://www.fmeainfocentre.com/>

2) <http://www.intel.com/design/iio/>

3) <http://whatis.com>

2.33**operations bridge**

central facility used for monitoring and managing systems, services and networks

2.34**paper test**

mechanism for proving the hypothetical effectiveness of a process by working through scenarios in a discursive forum

2.35**point in time (PIT)**

consistent copy of the data taken at the same instance in time for one or more systems

2.36**recovery procedures**

procedures which result in the restoration of services following an incident

2.37**redundant routing**

resilient approach to data networking in which there are a minimum of two routes from each node in the network

2.38**rehearsing**

the critical testing of ITSC strategies and ITSCs, rehearsing the roles of team members and staff, and testing the recovery or continuity of an organization's systems (e.g. technology, telephony, administration) to demonstrate ITSC competence and capability

***NOTE** A rehearsal may involve invoking business continuity procedures but is more likely to involve the simulation of a business continuity incident, announced or unannounced, in which participants role-play in order to assess what issues may arise, prior to a real invocation.*

2.39**replication appliance**

device which provides functionality to replicate data to other storage systems

2.40**risk**

combination of the probability of an event and its consequence [ISO Guide 73:2002]

2.41**risk communication**

exchange or sharing of information about risk between the decision-maker and other stakeholders [ISO Guide 73:2002]

2.42**risk management plan**

document that sets out to define a list of activities, lead times and dependencies in order to mitigate one or more identified risks

2.43**risk mitigation**

set of actions that will affect either the probability of the risk occurring or its impact should the risk occur. These are summarized as risk transference, tolerate the risk, terminate or treat

2.44**risk monitoring**

iterative process of the risk owner checking and reporting on any changes in status of the risk log in terms of risk proximity, impact and response

2.45**stateful/stateless**

describe whether a computer or computer program is designed to note and remember one or more preceding events in a given sequence of interactions with a user, another computer or program, a device, or other outside element

***NOTE** Stateful means the computer or program keeps track of the state of interaction, usually by setting values in a storage field designated for that purpose. Stateless means there is no record of previous interactions and each interaction request has to be handled based entirely on information that comes with it. Stateful and stateless are derived from the usage of state as a set of conditions at a moment in time. (Computers are inherently stateful in operation, so these terms are used in the context of a particular set of interactions, not of how computers work in general).*

2.46**storage array**

two or more hard disk drives working in unison to improve fault tolerance and performance

2.47**synchronous replication**

instantaneous physical replication of data from one storage area to another, typically over a high speed interconnect such as fibre channel

2.48**test scripts**

definition of the specific tests to be enacted when proving the functionality and operation of a system or service

2.49**vulnerability report**

report which identifies the specific vulnerabilities of a specific system or service

2.50**work schedule**

defined set of activities and deliverables which, once completed, will result in the desired outcome of a procedure or project

2.51**Zero Data Loss (ZDL)**

remote replication method that guarantees not to lose any live data

2.52**zoning**

allocation of resources for device load balancing and for selectively allowing access to data only to specific systems

NOTE *Zoning allows an administrator to control who can see what is in a SAN.*

3 Abbreviations

For the purpose of this PAS, the following abbreviations apply.

BCM	Business Continuity Management
BCMP	Business Continuity Management Plan
BCMT	Business Continuity Management Team
BCSG	Business Continuity Steering Group
CMT	Crisis Management Team
DAS	Direct Attached Storage
DBMS	Database Management System
IMT	Incident Management Team
I/O	Input/Output
IT	Information Technology (also includes Information Systems (IS))
ITIL	Information Technology Infrastructure Library
ITSC	Information Technology Service Continuity
NAS	Network Attached Storage
OS	Operating System
RAID	Redundant Array of Independent Disks
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAN	Storage Area Network
UPS	Uninterruptible Power Supply
WAN	Wide Area Network

4 IT Service Continuity management

Information Technology Service Continuity (ITSC) is the collection of policies, standards, processes and tools through which organizations not only improve their ability to respond when major system failures occur but also improve their resilience to major incidents such that critical systems and services do not fail. It is related to a number of disciplines and should be undertaken with a complete and thorough understanding of the organization's policies, standards, processes and supporting services for:

- a) Business Continuity Management;
- b) Major Incident and Crisis Management;
- c) Corporate Governance and Risk Management;
- d) Information Technology (IT) Governance;
- e) Information Security and Data Protection.

ITSC management should also have a significant influence on IT strategy to identify information systems and services which require high levels of resilience, availability and capacity.

The purpose of risk management and ITSC management is not simply to be able to say that risk-based control mechanisms have been implemented. The management of risk can result in many tangible and intangible benefits to the organization if implemented with commitment and the right motivation. Risk management can be used to improve product quality, productivity, financial performance and working conditions. These benefits should be at the forefront of the participants' thinking throughout the process.

Risk can be seen as a positive approach to improving all aspects of the organization's performance. Every stakeholder can make a significant, positive contribution by considering, on a regular basis, the ways in which the organization's ability to achieve its objectives could be at risk. In order to do so, the organization's objectives should be communicated clearly to everyone involved in their achievement and communication on risks should be encouraged.

ITSC management addresses risks that could cause a sudden and serious impact, such that they could immediately threaten the continuity of the business. These typically include:

- a) loss, damage or denial of access to key infrastructure services;
- b) failure or non-performance of critical providers, distributors or other third parties;
- c) loss or corruption of key information;

- d) sabotage, extortion or commercial espionage;
- e) deliberate infiltration or attack on critical information systems.

Business Continuity Management (BCM) is concerned with managing risks to ensure that at all times an organization can continue operating to, at least, a pre-determined minimum level. The BCM process involves reducing the risk to an acceptable level and planning for the recovery of business processes should a risk materialize and a disruption to the business occur. In essence ITSC management should be a part of the overall Business Continuity plan and not dealt with in isolation.

5 Service Continuity strategy

5.1 Defining an IT Service Continuity strategy

NOTE The following frameworks are well regarded and respected and can be used for additional information when creating a comprehensive IT Strategy that will assist in clarifying and defining your ITSC Strategy. For additional reading please refer to:

- CMM, Capability Maturity Model, <http://www.itservicecmm.org>;
- CobiT 4.0, Control Objectives for Information and related Technology, <http://www.itgi.org>;
- ITIL, IT Infrastructure Library, <http://www.itil.co.uk>.

An ITSC strategy should define the direction and high-level methods that should meet IT service level objectives. It should ensure a business is never compromised by a lack of IT availability beyond acceptable, predefined and regularly reviewed levels of uptime and performance.

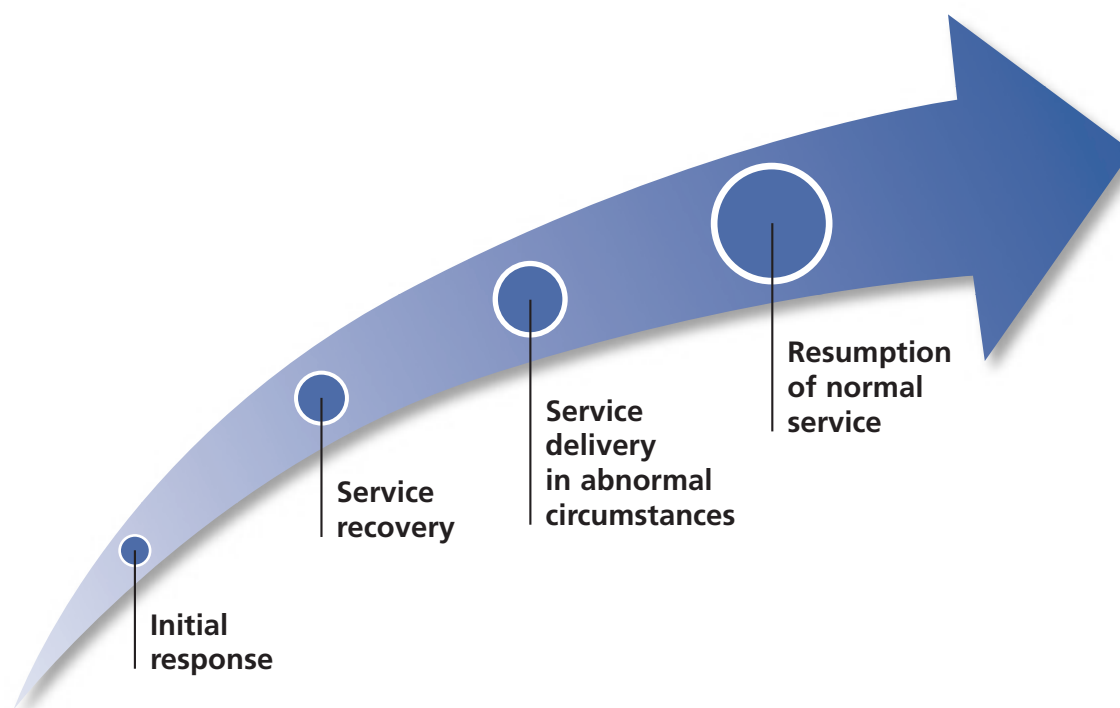
The ITSC strategy should be agreed at Board level and ideally be fully endorsed by the CEO. A Board member should be accountable for the strategy and be referred to when deciding on new business initiatives including mergers and acquisitions, directional change and any decision that could have an impact on ITSC.

In devising an organization's ITSC strategy, it is advisable to consider four discrete but linked stages in the management

of a major incident, as also shown in Figure 2:

- initial response – covering the initial actions required to ensure the safety and welfare of people affected by the incident, to activate the relevant incident management teams and determine the level of response which is appropriate to the incident;
- service recovery – this may take place in a number of stages depending upon the needs and scale of the organization but should involve the restoration of all required services in priority order to pre-agreed (possibly degraded) levels of service;
- service delivery in abnormal circumstances – until the organization is ready and able to resume normal service operations there is still a need to continue to operate required services at the pre-agreed service levels until the circumstances permit these 'abnormal services' to be failed back to 'business as usual' and decommissioned;
- normal service resumption – as with service recovery, the resumption of normal service may take place in stages according to the needs and priorities of the organization. Only when each service has been validated and verified as being 'back to normal' should the secondary systems be decommissioned. This stage is only complete when all of the organization's IT services are restored to normal service levels.

Figure 2 – Major Incident Management



The ITSC strategy should enable the organization to plan for and rehearse the whole life cycle of a major incident from the point of initial disruption, through the recovery, to abnormal service to the point where normal service levels are once again guaranteed.

The strategy should be developed from a clear understanding of the organization's need for IT services and the agreed service levels that are required from time to time, taking into account:

- a) priority for key business units at given moments in time;
- b) peak loads on business;
- c) strategically important business periods e.g. reporting periods, manufacturing deadlines etc;
- d) compliance with business Continuity Management Plans and objectives;
- e) investment vs. risk;
- f) impact of failure or loss;
- g) recovery time objectives;
- h) acceptable levels of downtime and performance;
- i) system changes and upgrades;
- j) new projects;
- k) interdependencies;

- l) compliance with legislation;
- m) deadline management;
- n) rehearsing and rehearsing recovery plans;
- o) data protection;
- p) data availability;
- q) plan maintenance;
- r) education and awareness programmes for all IT staff.

The strategy should not define the detailed tactics but should set the direction of the individual components of an ITSC plan.

5.2 Creating an ITSC strategy

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

As shown in Figure 3, an ITSC strategy should have six main elements all of which are part of a continuous cyclical process.

Figure 3 – ITSC strategy elements



The six elements in the ITSC Strategy Process are:

- a) Understanding the business requirements and agreeing service levels – The ITSC strategy should be aligned with corporate strategy and in line with the pre-defined business goals of the organization. To provide a sound base to start from and allow for continued and controlled growth of the ITSC strategy a defined service level should be agreed. This will allow for clearly defined service levels which are specific and can be measured, analysed and improved on.
NOTE Refer to ITIL [1] for guidance on agreeing service levels.
- b) Reviewing the IT strategic vision and updating objectives – Change is inevitable and allowances should be made to ensure that the ITSC strategy is always aligned with the overall IT strategy and business goals. The overall IT strategy and its ITSC strategy should be constantly assessed and updated.
- c) Performing regular risk assessment and dependency modelling (internal and external) – Changes in the nature of the risks and dependencies should be expected and in order to ensure that these variations are controlled and taken into cognisance in the ITSC strategy they should be reassessed regularly. The quantity and quality of the regular dependency modelling exercises will depend on the nature of the environment.
- d) Building and embedding an ITSC culture from new project inception – When initiating an IT project consideration should be given to how the deliverables will support or enhance the ITSC strategy.
- e) Exercising, maintaining and auditing continuity and recovery plans – The continued rehearsals, maintenance and auditing of the continuity and recovery plans an organization can ensure that:
 - 1) the plans are constantly improved on and up to date;
 - 2) staff are familiar with the plans' contents;
 - 3) the plans are fit for purpose and relevant;
 - 4) resource requirements for management of major incident are understood and planned for;
 - 5) visibility and governance are provided for the teams exercising the plans and the organization as a whole.
- f) Monitoring performance – Constant improvements can only be made if the pre-defined service levels in the first stage are constantly monitored, measured, analysed and reported on. Monitoring performance should be central to this.

Everyone within the organization who is likely to participate should be reminded of the importance of initiating an ITSC programme and the priority it should be afforded.

NOTE Experience shows that a better quality of response is achieved if appropriately worded instructions are received from

an executive level within the organization. This is particularly true within larger organizations where a variety of individuals and levels of management are likely to be involved.

A suitable mandate should be sent to the relevant department heads and others who may be involved in the programme as a matter of priority before the commencement of the programme.

The business should define the levels of service it expects from the IT department. It should clearly define priorities, allowing the Head of IT to determine which services have greater protection, resilience and redundancy over others.

IT resilience costs money. The depth and detail of an ITSC strategy will for many companies be driven by risk versus cost. A strategy should be developed that delivers improvement over time focusing on key issues and priorities where risks are high and the impact of loss or failure significant. This in itself is not a simple algorithm and will require an impact and risk analysis before budgets can be assigned and a strategy ratified.

An initial strategy should be chosen by defining a strategy around the priorities and calculating the associated costs for delivery or by allocating a budget and then building a strategy around the available budget.

NOTE It is rare that an organization will have implemented an ITSC plan from the outset of IT infrastructure implementation. Many IT environments have evolved over time and are often a combination of a number of inconsistent strategies.

5.3 The role of the Board and Executive

At Board or Executive level, business priorities should be defined focusing on key deliverables such as manufacturing deadlines, financial reporting, customer service levels etc. The impact of loss or failure should be defined, often a by-product of a BCMP. These priorities should help to define which areas of the IT infrastructure need strengthening to improve resilience.

The Head of IT should then determine which IT processes and systems the key business priorities depend upon. This dependency modelling should show the impact of individual or collective component failure. It should allow the strategist to determine vulnerable weaknesses in an IT infrastructure and measure the impact of failure from an operational level.

The Board of Directors (or equivalent) should have a vision for the organization's future, a growth plan and a series of objectives. This information acts as a long-term steer for the ITSC strategy which will in time help steer investment decisions and corporate direction.

5.4 Identifying requirements and weaknesses

The foundation of an ITSC strategy should be to ensure an embedded resilience throughout an IT infrastructure. The Head of IT should commission an internal review of all areas of potential weakness from single points of failure through to redundancy, supply chain dependence and general IT housekeeping processes such as secure back-up and restore technology. From this review, a strategy of improved resilience can be determined.

An ITSC strategy should make use of history and trend reports highlighting downtime experience, proven areas of weakness and service level reports.

A vulnerability report is highly likely to involve expenditure. Key to implementing an ITSC strategy is to measure the costs of downtime vs. resilience expenditure i.e. impact and risk vs. cost. This should be done by working with the Board to calculate the cost of downtime on key business functions on an hourly basis. This determines budgets and also focuses attention on service level agreements required as a result of measured downtime.

Department Heads should provide their service level requirements and the level of uptime they require within a steady state as well as the recovery time objectives after an incident. These should be measured using a downtime vs. cost vs. benefit model.

Advancements in technology carry an inherent demand for constant change and improvement. Enhancements to an IT infrastructure should be planned, rehearsed, and carefully managed with clear contingency plans in place should the implementation fail. The ITSC strategy should take into account a tolerance for downtime for major system upgrades and changes. Should scheduled downtime be unacceptable then plans should be put in place for duplicate environments running parallel systems. Agreement should be reached on levels of foreseen downtime prior to defining the strategy.

Due consideration and research should be undertaken on current and forthcoming legislative requirements as well as good practice guidelines on aspects of business continuity and IT resilience. The Board (or equivalent) and especially Non-Executive Directors, if present, should steer an organization towards compliance and healthy business management.

The ITSC strategy should also include an ongoing and continuous process for change management including involvement of third party suppliers as well as internal customers. An agreement should be reached at Board or Executive level on levels of investment and priorities for

expenditure on IT resilience. It should agree on its policy on outsourcing risk management to third party suppliers e.g. incident recovery companies and third party maintenance organizations, (see Clause 11).

5.5 Management structure and roles

5.5.1 General

The management structure should be a standard, three tiered structure used widely within both the private and public sectors for major incident and crisis management.

The three tiers are:

- a) Bronze – operational level: Incident Management Team (IMT);
- b) Silver – tactical level: Business Continuity Management Team (BCMT);
- c) Gold – strategic level: Crisis Management Team (CMT).

In terms of relative size and subsidiarity, the relationship between these teams is illustrated in Figure 4:

Figure 4 – Management structure



Depending upon the seriousness of the incident, ITSC should be managed at both Silver (BCMT) and Bronze (IMT) levels, with Bronze teams being established for each IT service, coordinated by a dedicated IT service Silver team. The Gold team (CMT) should provide high level direction, prioritisation and coordination and should take sole and direct responsibility for communicating with external stakeholders, including the media, emergency services and public authorities where that is appropriate or required.

Some organizations (mainly large) have internal teams specializing in Corporate Risk and Business Continuity Management from whom support and assistance should be sought when constructing, rehearsing and invoking ITSC Plans.

As these teams are most likely to comprise members of the organization's management team, i.e. not business continuity or incident management specialists, it is possible that for both rehearsals and live activations additional specialist support may be appropriate. Consideration should also be given to the resource requirements implied by the activation of these teams and their associated ITSC Plans, since there is a possibility that more resources will be required during the initial stages than are directly available within the organization.

5.5.2 Incident Management Team

In the event of disruption, whether from a predicted source or elsewhere, the IMT for the affected IT service should be activated.

The IMT should determine whether the nature and extent of the disruption warrant the deployment of the relevant BCMP, and if so should:

- a) Determine the nature of the disruption and, if necessary, coordinate with the organization's Problem Management⁴⁾ function to adapt existing procedures for the initial response to the disruption.
- b) Implement the selected procedures, securing the required resources through the BCMT where appropriate.
- c) Identify, and where appropriate adapt, the relevant continuity procedures to ensure that the business continues to operate as near to normal a manner as possible for the duration of the disruption. All such activities should be coordinated through the BCMT.
- d) Identify, and where appropriate adapt, the relevant recovery procedures to ensure that the business recovers from disruption in a timely and controlled manner once the root cause of the disruption has been

eliminated. All such activities should be coordinated through the BCMT.

- e) Activate the BCMT who investigate the requirement for further Bronze teams to be activated. Whilst the IMT is active, all activities should be coordinated through the BCMT to ensure that no action taken by one IMT conflicts with actions taken by others.
- f) Communicate with all parts of the organization affected by the disruption on a regular basis regarding progress and the actions initiated by the IMT.
- g) Organize, once recovery actions have been completed, a thorough review of its management of the disruption so all relevant lessons from the experience can be learned and incorporated into procedures and training programmes.

5.5.3 Business Continuity Management Team

The BCMT should determine the nature and extent of the disruption and should:

- a) coordinate the activation and management of all relevant IMTs;
- b) coordinate the allocation of resources to IMTs;
- c) coordinate the management of undisturbed business;
- d) manage communication with regulators, investors, the media, associates and staff;
- e) ensure that the active IMTs have all the facilities, people and other resources that they require to mount effective response, continuity and recovery operations;
- f) where appropriate, activate the CMT.

5.5.4 Crisis Management Team

The CMT should be activated when an incident, or a combination of incidents, have such wide ranging impact as to require organization-wide response coordination. When active, the CMT should take responsibility for the coordination of all active BCMTs and for all communication with all external stakeholders, especially customers, suppliers, regulators, the media and the public.

5.5.5 Learning lessons

In order to ensure that each real or rehearsed invocation of the ITSC management contributes to the ongoing improvement of the ITSC strategy and related plans, each team should maintain a comprehensive journal, including details of:

- a) the reasons for the team being activated, including details of the disruption that occurred, and justification for the team being activated;
- b) any amendments made to the ITSC strategy and related plans and procedures as a result of the actual disruption being different in character to that predicted;
- c) all decisions made during the disruption, including supporting evidence;

4) <http://whatis.com>

- d) all events transpiring during the disruption, their effects and likely causes;
- e) all actions taken and evidence of their results;
- f) all communication in relation to the disruption, including the other parties involved, the nature of the communication and what information was passed in each direction.

This journal should cover the period from the time the team is activated to the time it stands down. All entries in the journal should include details of the date and time the entry was made, and by whom.

The completed journals should be used to support future reviews of business and IT service continuity plans and their effectiveness. Therefore, stringent change control should be applied on these journals, and no changes of any nature should be permitted once the team has stood down.

5.6 IT Service Continuity in a changing environment

Business is by its very nature dynamic. It changes regularly and with change comes risk; not only risk of failure but risk of destabilizing existing policies and strategies. Therefore, the ITSC strategy should be resilient to change and also adaptable.

The key factors that should be considered to ensure that the ITSC strategy and plans remain appropriate for the organization as it and its environment change include the following.

- a) Board level responsibility and accountability for the ITSC strategy should be to help keep an ITSC strategy current as the organization changes, develops and grows. BCM and ITSCM should be a high-profile ingredient to Board level thinking and should be the most important aspect of any continuity plan.
- b) The change management process should include all parties responsible for the ITSC strategy, both its compilation and its delivery. No change to the IT infrastructure should be considered until the implications of the change have been assessed and understood and contingency plans are rehearsed.
- c) The procurement process for new IT systems should include sign-off that resilience has not been compromised by even the most simple of upgrades or improvements. Non-IT expenditure could still have an impact on IT resilience such as recruitment (system overheads), marketing campaigns (web site activity) etc.
- d) Due diligence on merger and acquisition (M&A) activity should include a resilience assessment. Often, M&A activity can bring perceived cost saving benefits such as branch or office closure. This can also reduce resilience through loss of fail-over sites, loss of secondary systems, and inherent redundancy.

- e) Service levels (e.g. uptime statistics) should be reviewed as a Board agenda item each month. Trend analysis can show even a slight decline in service which can be an indicator of bigger problems.
- f) Testing and rehearsing contingency and recovery plans should be an essential ingredient to keeping an ITSC strategy current. Ensuring a department or application can be recovered fully, after failure can ensure simple errors and problems are minimized. This includes performing complete data back-ups as well as testing third party suppliers.
- g) Supplier's ability to maintain appropriate levels of service should be regularly assessed. Including suppliers such as incident recovery and maintenance providers in the change management loop is highly recommended.
- h) Remunerating staff against service levels can help ensure the relevant level of awareness reaches all levels of the organization.
- i) An internal/external audit of plans.